LUISS

Dipartimento
di Giurisprudenza

Cattedra di Diritto Penale, Parte speciale

Profili penali delle criptovalute

Prof. Antonino Gullo
_____
RELATORE

Prof. Maurizio Bellacosa
_____
CORRELATORE

Antonio Rosato
Matr. 130533
_____
CANDIDATO

Anno Accademico 2018/2019

A chi mi vuol bene

PROFILI PENALI DELLE CRIPTOVALUTE

INDICE

INTRODUZIONE

Verso la fine del 2008 viene pubblicato da Satoshi Nakamoto il *white paper* "*Bitcoin: a Peer-to-Peer Electronic Cash System*" nel quale in sole nove pagine vengono enunciati i principi teorici e di funzionamento del protocollo *Bitcoin*.

Obiettivo dichiarato della sua creazione è quello di dar vita ad una "moneta elettronica" basata sul modello di rete *peer-to-peer* usufruibile in assenza di un ente centrale (banche o istituti finanziari) che garantisca il corretto funzionamento del sistema di pagamento. Il carattere innovativo proposto nel protocollo *Bitcoin* è la risoluzione del c.d. "*problema della doppia spesa*" (che si pone quando un soggetto "spende" più volte la stessa valuta digitale, reso possibile dalla facile duplicabilità dei dati informatici), costituita dall'utilizzo della *proof of work* e in particolare della *blockchain* (letteralmente "catena dei blocchi").

Quest'ultima, è probabilmente la soluzione tecnologica più innovativa degli ultimi anni, che si presta ad innumerevoli ed (ancora) inesplorate applicazioni pratiche. Non solo, quindi, è alla base del funzionamento di tutte le criptovalute attualmente in circolazione, ma ha visto crescere il suo utilizzo e sviluppo con la creazione dei c.d. *smart contracts* ("contratti intelligenti").

Giacché da sempre è il diritto a rincorrere la tecnologia, come Achille e la tartaruga, è necessario comprendere a pieno il funzionamento delle nuove tecnologie per poter riuscire a regolare correttamente e senza ambiguità i loro utilizzo e i conseguenti effetti sulla vita dei consociati.

Quando il legislatore si trova a dover emanare norme che tengano conto dei tecnicismi delle nuove tecnologie, molto spesso si assiste ad una produzione legislativa imprecisa e contraddittoria; oppure, si danno vita a norme che al momento della loro entrata in vigore risultano già obsolete, in virtù dell'ampia differenza di passo del progresso scientifico rispetto alla macchina legislativa.

Per questo motivo, nella prima parte del seguente elaborato verrà analizzata e sviscerata la tecnologia *blockchain*, dal suo funzionamento alle diverse declinazioni

pratiche: non solo le criptovalute (*bitcoin* ed altro) e *smart contracts,* ma anche le nuove forme di raccolta diffusa di capitale, le c.d. "*Initial coin offerings*" (ICO).

Verranno anche esaminate le norme attualmente in vigore (e in continuo aggiornamento) nel nostro ordinamento e non, cercando anche di enucleare quelle che possono essere le migliori strade da percorrere a livello legislativo, per evitare di imbrigliare la tecnologia negli enunciati normativi con l'effetto di stroncarne sul nascere lo sviluppo. Il tutto, corroborato dall'esigenza di tutelare gli individui dai significativi abusi che possono comportare serie offese ai più importanti beni giuridici.

In virtù di quest'ultima considerazione, nella seconda parte si entrerà nel vivo nell'oggetto di indagine di questa tesi, ossia i profili penali delle criptovalute.

Quest'ultime, si prestano a diverse e polivalenti finalità illecite dovute sia alle loro intrinseche peculiarità (*in primis* l'anonimità/), sia alla circostanza che vengono utilizzate, nella maggior parte dei casi, per commettere crimini mediante sistemi informatici o la rete *internet*.

È stata circoscritta l'analisi delle fattispecie criminose configurabili attraverso le criptovalute ai reati contro il patrimonio e finanziari.

In particolare, verrà trattato il reato di riciclaggio e autoriciclaggio, unitamente al tema del *cyberalundering*, la nuova frontiera della ripulitura del "denaro sporco". Infatti, le criptovalute ma in generale la rete *internet* hanno dato vita a nuove modalità di realizzazione dei reati di riciclaggio. Il legislatore italiano (ma soprattutto a livello comunitario) ha provveduto ad emanare ed aggiornare le attuali discipline antiriciclaggio col fine di coinvolgere anche i prestatori di servizi relativi alle criptovalute, nella specie gli *exchange*, soggetti virtualmente posti alle dogane del mondo virtuale e reale.

Inoltre, verrà analizzata la possibilità di configurare i reati relativi all'abusivismo bancario e finanziario presenti nel T.U.B e T.U.F.: essendo l'utilizzo più diffuso delle criptovalute quello di mezzo alternativo al denaro, condotte che emulino le funzioni e le attività degli istituti bancari e finanziari senza la necessaria autorizzazione potrebbero integrare le fattispecie criminose previste nei due testi unici citati.

Infine, verrà anche valutata la possibilità dell'integrazione delle condotte dei reati tributari, offrendo una panoramica di quello che è l'inquadramento fiscale delle criptovalute. È molto frequente la compravendita o conversione delle criptovalute sulle

piattaforme c.d. *exchange*, che, grazie alla alta volatilità dei prezzi, può generare ingenti profitti. Inoltre, bisogna anche considerare i redditi dei diversi soggetti professionali che prestano servizi relativi all'utilizzo delle criptovalute, e valutare se concorrono a determinare reddito imponibile, la cui mancata dichiarazione o versamento potrebbe configurare i reati tributari previsti dal D.lgs. 74/2000.

Nella terza ed ultima parte, con l'obiettivo di fornire un'indagine completa dei profili penali non solo dal punto di vista sostanziale ma anche squisitamente processuale, verranno affrontate le tematiche delle prove elettroniche e delle indagini informatiche.

Nello specifico, verranno anche tracciate quelle che sono le problematiche che si presentano quando oggetto dei mezzi di ricerca della prova siano le criptovalute (in particolare in sede di sequestro), e verranno enucleate le peculiarità della c.d. *bitcoin forensics,* ossia le tecniche investigative e di indagine correlate alle criptovalute.

Pertanto, obiettivo di questo elaborato è tracciare i profili di rilevanza penale nelle odierne fattispecie in vigore derivanti dall'utilizzo delle criptovalute, ma, nel corso della trattazione si coglierà l'occasione per proporre nuove soluzioni legislative e per sottoporre all'attenzione del lettore problematiche attualmente non di agevole soluzione. Si vedrà, in particolare, come in alcuni casi uno sforzo ermeneutico non sia sufficiente, anche in virtù del divieto di analogia *in malam partem* che caratterizza a tutto tondo il diritto penale.

CAPITOLO I

LA *BLOCKCHAIN*: LA TECNOLOGIA ALLA BASE DELLE CRIPTOVALUTE. PROFILI GIURIDICI

SOMMARIO: 1. L'innovazione tecnologica e le trasformazioni socio-economiche. – 1.2. La *blockchain* e il *Bitcoin*. Una breve disamina storica. – 1.3. Le possibili applicazioni della *blockchain*. – 1.4. Le caratteristiche della *blockchain* e del protocollo *Bitcoin*. – 1.5. La *blockchain*, inquadramento giuridico. Una prima definizione nell'Ordinamento italiano. – 1.6. Le tipologie di *blockchain*. – 1.7. La crittografia nella *blockchain*. Chiavi pubbliche e private. – 1.7.1 (*Segue*) I principi teorici del funzionamento di *Bitcoin*: il principio del consenso e la teoria dei giochi. – 1.7.2. (*Segue*) Il *mining* e la *proof of work*. – 1.7.3. (*Segue*) La *proof of stake* e altre soluzioni tecniche per il sistema del consenso. – 1.8. I *token*. – 1.9. Le ICO e i relativi profili giuridici. La casistica statunitense. – 1.9.1. (*Segue*) Le casistiche europee: le linee guida della FINMA. – 1.9.2. (*Segue*) Le norme riguardanti le ICO della Repubblica di Malta. – 1.9.3. (*Segue)* Le pronunce dell'Agenzia delle Entrate, CONSOB e Banca d'Italia in tema ICO e *tokens*. – 1.9.4. Il report dell'ESMA sulle ICO e i "*Crytpo-Assets*". – 1.10. La *blockchain* come veicolo di valuta: il *bitcoin*. Il suo inquadramento giuridico e profili penali. – 1.11. Oltre i *bitcoin*: *Ethereum* e le altre criptovalute. – 1.12. Conclusioni.

1. L'innovazione tecnologica e le trasformazioni socio-economiche

Nel corso della storia, il succedersi di continue e cicliche innovazioni tecnologiche ha mutato il modo di vivere dell'uomo, di interagire ed organizzare la propria vita. Anche l'economia è stata da sempre influenzata dalle scoperte in ambito scientifico e tecnico: la rivoluzione industriale, l'elettricità, il petrolio, hanno portato cambiamenti nei metodi di produzione e di trasporto, incidendo profondamente sul contesto socio-economico.

In particolare, negli ultimi anni la storia dell'uomo è stata caratterizzata dal passaggio da un tipo di società industriale ad un tipo di società cosiddetta «*dell'informazione*»[1] rivoluzionando profondamente il contesto sociale in cui vive l'uomo. Se nel passato prossimo era la produzione industriale a dominare la scena

[1] SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, ed. III., Torino, 2016, 1

economica ora sono i "dati" ad essere al centro dell'attenzione. L'invenzione del *computer*, del *world wide web*, degli *smartphones* e da ultimo l'accrescersi del fenomeno dell'*internet of things,* hanno sempre più trasformato l'individuo e la società[2]. Il cittadino vive oggi in un mondo globalizzato, interconnesso e dominato dalla tecnologia[3].

Al pari delle precedenti rivoluzioni delle arti e della tecnica, anche i ritrovati tecnologici più recenti offrono numerose opportunità, ma nascondono rischi significativi. L'annullamento dei confini nazionali, l'interconnessione degli individui e dei *devices* utilizzati mette in pericolo i beni giuridici c.dd. di nuova generazione quali la *privacy*, l'identità digitale, il diritto all'oblio.

Il vortice del cambiamento avvolge anche il singolo individuo, che è costretto a sviluppare nuove e specifiche capacità tecniche correlate all'uso dei nuovi dispositivi di nuova generazione; si tratta di competenze sempre più specialistiche, in continua e rapida evoluzione[4].

Una delle innovazioni tecnologiche che sta prendendo piede negli ultimi anni è la *blockchain* (letteralmente "catena di blocchi"), tutt'oggi conosciuta generalmente come la tecnologia alla base del funzionamento delle criptovalute[5]. Essa, in realtà, non è impiegata unicamente come veicolo del flusso delle valute virtuali ma vanta applicazioni pratiche in contesti eterogenei per la soluzione di svariate problematiche[6]. A seconda delle applicazioni pratiche, la *blockchain* può far sorgere questioni collegate

---

[2] OECD, *Future Technology Trends,* in *OECD Science, Technology and Innovation Outlook,* 2016, Parigi, 79

[3] «*la circostanza che l'impiego delle tecnologie, di cui si è detto, permette una globalizzazione delle relazioni umane prima inimmaginabile, incidendo pure sul tipo del luogo dell'incontro. Il flusso dei rapporti resi possibili dall'energia dei* bit*, che si sviluppa attraverso il supporto pur sempre materiale delle reti, si delocalizza, dematerializzandosi e, ad un tempo, dilatandosi: crea uno spazio nuovo, cui convenzionalmente possiamo ricondurre la metafora della nuvola (*cloud*)*» BERLINGÒ V., *Il fenomeno della* datification *e la sua giuridicizzazione* in *Rivista trimestrale di diritto pubblico*, fasc. 3, 2017, 642

[4] «*abbiamo uno sviluppo esponenziale della tecnologia che si presenta come capace di sostituire l'uomo, tanto più se è persa la consapevolezza che in molti ambiti l'apporto umano è valore aggiunto fatto non solo di tecnicalità, ma di capacità critiche e di inventiva, basate su competenze sedimentate che non possono appartenere alle macchine.*» NASTRI M., *Nuove tecnologie: l'ultima domanda* in *Notariato* n. 5/2018, 485

[5] «*nowadays the blockchain technology is cosidered as the most significant invention after the internet. if the latter connects people to realize online business processes, the former could decide the trust problem by peer-to-peer networking and public-key criptography.*», EFANOV D., ROSCHIN P., *The all-pervasiveness of the Blockchain technology* in *Procedia computer science* n. 123, Mosca, 2018, 116

[6] OECD, *op. cit.*, 81

al suo "abuso", inteso come un utilizzo a fini illeciti. La storia delle scoperte scientifiche è ricca di esempi di nuovi strumenti concepiti per la soddisfazione di un determinato bisogno strumentalizzati per scopi criminosi. Nel corso dei seguenti paragrafi verrà fornita una panoramica della *blockchain*, del suo possibile utilizzo e del suo inquadramento giuridico in relazione alle fattispecie di reati configurabili.

1.2 La *Blockchain* e il *Bitcoin*. Una breve disamina storica

La *blockchain*, in prima analisi, non costituisce nei suoi elementi essenziali una novità per quanto riguarda l'esigenza dell'uomo di registrare e contabilizzare transazioni. Infatti, essa non è altro che un libro mastro (*ledger*) distribuito e decentralizzato dove sono riportate tutte le transazioni raggruppate in una catena di "blocchi" collegati fra loro in successione cronologica[7].

Dalla nascita dei primi commerci ai tempi della Mesopotamia fu avvertito il bisogno di annotare i propri rapporti di credito e di debito; successivamente, viene innovato il metodo di tenere la contabilità, con la teorizzazione della partita doppia[8], sfruttata dai primi istituti bancari italiani.

Con l'avvento dei *computer*, *internet*, e i servizi di *cloud storage* è stato possibile conservare la contabilità ed i propri dati informatici sul proprio dispositivo ma anche "sulla nuvola", prevenendo ogni possibile distruzione o alterazione fisica di quello che in precedenza era un registro cartaceo dove venivano annotate le transazioni. Si è così rivoluzionato ulteriormente il modo in cui l'uomo trascrive e conserva i propri dati.

La *blockchain* ha rinnovato il modo di registrare le transazioni e di conservare i dati, trascrivendoli in una catena di blocchi concatenati. Sebbene si tratti di una tecnologia profondamente innovativa, essa sfrutta e riunisce in sé diverse soluzioni tecnologiche già esistenti prima della sua ideazione.

---

[7] MANENTE M., Blockchain*: la pretesa di sostituire il notaio,* in *Notariato*, n.3/2016, 212

[8] Le transazioni *bitcoin* derivano concettualmente dal metodo della partita doppia, infatti, «*tali transazioni sono iscritte con un metodo che ricorda da vicino le scritture contabili in partita doppia: semplificando, all'interno di ciascun blocco la differenza complessiva tra dare e avere, vale a dire tra bitcoin trasmessi e* bitcoin *ricevuti, deve sempre corrispondere a zero. La* blockchain *tiene traccia dell'attuale situazione di titolarità di tutti i* bitcoin *esistenti e della catena di trasferimenti che li ha riguardati a partire dalla loro creazione, in uno storico perpetuo delle transazioni.*», RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete* in *Contratto e impresa* n. 1/2019, 262

Una prima teorizzazione della *blockchain* è avvenuta nel 1991 con la pubblicazione dell'articolo "*How to time-stamp a digital document*" di Stuart Haber e W. Scott Stornetta, in cui furono teorizzati sistemi di certificazione temporale di *file* digitali, anticipando di fatto alcune soluzioni tecnologiche adottate nelle *blockchain* utilizzate al giorno d'oggi.

In generale, però, si riconduce la sua nascita con la pubblicazione del *white paper* di Satoshi Nakamoto[9] nel 2008 dove viene delineato l'innovativo protocollo del *Bitcoin*[10] basato appunto sulla *blockchain*. La vera innovazione, però, è nell'aver combinato tecnologie esistenti con la teoria dei giochi[11] ed un efficace sistema di incentivi che portano alla soluzione di alcuni problemi già sorti in precedenza riguardo i pagamenti tra più soggetti interconnessi in assenza di una terza parte che garantisse la veridicità e l'assenza di frodi da parte degli utenti[12].

Anche il *Bitcoin* però ha origini teoriche e pratiche che risalgono a molti anni prima della sua creazione. In particolare, nel 1994 venne concepito un sistema di pagamento virtuale con *Digicash*, creato da D. Chaum, ma a differenza del protocollo *Bitcoin* prevedeva ancora un ente terzo che garantisse sul buon fine di tutte transazioni.

Nello stesso periodo, un movimento di attivisti chiamato "*Cypherpunk"* nato circa alla fine degli anni Ottanta[13], pubblica nel 1993 il *«Cypherpunk Manifesto»*[14], il cui contenuto si incentra su temi quali la *privacy* e sull'uso della crittografia per tutelarla. Secondo il pensiero di suddetto movimento, la *privacy* in una società aperta necessita di sistemi di transazioni anonime, e l'anonimità della transazione non significa segretezza della stessa; l'anonimato è strumentale alla vera essenza della *privacy*, in quanto conferisce la facoltà agli utenti di rivelare la propria identità quando e solo se lo desiderano. Inoltre, il movimento si promette di difendere e garantire la *privacy* con

---

[9] "Satoshi Nakamoto" è soltanto uno pseudonimo, non si conosce attualmente la sua vera identità.

[10] Con il termine "*Bitcoin*" si indica il protocollo della criptovaluta; con "*bitcoin*", con l'iniziale in minuscolo, si fa riferimento alla "valuta"; CUCCURU P., *Blockchain ed automazione contrattuale. Riflessioni sugli* smart contracts in *Nuova giurisprudenza civile commentata*, parte seconda n. 1/2017, 108

[11] V. *infra* §1.7.11

[12] ANTONOPOULOS M. A., *Mastering Bitcoin*, 2015, 6

[13] ARVIND N., *What appened to the crypto dream, Part 1*, in *IEEE Security & privacy*, v. 11, 2, marzo-aprile, 2013, 3

[14] HUGHES E., *A Cypherpunk's Manifesto,* consultabile al seguente link: *https://www.activism.net/cypherpunk/manifesto.html*

la crittografia, firme digitali e valute elettroniche: tutti elementi che verranno ripresi come base teorica oltre dieci anni dopo da Satoshi Nakamoto per ideare il protocollo *Bitcoin*. In generale, i principi fondanti il movimento crittoanarchico[15] si concentrano sulla contrapposizione e sull'inevitabile indebolimento del potere statale e delle istituzioni, non tenendo in considerazione l'esistenza delle leggi, eccettuate quelle espresse e applicate da codici informatici[16].

Nel 1998, veniva divulgato da Wei Dai B-money, un *white paper*[17] (dichiaratamente ispirato ai principi del movimento crittoanarchico) dove venivano proposti due modelli di sistemi di pagamento decentralizzati con cifratura; il primo sistema di pagamento è stato dallo stesso autore definito impraticabile in virtù dell'assenza della risoluzione al problema della doppia spesa; il secondo, invece, si basa sulla *"proof of stake"*[18] che incentiva gli utenti a non porre in essere condotte fraudolente minacciandoli di far perdere loro quanto depositato, promuovendo cosi l'adozione di condotte non fraudolente.

Infine, nel 2004 viene teorizzata da Hal Finney, prendendo a modello il funzionamento di *Hashcash* (sistema *antispam* proposto da Adam Back nel 1997), ciò che costituisce uno dei cardini del protocollo *Bitcoin*, la "*proof of work*"[19].

Dunque, quello poc'anzi illustrato è il *background* storico, teorico e tecnologico che ha portato Satoshi Nakamoto alla l'ideazione del protocollo *Bitcoin* sfruttando la tecnologia *blockchain* nel 2008, e nel 2009 a creare il primo "blocco" (*Genesis block*) della *blockchain* di *Bitcoin*. Infatti, alcuni autori[20] considerano il *Bitcoin* come l'espressione pratica dell'ideologia del movimento crittoanarchico, basato sull'assenza di necessità dell'intermediazione statale nell'ambito dei sistemi digitali di pagamento e delle transazioni dei privati, cosi come più in generale nell'contesto dell'emissione e gestione del mercato della moneta.

---

[15] Espressi da Timothy C. May, nel c.d. "*Cryptoanarchist Manifesto*".
[16] ARVIND N., *op. cit.*, 4
[17] Consultabile al seguente link: *http://www.weidai.com/bmoney.txt*
[18] V. *infra* 1.7.3
[19] V. *infra* 1.7.2
[20] Tra cui ROSEMBUJ T., *Bitcoin*, Barcellona, 2016, 15

1.3 Le possibili applicazioni della *blockchain*

Nonostante la sua funzione più diffusa e conosciuta sia quella relativa al protocollo *Bitcoin*, la *blockchain* si presta a innumerevoli applicazioni pratiche in diversi contesti.

La *blockchain* utilizzata come valuta ha potenzialità rilevanti[21] nel settore della finanza e dei pagamenti digitali[22]. Essa può essere utilizzata per registrare e conservare in modo sicuro transazioni di acquisto e vendita di strumenti finanziari abbattendo i costi delle commissioni richiesti dagli intermediari o dalle banche[23]. Ovvie sono poi le applicazioni nel campo dei pagamenti digitali, tramite lo scambio di "cripto monete" annotate nei blocchi, ma in quest'ambito ci sono ancora aspetti e criticità da risolvere e che sono già oggetto di sviluppo, quali il tempo di validazione delle transazioni[24]. A parte queste immediate applicazioni pratiche, vi rientrano anche l'emissione di mutui, prestiti e di strumenti finanziari da parte di banche e intermediari finanziari.

Astraendo la *blockchain* dall'impiego per finalità valutarie, numerose sono le potenzialità in settori diversi da quello finanziario. Uno di questi riguarda la registrazione e conservazione della titolarità di beni immobili o mobili[25], allo stesso modo del catasto[26]. Sarà possibile certificare la titolarità del bene, iscriverci ipoteche e altri privilegi, tutto nella più completa trasparenza ed efficienza, risparmiando tempo e costi per la Pubblica Amministrazione.

---

[21] OECD, *Future Technology Trends,* in *OECD Science, Technology and Innovation Outlook,* Parigi, 2016, 82

[22] CUCCURU P., *op. cit.* 110

[23] «*Ma è ormai un dato incontrovertibile che il* Bitcoin *e le altre monete digitali propongano — nel loro utilizzo — costi di transazione più bassi rispetto ai servizi di pagamento tradizionali, potendo, per tale motivo, spingere gli attuali market leader aduna riduzione dei prezzi sotto la pressione concorrenziale. Infatti, la sicurezza garantita dalla crittografia senza alcun tipo di investimento particolare, e l'assenza di soggetti terzi per l'intermediazione del pagamento, rendono le transazioni in* Bitcoin *sostanzialmente più economiche e più veloci rispetto ai circuiti di pagamento elettronico tradizionali, aprendo il mercato dei micropagamenti e garantendo per le rimesse internazionali un nuovo strumento di riduzione dei costi, idoneo tecnicamente ad integrarsi con gli altri sistemi di pagamento elettronici.*», BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto e informatica*, 2017, 48

[24] Il protocollo *Bitcoin* elabora circa 7 transazioni al secondo, mentre il circuito Visa circa 24.000. Altre criptovalute esistenti hanno tempi di transazione più rapidi rispetto al protocollo *Bitcoin* ma sono ben lontane dalla velocità di Visa (*Ripple*: 1500 transazioni al secondo, *BitcoinCash* 60, *Ethereum* 20). Fonte: *https://howmuch.net/articles/crypto-transaction-speeds-compared*.

[25] Critico a riguardo, MANENTE M., *op. cit.* 214

[26] NASTRI M., *op. cit.* 487

Nell'ambito dell'arte e della commercializzazione di opere d'arte, un esempio dell'uso della *blockchain* in questo settore è costituito da *Codex*[27], una *start up* che focalizzando l'attenzione sull'importanza della provenienza dell'opera, permette di trascrivere nella *blockchain* le informazioni rilevanti a riguardo (precedenti proprietari, certificazioni di stimatori ecc.) contribuendo così al mantenimento del valore economico dell'opera stessa in seguito al suo passaggio di proprietà da un soggetto all'altro[28].

Analoga funzione di certificazione di provenienza riguarda l'uso di questa tecnologia del mercato della produzione e commercializzazione dei diamanti, dove *start up* come "*Everledger*"[29] creano identità digitali ad ogni passaggio della creazione del diamante rendendone certa la provenienza e qualità.

Identico discorso nell'ambito dell'agricoltura e delle filiere alimentari, dove è possibile certificare e iscrivere nella *blockchain* ogni fase della filiera produttiva garantendo senza possibilità di manomissione il percorso dalla coltivazione alla tavola, tutto a vantaggio del consumatore. Bisogna, però, prestare attenzione alla circostanza che ciò che garantisce la *blockchain* non è la corrispondenza alla realtà di quanto immesso nel sistema: se venisse registrato un dato errato o non veritiero, esso rimarrà lungo tutta la catena dei blocchi senza possibilità di essere modificato. La *blockchain* pertanto non può, da sola, debellare comportamenti fraudolenti degli operatori nel settore.

Particolarmente interessante è l'uso della *blockchain* nel settore dell'energia[30]. Essa può dar vita a piattaforme dove i "*prosumer*" [31] e i consumatori commerciano la propria energia non utilizzata in eccesso[32]. Le *smart grids*[33] (reti intelligenti)

---

[27] Per ulteriori approfondimenti *https://codexprotocol.com*

[28] EFANOV D., ROSCHIN P. *op. cit.,* 118

[29] Per ulteriori approfondimenti, *https://diamonds.everledger.io*

[30] OECD, *op. cit.,* 83

[31] «*Crasi dei termini producer e consumer che indica un consumatore che è a sua volta un produttore o, nell'atto stesso che consuma, contribuisce alla produzione*». MENDUNI E., *Enciclopedia della scienza e della tecnica*, 2010. Consultabile presso il seguente link: *http://www.treccani.it/enciclopedia/prosumer_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/*

[32] MAUGERI M., *Elementi di criticità nell'equiparazione, da parte dell'AEEGSI, dei* «prosumer» *ai «consumatori» e ai «clienti finali»* in *Nuova giurisprudenza civile commentata*, parte seconda, 2015, 407

[33] ANDONI M., - ROBU V., - FLYNN D., - ABRAM S., - GEACH D., - JENKINS D., - MCCALLUM P., - PEACOCK A., *Blockchain technology in the energy sector: A systematic review of challenges and opportunities* in

distribuiscono l'energia in maniera più efficiente tra gli utenti in modo tale da ridurre gli sprechi, permettendo la compravendita di energia da parte di chi ha impellenti necessità energetiche (impianti industriali *in primis*) da chi possiede energia elettrica in eccesso; ovviamente il tutto registrato e conservato nella *blockchain* che ne garantisce la veridicità e permette di calcolare la quantità di energia acquistata e venduta.

Nell'ambito della Pubblica Amministrazione, la creazione di una identità digitale[34] basata sulla *blockchain* può comportare maggior controllo dell'evasione fiscale e della sicurezza nazionale[35]. Inoltre, può essere utilizzata per facilitare la circolazione dei dati tra le diverse pubbliche amministrazioni e per conferire maggior velocità e sicurezza agli attuali sistemi dei registri pubblici come il catasto, registro delle imprese ecc. Anche nel settore sanitario la *blockchain* potrebbe semplificare e rendere più efficiente lo scambio e la trasmissione dati riguardanti i singoli pazienti[36].

Si è molto discusso in specie fuori dai confini nazionali riguardo la possibilità di implementare un nuovo sistema di voto sfruttando la *blockchain* per permettere agli elettori di verificare i voti e il loro conteggio senza l'intermediazione di un'autorità centrale che garantisca la trasparenza e la correttezza delle procedure. Simili sistemi di voto sono stati utilizzati in Danimarca per le elezioni interne dei partiti politici e sono state anche utilizzate come sistema di voto degli azionisti di società per azioni. Di recente, anche in Italia si discute di implementare la *blockchain* nei sistemi di voto; in particolare alcuni esponenti del Movimento Cinque Stelle hanno dichiarato di volerla utilizzare relativamente alla piattaforma "Rousseau" dove vengono messi al voto degli iscritti alla piattaforma quesiti o proposte di legge[37]. Non è questa la sede più opportuna per trattare della compatibilità costituzionale e degli aspetti positivi o problematici del

---

Renewable and Sustainable Energy Reviews n. 100, 2019, 151

[34] Scettico sul punto, MANENTE M., *op. cit.* 216

[35] EFANOV D., ROSCHIN P., *op. cit.*, 116

[36] NASTRI M., *op. cit.*, 485

[37] Per ulteriori approfondimenti consultare i seguenti link: *https://www.corriere.it/politica/19_marzo_07/rousseau-la-nuova-piattaforma-si-basera-blockchain-8ed89fb2-40d9-11e9-8d4c-9b3b6b114344_preview.shtml?reason=unauthorized&cat=1&cid=FQ3Nr1mh&pids=FR&origin=http%3A%2F%2F*; *www.corriere.it%2Fpolitica%2F19_marzo_07%2Frousseau-la-nuova-piattaforma-si-basera-blockchain-8ed89fb2-40d9-11e9-8d4c-9b3b6b114344.shtml*; *https://cryptonomist.ch/it/2019/03/11/codice-piattaforma-rousseau-blockchain/*

"*Blockchain e-Voting*", ma il tema diventerà sempre più attuale e sarà interessante il dibattito che verrà a formarsi tra chi accoglie con favore il progresso tecnologico e chi "teme" l'utilizzo della tecnologia in questi delicati contesti.

Infine, l'applicazione pratica più versatile della *blockchain* è rappresentata dalla creazione degli "*smart contracts*"[38], i quali sono dei *software* informatici che all'avverarsi di determinate condizioni, eseguono tutto ciò che è stato programmato, con la conseguente registrazione sulla *blockchain*[39]. Essi possono essere sfruttati, ad esempio, in tutti i casi in cui al verificarsi di un evento, un soggetto deve trasferire una somma di danaro (o meglio, di criptovaluta) o altro bene ad una controparte[40]: l'esecuzione automatica del "contratto" rende impossibile l'inadempimento, ma comporta serie problematiche come nel caso di necessità di doverne annullare l'esecuzione (al pari degli effetti dell'azione civile di annullamento o nullità), in quanto la *blockchain* è (relativamente[41]) immodificabile.

Date queste premesse sulle possibili applicazioni della *blockchain*, possiamo affermare, sia pur in linea di prima approssimazione, che la rilevanza delle attività giuridiche che tramite di essa possono essere compiute porterà a criticità di tutto conto.

Infine, bisogna sempre tenere in considerazione che molte delle applicazioni pratiche della *blockchain* si possono risolvere in un c.d. "eccesso di tecnologia", ossia dei casi in cui si utilizza la *blockchain* per assolvere a una funzione che potrebbe essere o che è già assolta efficientemente attraverso una tecnologia meno complessa. Un esempio classico di eccesso di tecnologia è rappresentato dalla *blockchain* utilizzata dalle università per garantire l'esistenza di certificati di laurea[42]. Si è obiettato che la garanzia della certezza e della veridicità di quanto statuito nei certificati emessi dalle università può essere ben ottenuta attraverso un *database* che utilizza la crittografia asimmetrica per "firmare" elettronicamente i documenti.

---

[38] Una delle criptovalute appositamente per concepita per essere utilizzata per l'esecuzione degli *smart contracts* è *Ether*, utilizzata sulla piattaforma *Ethereum* e attualmente è la più utilizzata dopo il *bitcoin*.
[39] CUCCURU P., *op. cit.*, 112
[40] MANENTE M., *op. cit.*, 214
[41] Nei successivi paragrafi verrà meglio chiarito perché la *blockchain* sia solo relativamente immodificabile.
[42] In particolare l'Università di Cagliari è stata la prima in Italia e in Europa ad adottare la *blockchain* per i certificati di laurea emessi. *http://www.ansa.it/sardegna/notizie/2018/07/18/cagliari-certificati-laurea-blockchain_2ac581e3-3427-43e5-ab91-02e649e8df64.html*

Pertanto, è auspicabile l'adozione della tecnologia *blockchain* se e solo se sia realmente necessaria per il raggiungimento di determinati obiettivi e la soddisfazione di specifici interessi.

1.4 Le caratteristiche della *blockchain* e del protocollo *Bitcoin*

La *blockchain*, è un registro distribuito e decentralizzato (*Distributed Ledger Technlology* o *DLT*), caratterizzato dalla trasparenza e dalla (tendenziale)[43] immutabilità[44] e irrepudiabilità, che sfrutta la crittografia asimmetrica per la protezione e l'autenticazione delle transazioni (attraverso chiavi pubbliche e private), le quali sono iscritte e conservate in "blocchi" collegati tra loro cronologicamente.

Essa è un sistema decentralizzato in quanto non vede la partecipazione di alcuna autorità centrale che certifichi e garantisca la veridicità delle transazioni[45]. Pertanto, mentre in un sistema centralizzato la fiducia dei partecipanti è riposta nell'ente centrale che lo gestisce o lo supervisiona, in un sistema decentralizzato e distribuito la fiducia è nell'infrastruttura in sé, composta da tutti i partecipanti della rete[46] (i nodi, organizzati secondo l'architettura della rete *peer to peer* o P2P[47]), secondo il principio del consenso[48] e il meccanismo delle ricompense (*proof of work*). Inoltre, una copia dell'intero *ledger* è conservata a cura di ogni singolo nodo della rete, ed è accessibile da ognuno di essi, rendendo la *blockchain* trasparente e verificabile. Quindi, si differenzia dai comuni *database* centralizzati in quanto i dati non sono conservati in uno (o più) *server*, dove tra i partecipanti alla rete vi è un rapporto *client-server,* ma ogni nodo è in posizione paritaria l'uno con l'altro. Ciò comporta anche una maggiore

---

[43] La *blockchain* non è tecnicamente impossibile da modificare, ma generalmente viene definita immodificabile poiché attacchi idonei a creare blocchi fraudolenti o ad alterare i dati attualmente hanno una probabilità minima di realizzarsi., ANTONOPOULOS M. A., *op. cit.,* 215

[44] Per esprimere questo concetto, nella lingua inglese è solito usare il termine "*unfeasible"*, tradotto con "irrealizzabile, impraticabile" (Cambridge dictionary: *https://dictionary.cambridge.org/it/dizionario/inglese/unfeasible*); l'espressione sta a significare che modificare la *blockchain* è possibile, ma è molto difficile che ciò accada.

[45] CUCCURU P., *op. cit.*, 116

[46] KWONG Y. – KWOK R., *Peer-to-Peer Computing. Applications, Architecture, Protocols and Challenges,* Boca Raton-London-New York, 2012, 27

[47] MANENTE M., *op. cit.*, 215

[48] LI X., - JIANG P., - CHEN T., - LUO X., - WEN Q., *A survey on the security of blockchain systems* in, *Future Generation Computer Systems*, 2017, 3

sicurezza del sistema in quanto l'attacco ad un singolo nodo non comprometterà il funzionamento né l'integrità dei dati.

Un'altra caratteristica della *blockchain* è la «*scarsità digitale*»[49]: essa permette di far assumere valore economico e di scambio a ciò che viene registrato sui registri distribuiti[50]. I comuni documenti informatici, invero, possono essere copiati e duplicati senza particolare difficoltà infinite volte rendendoli indistinguibili l'uno dall'altro; l'uso della crittografia, invece, rende ogni transazione unica e quindi non duplicabile[51], conferendo così "scarsità" e quindi valore a tutto ciò che viene trascritto sulla *blockchain*.

Ciò che però caratterizza la *blockchain* come *species* del *genus distributed ledger technolgy*, è il raggruppamento delle transazioni in "blocchi" concatenati tra loro. Ogni "blocco" è costituito da vari elementi: in particolare, l'*header* (intestazione) contiene tre tipi di metadati; il primo, è costituito dall'*hash*[52] del blocco precedente; il secondo riguarda il *mining*[53] e raggruppa il *difficulty target* (la difficoltà della *proof of work*, richiedendo un certo numero di "0" come prime cifre dell'*output* della funzione SHA256[54]), il *time stamp* (il tempo della creazione del blocco) e il *nonce* (un parametro utilizzato per variare l'output della funzione crittografica SHA256 e soddisfare i requisiti del *difficulty target*). Il terzo, il *merkle tree*[55], altro non è se non un *hash* contenente tutte le transazioni del blocco e che permette di verificare se una transazione è inclusa nel blocco stesso.

---

[49] SARZANA DI S.IPPOLITO F. – NICOTRA M., *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, 18

[50] «*Il concetto di unicità digitale, dal punto di vista informatico, rappresenta una caratteristica di notevolissima rilevanza, che si contrappone all'infinita replicabilità che normalmente connota i contenuti elettronici*.» RINALDI G. *Approcci normativi e qualificazione giuridica delle criptomonete* in *Contratto e impresa* n. 1/2019, 263

[51] AMETRANO F., *Oltre l'oro digitale? Ben poco altro*, reperibile al link: http://nova.ilsole24ore.com/

[52] Per i relativi approfondimenti: *https://it.wikipedia.org/wiki/Funzione_crittografica_di_hash*

[53] V. *Infra* 1.7.2

[54] «*Con il termine SHA (acronimo dell'inglese Secure Hash Algorithm) si indica una famiglia di cinque diverse funzioni crittografiche di hash sviluppate a partire dal 1993 dalla National Security Agency (NSA) e pubblicate dal NIST come standard federale dal governo degli USA (FIPS PUB 180-4). Come ogni algoritmo di hash, l'SHA produce un message digest, o "impronta del messaggio", di lunghezza fissa partendo da un messaggio di lunghezza variabile*». Fonte: *Wikipedia*. Consultabile al *link* seguente: *https://it.wikipedia.org/wiki/Secure_Hash_Algorithm*

[55] "*è una struttura dati usata per indicizzare efficientemente e verificare l'integrità di un grande gruppo di dati*". ANTONOPOULOS M. A., *op. cit.*, 170

La creazione di un nuovo blocco e il suo "incatenarsi" ai blocchi già presenti nella *blockchain* avviene attraverso il *mining*, ossia l'attività dei "*miners*" (estrattori) del risolvere "l'indovinello crittografico" che richiede una notevole quantità di risorse computazionali (e di energia elettrica). La risoluzione dell'algoritmo sarà la prova di aver dedicato ingenti risorse computazionali (la *proof of work*) e gli altri nodi andranno a verificare la correttezza della soluzione. In caso di esito positivo, il blocco "risolto" sarà aggiunto alla *blockchain*, in virtù del principio del consenso basato sulla *proof of work*.

1.5 La *blockchain*, inquadramento giuridico. Una prima definizione nell'Ordinamento italiano

Come verrà evidenziato nel corso dei paragrafi seguenti riguardo le ICO e i *tokens*, è ormai opportuno implementare in nuove norme, o in quelle già in vigore, la tecnologia *blockchain* e in generale le *distributed ledger technolgies* (DLT). Il legislatore nel regolare l'uso di queste nuove tecnologie dovrebbe adottare però un approccio non eccessivamente rigoroso e restrittivo. Un approccio di tal genere non farebbe altro che soffocare e reprimere l'utilizzo, la diffusione e lo sviluppo di una tecnologia che in sé e per sé non è dannosa, ma presenta notevoli applicazioni utili, molte delle quali ancora sconosciute o di cui ancora non si possono apprezzare i reali benefici. Il *bitcoin* stesso viene spesso demonizzato come la valuta utilizzata da organizzazioni criminali per riciclaggio di denaro[56], acquisto di armi e altri beni vietati, ma anche l'Euro e il Dollaro si prestano senza problemi a tali scopi illeciti, sottolineando come non è la tecnologia in sé ad essere criminogena ma è il comportamento delittuoso umano che porta alla commissione di reati facilitati appunto dall'uso della tecnologia.

Internet è un esempio di come una nuova tecnologia ha visto crescere la sua diffusione e le rispettive applicazioni attraverso una efficace regolamentazione del suo uso da parte degli individui, ma senza sopprimerne l'utilizzo attraverso norme

[56] «*la rete di valute virtuali può prestarsi a essere utilizzata per transazioni connesse ad attività criminali, incluso il riciclaggio di denaro; pur essendo le transazioni in valuta virtuale visibili, infatti, i titolari dei portafogli elettronici e, più in generale, le parti coinvolte possono generalmente rimanere anonimi.*», BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto e informatica*, 2017, 46

stringenti e demonizzanti; nonostante gli indiscutibili aspetti strutturali potenzialmente criminogeni di *internet* come transnazionalità, anonimità[57], velocità di esecuzione e la desensibilizzazione del reo, le norme che sono state implementate nei vari ordinamenti giuridici hanno permesso di regolare il comportamento degli individui dell'uso di *internet* offrendo adeguate tutele e protezioni cosi come anche imponendo obblighi e regole cautelative, favorendo conseguentemente l'esponenziale diffusione e utilizzo dello stesso.

Una regolamentazione della *blockchain* necessita di essere implementata negli ordinamenti giuridici[58] alla stessa maniera di come è stato brillantemente fatto nei riguardi di *internet* e delle tecnologie secondarie che man mano sono state sviluppate, auspicabilmente con norme uniformi a livello europeo e ancor di più a livello globale per mitigare il *forum shopping* in giurisdizioni più favorevoli e permissive.

Sorprendentemente, il nostro ordinamento ha fornito una prima definizione di *blockchain*, dedicandone ad un'apposita norma nel disegno di legge "Semplificazioni" convertito in legge con modificazioni dalla legge n. 12 del 11/02/2019.

Si legge nel DDL al comma 1 dell'art. 8-ter rubricato «*Tecnologie basate su registri distribuiti e* smart contract», «*Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili»*.

Seppur encomiabile l'intento di dare una definizione di *blockchain*, l'art. 8-*ter* presenta imprecisioni e criticità di non poco conto. La norma ha un'impronta

[57] Più precisamente, «*Le transazioni* bitcoin *non sono anonime, bensì pseudonime. Tutte le operazioni effettuate all'interno del sistema sono registrate e archiviate nella* blockchain *(ciascuna con una propria marcatura temporale), e restano liberamente consultabili, per un periodo di tempo illimitato, da qualunque soggetto, anche se questi non partecipa alla rete.*», RINALDI G., *op. cit.*, 265

[58] WERBACH, *Trust, But Verify: Why the Blockchain Needs the Law*, in *Berkeley Technology Law Journal*, 2018, 487

eccessivamente definitoria e puntuale, che rischia di lasciar fuori le diverse declinazioni di registri distribuiti attualmente esistenti ma soprattutto quelle che verranno in futuro.

È importante quando si ha a che fare con le nuove tecnologie lasciare ampio margine nelle definizioni in modo tale da prevedere e far rientrare nelle norme anche le diverse e nuove soluzioni tecniche[59]. Inoltre, ad essere precisi, il primo comma delinea non una definizione di *blockchain*, ma una definizione generale di DLT (*distributed ledger technology* o come da rubrica *Tecnologie basate su registri distribuiti)*. La *blockchain* infatti appartiene alla categoria di tecnologie basate su registri distribuiti, ma è caratterizzata dalla peculiarità di conservare i dati in blocchi collegati tra loro; in comune con le DLT vi è solo la caratteristica di essere decentralizzata, ossia non è presente l'architettura *client-server* dove i dati sono conservati solo in un (o più) server, ma sono conservati da ogni nodo della rete strutturata secondo il modello *peer to peer*.

Un'altra questione che suscita perplessità è l'espressione "*architetturalmente decentralizzato su basi crittografiche"*. Si potrebbe creare confusione con l'espressione «*architetturalmente decentralizzato*» in quanto le *blockchain* o comunque le DLT sono caratterizzate dalla circostanza che la totalità dei dati sono presenti in tutti i nodi della rete e non che una porzione del registro è custodita da ciascun nodo. Inoltre, l'uso del termine «*basi crittografiche*» pecca di precisone in quanto la crittografia ha come funzione la tutela dell'integrità dei dati e la loro autenticità, e permette la concatenazione dei blocchi sfruttando la funzione crittografica di *hash*. Pertanto, si sarebbe dovuto far riferimento alla crittografia come strumento di garanzia di integrità in relazione alla concatenazione di blocchi (dove ogni blocco contiene l'*hash* del blocco precedente e cosi via, rendendo palese quando un blocco fraudolento è stato aggiunto alla catena) e la relativa immutabilità degli stessi, non quindi, alla decentralizzazione «*su basi crittografiche*». Nella norma non vi è nemmeno un riferimento al sistema del consenso come regola base per «aggiornare» i dati della

[59] «*La normativa, specie se confrontata con l'inerzia dei precedenti esecutivi sul tema, ha il pregio di porsi all'avanguardia nella regolamentazione della tecnologia blockchain "oltre" gli aspetti prettamente finanziari connessi ai fenomeni delle criptovalute e della tokenizzazione. La formulazione normativa lascia spazio, tuttavia, ad alcuni dubbi interpretativi, che potranno essere in parte risolti in sede di predisposizione delle linee guida che l'AgID dovrà adottare in conformità a quanto indicato nel medesimo Decreto Semplificazioni*.», GALLI M., - GAROTTI L., Blockchain *e* smart contract*: le novità previste dal Decreto semplificazioni* in *Quotidiano Giuridico,* 26-2-2019, 1

blockchain (anche se si fa riferimento alla «convalida» e quindi del meccanismo del consenso dei nodi che convalidano un nuovo blocco dopo aver verificato la *proof of work*) e del *mining*, che permette il funzionamento e la sua continuità del sistema *blockchain*[60]. Di fatto, a voler essere scrupolosi, la norma definisce un *database* distribuito che utilizza la crittografia per la protezione dei propri dati, ma non una *blockchain*. Sembra che il legislatore abbia in mente il funzionamento della *blockchain* ma l'abbia espresso malamente, con imprecisioni e contraddizioni.

Gli elementi che più destano perplessità, infine, sono la "non alterabilità" e "non modificabilità" che seguono la contraddittoria possibilità di "aggiornamento" dei dati. Innanzitutto il termine "aggiornamento" è altrettanto poco chiaro, in quanto si sarebbe dovuto specificare che in una DLT è possibile la "scrittura" di nuovi dati senza la cancellazione dei precedenti nello storico del registro. Inoltre, è ben risaputo che le *blockchain* non sono astrattamente impossibili da modificare ma sono solo nella pratica "impossibili da modificare"; modificare una *blockchain* è possibile, per esempio, mettendo in atto il così detto «*51% attack*»[61] che viene attuato quando dei *miners* in concerto detengono la maggioranza della potenza di calcolo rispetto agli altri *miners* presenti nella rete e aggiungono blocchi fraudolenti sfruttando la loro maggior velocità del creare nuovi blocchi con transazioni false o spendendo due volte le stesse "monete"[62].

Questa tipologia di "attacco" alla *blockchain* seppur possibile, attualmente è nella pratica impossibile riuscire a detenere la maggioranza della potenza computazionale della rete; questo discorso ovviamente vale per le *blockchain* a cui partecipano un cospicuo numero di *miners* e di nodi come *Bitcoin* ed *Ethereum*, ma in caso di *blockchain* con pochi *miners* diventa più semplice e meno oneroso detenere il 51%

---

[60] «*La definizione, infine, non valorizza gli elementi del protocollo del consenso e dell'incentivo economico, cioè a dire gli elementi centrali e innovativi che contraddistinguono la tecnologia* blockchain *(intesa come infrastruttura* public *e* permissionless*) da semplici* database *decentralizzati (DLT). Il rischio è di estendere gli effetti giuridici previsti dalla normativa anche a soluzioni private e* permissioned*, caratterizzate dalla presenza di un "regolatore" centrale e, nella sostanza, non molto diverse da semplici* database.», GALLI M., - GAROTTI L., *op. cit.*, 2

[61] «*Anche le blockchain pubbliche più conosciute,* Bitcoin *ed* Ethereum*, possono essere alterate con il consenso della maggioranza dei nodi e, perciò, esposte ai cosiddetti attacchi del 51%.*», GALLI M., - GAROTTI L., *op. cit.,* 3

[62] LI X., - JIANG P., - CHEN T., - LUO X., - WEN Q., *op. cit.*, 4

della potenza di calcolo della rete. Quindi, definire una *blockchain* come non alterabile e non modificabile è sviante, e può suscitare problemi applicativi di non poco conto.

Infine, ulteriori perplessità si hanno al terzo e quarto comma di seguito riportati «*3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.*"», «"*4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3*».

Può essere dubbia la scelta di affidare ad una fonte di rango secondario (le linee guida dell'Agenzia italiana per il digitale) la definizione dei requisiti tecnici necessari a far scaturire effetti giuridici dalla validazione temporale dei dati iscritti nella *blockchain*; ma senza dubbio è da accogliere con favore la scelta di dare effetti e validità giuridica alla *blockchain* nell'ambito della validazione temporale elettronica[63]. In conclusione, lodevole è aver tentato di definire e di riconoscere giuridicamente le DLT ma sicuramente è necessario limare le norme appena emanate per evitare problemi applicativi e contraddizioni.

Le linee guida dell'ESMA, oggetto di analisi dei paragrafi seguenti, delineano nella parte dedicata al glossario due distinte definizioni di *blockchain* e di DLT; nella definizione di *blockchain* viene posta l'enfasi sulla concatenazione in blocchi e sull'appartenenza al *genus* di DLT. Mentre, le DLT vengono definite come un registro distribuito dove la totalità dei dati è conservata in più luoghi e utilizza la crittografia a chiave asimmetrica. Possiamo notare come a livello europeo sia stata espressa meglio e con più precisione e attenzione ai dettagli il rapporto tra *blockchain* e DTL e le loro effettive caratteristiche. Inoltre, vengono anche dedicate apposite definizioni dei *miners* ed anche dei tipi di meccanismo di consenso (*proof of work* e *proof of stake*),

[63] «*La questione presenta importanti risvolti, soprattutto sotto il profilo della* data protection*: è noto, infatti, che la memorizzazione in* blockchain *di documenti informatici contenenti dati personali può presentare problematiche sotto diversi profili – tra le quali, ad esempio, l'esercizio da parte dell'interessato del diritto di rettifica e cancellazione, la determinazione di un periodo certo di data* retention *e i trasferimenti di dati personali extra-UE.*», GALLI M., - GAROTTI L., *op. cit.*, 3

non tralasciando così nulla del funzionamento delle *blockchain* senza una apposita e chiara definizione.

L'art 8-ter del DDL semplificazioni però, non fornisce solamente una definizione di DTL, ma si occupa anche di *smart contracts*[64] al secondo comma: «*Si definisce "smart contract" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto*». Innanzitutto manca un coordinamento con la disciplina dei contratti regolata dal codice civile, creando non poche incertezze sulla disciplina dei "contratti" basati sugli *smart contracts*[65]. Infatti, sarebbero da approfondire le questioni che potrebbero sorgere in virtù dell'esecuzione automatica del contratto come, ad esempio, rescissione e risoluzione, annullamento o nullità con effetti *ex tunc*: essendo ciò che è incorporato in una *blockchain* "immodificabile", è difficile da un punto di vista tecnico risolvere problematiche in linea con gli istituti giuridici esistenti; la responsabilità, poi, civile o penale del soggetto che programma il *software* costituisce un altro interessante tema che necessariamente dovrà essere affrontato dal legislatore o dalla giurisprudenza. Inoltre, riguardo la «identificazione informatica» di cui parla il secondo comma, è da sottolineare come le *blockchain* utilizzano il sistema di crittografia asimmetrica per garantire la provenienza delle transazioni, la quale è la stessa tecnologia alla base delle firme elettroniche, già aventi valore legale[66]. Infine, la

---

[64] CUCCURU P., *op. cit.*, 114 «*Il concetto di smart contract è stato introdotto per la prima volta a metà degli anni novanta da Nick Szabo. Tuttavia, il loro sviluppo è rimasto teorico fino allo sviluppo della tecnologia blockchain.*» Per approfondimenti, consultare SZABO, *Formalizing and Securing Relationships on Public Networks,* in *First Monday,* Vol. 2, n. 9, 1997, in http://journals.uic.edu/ojs/index.php/fm/article/view/548/469.

[65] Inoltre, «*La definizione presenta elementi di potenziale criticità, specie laddove indica che è la "esecuzione" dello* smart contract *a vincolare le parti. È noto che l'efficacia vincolante di un contratto discende dall'accordo delle parti (art. 1326 c.c.) e non dal momento (successivo e potenzialmente inesistente) connesso alla sua esecuzione: e ciò sia che si intenda il concetto "esecuzione" in senso giuridico, come esecuzione della prestazione oggetto del contratto, sia in senso informatico, come atto di eseguire il programma in sé.*»., GALLI M., - GAROTTI L., *Op. cit.,* 3

[66] «smart contract *già costituisce un documento informatico come definito nel Codice dell'Amministrazione Digitale ("documento elettronico che contiene la rappresentazione informatica di*

norma manca di specificare a cosa vincola l'esecuzione del codice dello *smart contracts*; in caso di vincolo a corrispondere valore, lo *smart contract* può soltanto trasferire la titolarità di un *token* o di criptovaluta sulla *blockchain*, pertanto sarebbe anche da riconoscere la validità giuridica di tali strumenti di pagamento o di rappresentazione di valore su cui si basa il funzionamento degli *smart contracts*.

Quindi, anche la definizione di *smart contracts* e dei suoi effetti è approssimativa, migliorabile e da coordinare con altri istituti giuridici che sono interessati dall'uso da parte dei consociati di questi nuovi strumenti tecnologici.

1.6 Le tipologie di *blockchain*

Nonostante il paradigma più conosciuto di *blockchain* sia quello alla base del funzionamento del *bitcoin*, vi sono altre tipologie di *blockchain*: *blockchain* pubbliche (*permissionless ledger*), *blockchain* private (*permissioned ledger*), e infine un modello di *blockchain* che comprende parte delle prime due tipologie, le *blockchain* ibride[67].

Nella *blockchain permissionless*, tutti i partecipanti alla rete hanno libertà di accedervi, dispongono una copia dell'intera cronologia del *ledger*, e possono liberamente iscrivere nuove transazioni (oltre a poter contribuire alla formazione dei nuovi blocchi col protocollo del consenso). L'esempio più diffuso di questa tipologia è la *blockchain* del protocollo *Bitcoin*, ideata col fine di far a meno di un ente centrale gerarchicamente superiore ai partecipanti alla rete che possa censurare o determinare quale transazione sarà aggiunta nei blocchi. Una volta soddisfatto il principio del consenso (*proof of work*) la transazione è considerata valida per tutti i nodi della rete e sarà aggiunta in un blocco a sua volta "incatenato" ai blocchi già creati e validati.

Le *blockchain permissioned*, invece, sono caratterizzate dalla partecipazione al *network* solo da parte di alcuni soggetti preventivamente determinati o autorizzati. Il

---

atti, fatti o dati giuridicamente rilevanti") che, ai sensi dell'art. 20, comma 1-bis CAD, "soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del codice civile quando (...) è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore".», GALLI M., - GAROTTI L., *op. cit.*, 3

[67] SARZANA DI S.IPPOLITO F. – NICOTRA M, *op. cit.*, 22

contenuto della *blockchain* non è accessibile a tutti, e solo alcuni soggetti possono iscrivere e validare le transazioni.

Volendo approfondire gli elementi delle *permissioned blockchain*, sono quattro gli elementi che le caratterizzano[68]: infrastruttura, ecosistema, applicazioni, e *governance*. Riguardo il primo elemento, essendo la fiducia degli utenti riposta nei partecipanti al *network*, le reti di questo tipo di *blockchain* devono essere a sua volta private, la cui garanzia di sicurezza è sotto la responsabilità dei partecipanti alla rete. Ciò fa in modo che in caso di falle nella sicurezza e di intrusione di soggetti estranei, verrebbe meno la fiducia nel sistema. L'elemento dell'ecosistema invece riguarda i partecipanti al *network*, i quali devono condividere gli stessi valori e regole, poiché la fiducia del sistema si basa sugli stessi partecipanti, e che essi opereranno in buonafede e nel rispetto delle regole condivise dal *network* per il raggiungimento degli obiettivi comuni. Le applicazioni, invece, devono essere realizzate in linea con la *governance* delineata dai partecipanti al *network*, pertanto ciò comporta che gli sviluppatori collaborino a stretto contatto con gli attori della rete. Infine, la *governance* riguarda il complesso di regole predisposte dai partecipanti, comprendenti anche i requisiti di partecipazione, forgiate con l'obiettivo di garantire la sicurezza del *network* e il raggiungimento degli obiettivi comuni.

Infine, al modello ibrido vanno ricondotte quelle *blockchain* dove il controllo, diversamente che dalle private, è distribuito e non centralizzato. Infatti, singoli nodi selezionati (*contributors*) determinano quali transazioni possono essere iscritte nei blocchi, ma l'elenco delle transazioni può essere a seconda dei casi aperto al pubblico o limitato ai partecipanti. Applicazioni pratiche di questa tipologia di *blockchain* sono in quei casi in cui si vuole riservare a pochi soggetti qualificati la possibilità di registrare le transazioni, ma di rendere accessibile a tutti la lettura del registro.

Diverse sono quindi le declinazioni della *blockchain*, ognuna più consona alla funzione che si vuole essere assolta da questa nuova tecnologia.

1.7 La crittografia nella *blockchain*. Chiavi pubbliche e private

[68] SARZANA DI S.IPPOLITO F. – NICOTRA M, *op. cit.*, 23 ; per ulteriori approfondimenti consultare il seguente link:s*https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/*

Le *blockchain* utilizzano la crittografia per garantire l'identità del mittente di una transazione, cosi come l'autenticità e l'integrità delle stesse. Questo metodo di scrittura e cifrazione di messaggi in realtà ha origini risalenti a più di 2000 anni fa; lo stesso Giulio Cesare era solito comunicare cifrando i propri messaggi sostituendone le lettere con altre, disposte a distanza di un determinato numero di posizioni dell'alfabeto[69]. Ma questo tipo di crittografia garantisce essenzialmente solo la riservatezza del messaggio cifrato. La tipologia di crittografia utilizzata nella *blockchain* è asimmetrica, in quando il mittente genera due chiavi, una pubblica e una privata[70]. La crittografia simmetrica, invece, è caratterizzata dal fatto gli interlocutori della transazione si scambino le rispettive chiavi; ma ciò comporta che un eventuale soggetto che intercetti la comunicazione abbia la possibilità di avere conoscenza delle chiavi e quindi del contenuto del messaggio. Ciò non accade nella crittografia asimmetrica, dove se un soggetto terzo intercettasse la comunicazione avrebbe conoscenza della chiave pubblica del mittente ma non potrebbe prendere visione del messaggio poiché necessita la chiave privata[71] del destinatario per decifrarlo.

Scendendo nel dettaglio del suo funzionamento, il mittente cifra il messaggio con la propria chiave pubblica del destinatario e invia il messaggio cifrato. Il destinatario, utilizzando la sua chiave privata, decifra il messaggio criptato e solo lui potrà avere contezza del contenuto del messaggio cifrato.

Il protocollo *Bitcoin* utilizza il sistema utilizzato della firma digitale per garantire la paternità e la genuinità delle transazioni[72]. La firma digitale nel *Bitcoin* si basa sul funzionamento della crittografia asimmetrica, ma prevede che la crittografia non si applichi all'intero testo in chiaro ma alla sua "impronta", utilizzando una funzione *hash*[73]. Il mittente "firma" con la propria chiave privata il messaggio di cui verrà

---

[69] SARTOR, G., *op. cit.*, 190

[70] CUCCURU P., *op. cit.*, 110

[71] Nei protocolli delle criptovalute, fondamentale è la corretta e sicura conservazione della *private-key,* la cui perdita o furto comporta conseguenze irrimediabili. Infatti, «*Although blockchains preserve anonymity and privacy, the security of assets depends on safeguarding the private key, a form of digital identity. If ones private key is acquired or stolen, no third party can recover it*», EFANOV D., ROSCHIN P., *op. cit.,* 119

[72] FRANCO, P. *Understanding Bitcoin: Cryptography, Engineering and Economics,* Hoboken, 2014, 56

[73] Una funzione "irreversibile" che «*accetta come input una stringa di bit (o byte) di lunghezza arbitraria e produce un risultato di dimensione fissa*» Ferguson-Schneier-Kohno, 2011, 71. Per approfondimenti, https://medium.com/@AndreaFerraresso/la-crittografia-dietro-a-bitcoin-72cc6ad3fa41

successivamente verificata la paternità attraverso la chiave pubblica del mittente. I *digital wallet*[74] (portafogli digitali) custodiscono le coppie di chiavi, e per ogni transazione verrà generata da una chiave privata (in genere scelta casualmente) attraverso una funzione crittografica, la chiave pubblica. Da essa, attraverso una funzione di *hash* verrà generato l'*address*, ossia l'indirizzo del mittente/destinatario (come l'IBAN bancario).

Questi quindi sono i principi che sono alla base del funzionamento del *bitcoin* e delle *blockchain* in generale, che permettono l'efficace esecuzione delle transazioni garantendo la loro riservatezza e autenticità.

1.7.1 (*Segue*) I principi teorici del funzionamento di *Bitcoin*: il principio del consenso e la teoria dei giochi

Essendo la *blockchain* e il protocollo *Bitcoin* caratterizzati da un sistema decentralizzato, non è presente un ente centrale che certifichi e garantisca la veridicità e la coerenza delle transazioni. Perciò, la *blockchain* utilizza un sistema di consenso distribuito basato sulla "fiducia" reciproca dei partecipanti alla rete[75], in modo tale da risolvere problematiche comuni ai sistemi di pagamento decentralizzati quali la questione della doppia spesa e la cosiddetta "Problematica dei generali bizantini"[76].

Inoltre, l'applicazione della teoria dei giochi al funzionamento della *blockchain* di *Bitcoin* permette di incentivare gli utenti a mettere a disposizione le proprie risorse per

---

[74] Le criptovalute «*non sono fisicamente detenute dall'utente ma sono movimentate attraverso un conto personalizzato noto come "portafoglio elettronico" (c.d.* e-wallet*), che si può salvare sul proprio computer o su uno* smartphone*, o che può essere consultato via* internet*, al quale si accede grazie ad una* password*. Questi portafogli elettronici sono generalmente* software*, sviluppati e forniti da appositi soggetti (c.d.* wallet providers*)*» BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto e informatica*, 2017, 29

[75] CUCCURU P., *op. cit.*, 118

[76] Problema informatico riguardante il raggiungimento del consenso in contesti dove vi possono essere errori o informazioni in contraddizione tra i partecipanti alla rete *peer to peer*. «*"A reliable computer system must be able to cope with the failure of one or more of its components. A failed component may exhibit a type of behavior that is often overlooked--namely, sending conflicting information to different parts of the system. The problem of coping with this type of failure is expressed abstractly as the Byzantine Generals Problem."*», LAMPORT L., - SHOSTAK R., PEASE SRI M., *International Byzantine Generals Problems*, *ACM Transactions on Programming Languages and Systems*, Vol. 4, No. 3, July 1982, 2

il corretto ed efficace funzionamento del sistema, contribuendo alla sua preservazione, continuità e sviluppo[77].

Partendo dall'analisi del principio del consenso distribuito[78], esso è di fondamentale importanza poiché è solo grazie al suddetto principio che la *blockchain* riesce a garantire la sua trasparenza di funzionamento[79]. Infatti, non essendoci una autorità centrale in cui gli utenti ripongono la propria fiducia (come banche, enti statali ecc.), è necessario che gli utenti facciano affidamento reciproco gli uni con gli altri[80]. Così, il meccanismo del consenso basato sulla *proof of work* previene condotte fraudolente che si possono esplicare in una duplice "spesa" degli stessi *bitcoin* o in un accordo tra più utenti per frodare il sistema.

Quest'ultimo, il "Problema dei generali bizantini"[81], teorizzato nel 1982 da Shostak, viene presentato dallo stesso autore mediante un esempio pratico: ci sono dei generali bizantini che, dopo aver circondato una città, devono deliberare quando attaccare o ritirarsi agendo necessariamente all'unisono; se ci sono generali "traditori", essi comprometteranno l'azione coordinata comportando la sconfitta dei bizantini. La soluzione al problema permette di trovare un accordo anche in presenza di informazioni discordanti (attaccare o ritirarsi) da parte dei generali fraudolenti. Con questa metafora vengono essenzialmente descritte le problematiche che possono sorgere in contesti di rete *peer to peer*, dove ci sono più nodi che scambiano informazioni tra di loro ed è possibile che alcuni nodi tentino di registrare transazioni mai avvenute o false come nel caso dei generali bizantini che compromettono l'assedio con la diffusione di ordini falsati in modo tale inficiare la simultaneità dell'attacco. Nel protocollo *Bitcoin* per

---

[77] Il *Bitcoin* «*si basa su un sistema di incentivazione economica che induce i partecipanti a rispettare le regole di funzionamento del protocollo, rendendo tendenzialmente svantaggiose le condotte disoneste*», RINALDI G., *op. cit.,* 264

[78] GRAMOLI V., *From blockchain consensus back to Byzantine consensus*, in *Future Generation Computer* Systems, 2017, 1

[79] *«il pregio maggiore del sistema bitcoin è forse quello di permettere a individui estranei tra loro di confidare nella sicurezza delle transazioni immesse nella* blockchain*, senza dover riporre fiducia in soggetti intermediari, enti certificatori, oppure nel potere deterrente o coercitivo dell'ordinamento giuridico»*, RINALDI G., *op. cit.* 263

[80] «*La correttezza del meccanismo, a questo punto, si basa su una scommessa e cioè sul fatto che a* miners *e* players *conviene che sia tutto sempre "*perfetto e inattaccabile perché è il loro lavoro e la loro fonte di guadagni sempre più lauti*". La correttezza di* Bitcoin *è quella che auspicano tutti gli attori della rete di pagamento*», BOCCHINI R., *op. cit.* 39

[81] LAMPORT L., - SHOSTAK R., PEASE SRI M., *op. cit.,* 4

garantire che un *miner* non aggiunga blocchi fraudolenti, viene utilizzata la *proof of work*: ogni nodo della rete così saprà che il "blocco" valido sarà solo il blocco aggiunto dal *miner* che ha impiegato una notevole quantità di energia computazionale per risolvere l'indovinello crittografico[82]. In questo modo, tutti gli altri nodi che verificheranno la risoluzione della *proof of work*, valideranno il blocco e tutte le transazioni presenti in esso in virtù del principio del consenso distribuito.

La *blockchain* risolve inoltre la problematica del *double spending*[83], ossia spendere per due volte le stesse "monete", inoltrando più volte lo stesso pagamento a destinatari differenti[84]. Nel sistema bancario sono proprio gli istituti di credito che garantiscono il non verificarsi della doppia spesa. Ma nell'ambito della virtualizzazione della moneta e in assenza di un ente centrale garante, la crittografia permette di "identificare ogni moneta" in modo tale che tutti i nodi sapranno che determinati *bitcoin* sono stati inviati ad un determinato indirizzo e che successivamente non potranno essere inviati ad un altro soggetto[85]. Quando vengono ricevuti dei *bitcoin*, non è possibile spenderli immediatamente, perché è necessario attendere almeno sei[86] conferme da parte di altrettanti nodi. Le conferme[87] si sostanziano nei blocchi successivi aggiunti in successione a quello in cui la transazione da validare è stata iscritta; quindi dopo circa

---

[82] GRAMOLI V., *op. cit.*, 2

[83] CUCCURU P., *op. cit.*, 119

[84] LI X., - JIANG P., - CHEN T., - LUO X., - WEN Q, *op. cit.,* 5

[85] La *blockchain* risolve ma non elimina il problema, che può fisiologicamente presentarsi. Infatti, il *double spending* «*is a well-known security concern named double-spending attack. Double-spending occurs when someone makes more than one payment using one body of funds (e.g., a quantity of bitcoins). This is possible in a peer-to-peer network because there may be propagation delays when pending payments are broadcast to the network or the networks many nodes receive unconfirmed transactions at different times. Blockchain tackles this problem by requiring miner nodes to solve a complex mathematical problem (mining) in order to verify the transaction*», EFANOV D., ROSCHIN P., *op. cit.,* 118

[86] È possibile determinare a proprio piacimento il numero di conferme necessarie per considerare la transazione come validata definitivamente, ma in genere si ritiene che il numero ideale sia sei, in quanto attualmente è estremamente difficile riuscire a iscrivere più di sei blocchi fraudolenti nella *blockchain*.

[87] *«Ciascuna transazione viene convalidata dalla generazione di 6 blocchi di conferma, sottoposti a verifica dai* peer *che compongono la rete, con un'operazione che può richiedere fino a un massimo di 50 minuti di tempo; la verifica avviene tramite l'applicazione dell'algoritmo di* hash*, funzione non reversibile che genera una stringa alfanumerica, detta* digest*, che varia al variare degli elementi del file. Ogni operazione sui* Bitcoin *viene convalidata dall'applicazione di una marca temporale, una procedura informatica che consente di associare data e ora certa al file, al fine di verificare che le attività si siano svolte secondo l'ordine temporale dichiarato, evitando che il cedente possa procedere a una nuova transazione con unità che ha già trasferito in precedenza*», BOCCHINI R., *op. cit.,* 39

sei blocchi incatenati la transazione può considerarsi valida e inserita stabilmente nella *blockchain* in quanto una sua modifica diviene altamente improbabile.

Può accadere che in uno stretto intervallo di tempo vengano aggiunti due blocchi alla catena, entrambi contenenti le stesse transazioni o soltanto alcune di esse dando origine ad un c.d. *fork* (una biforcazione della catena di blocchi). La soluzione a questo "inconveniente" è assicurata dal principio secondo cui la fiducia degli utenti è riposta nella catena "più lunga" ossia la catena di blocchi per cui è stata spesa più energia (*proof of work*). In tal modo, i *miner* andranno ad aggiungere i nuovi blocchi al ramo della catena più lungo, e le transazioni contenute nel blocco c.d. "orfano", verranno messe in coda per essere aggiunte ai successivi blocchi appartenenti alla catena più lunga.

L'altro aspetto innovativo della *blockchain* del protocollo *Bitcoin* è il sistema di incentivi che garantisce la continuità di funzionamento dell'intero sistema. Infatti, la *blockchain* oltre a utilizzare tecnologie già esistenti e a risolvere il problema dei generali bizantini e di doppia spesa, sfrutta la teoria dei giochi[88], modello matematico per lo studio delle "situazioni competitive".

Basandosi su di essa, Satoshi Nakamoto ha ideato un sistema secondo cui ogni nodo che partecipa alla rete, attraverso l'uso delle proprie risorse computazionali (energia elettrica), riceve un determinato ammontare di *bitcoin* come ricompensa oltre all'ammontare delle commissioni. Questo sistema è stato introdotto in quanto nel protocollo *bitcoin* non c'è un ente centrale che stampa e distribuisce la valuta. Perciò i nodi che dedicano le proprie risorse al *mining*, sono coloro che "coniano" i *bitcoin* e mettono in circolo la nuova moneta "estratta". Il sistema così incardinato, garantisce il successo del sistema *Bitcoin* in quanto gli utenti sono incentivati ad agire secondo le regole e non contro di esse, in quanto l'agire disonesto non comporta a vantaggi tali da preferirlo a condotte oneste. Infine, l'auspicio di Nakamoto è che quando verranno

[88] Modello matematico per lo studio delle situazioni competitive, in cui cioè sono presenti più persone (o gruppi di persone, o organizzazioni) dette appunto 'giocatori', con autonoma capacità di decisione e con interessi contrastanti. LUCCHETTI R., voce *Giochi (teoria dei)* in *Enciclopedia della Scienza e della Tecnica*. http://www.treccani.it/enciclopedia/teoria-dei-giochi_(Enciclopedia-della-Scienza-e-della-Tecnica)/

immessi nella rete il numero totale di *bitcoin* (21 milioni[89]) l'incentivo sarà costituito esclusivamente dalle commissioni. In questo modo, un *miner* disonesto deve scegliere tra la possibilità di effettuare transazioni inesistenti o partecipare a formare i nuovi blocchi onestamente, guadagnando con i costi di transazione: in questo modo, l'agire onesto sarà notevolmente più profittevole dell'agire disonestamente.

1.7.2 (*Segue*) Il *mining* e la *proof of work*

Come già accennato nel corso dei precedenti paragrafi, il *mining*[90] è l'attività dei di determinati soggetti che contribuiscono a sostenere il funzionamento del sistema *Bitcoin*. Essenzialmente, essi altro non fanno che permettere l'aggiunta di nuovi "blocchi" alla catena, e come ricompensa per le risorse prestate, ottengono *bitcoin*.

Riprendendo la struttura dei blocchi esposta nei precedenti paragrafi, la parte riguardante il *mining* contiene *il difficulty target* (la difficoltà della *proof of work*, richiedendo un certo numero di "0" come prime cifre dell'*output* della funzione SHA256), il *time stamp* (il tempo della creazione del blocco) e il *nonce* (un parametro utilizzato per variare l'*output* della funzione crittografica SHA256 e soddisfare i requisiti del *difficulty target*).

La creazione di un nuovo blocco e il suo "incatenarsi" ai blocchi già presenti nella *blockchain* avviene in base al principio del consenso distribuito, *la proof of work*. Essa quindi non è altro che la prova di aver speso una notevole quantità di energia computazionale per trovare il *nounce*, e quindi tutti gli altri nodi riterranno valido il blocco del *miner* che ha speso energia e risolto l'indovinello crittografico in quanto tutti potranno facilmente verificare la risoluzione dello stesso.

La difficoltà dell'indovinello (il numero di zeri iniziali dell'*output* della funzione SHA256) è calibrata dal sistema in base alla quantità di energia computazionale fornita dall'intero sistema[91]: più sono i *miners*, più sarà sicura la *blockchain* (in quanto sarà

[89] Si stima che l'ultimo bitcoin verrà "minato" nel 2140, in quanto ogni 4 anni viene dimezzato il premio dei *miner*. Attualmente è di 12.5 bitcoin ma successivamente andrà riducendosi progressivamente., ANTONOPOULOS A., *op. cit.,* 2

[90] Si utilizza il verbo "to mine" in quanto viene paragonato il *bitcoin* all'oro; esso viene estratto dalle miniere investendo energie cosi come fanno i *miners*, ANTONOPOULOS M. A., *op. cit.,* 177

[91] LI X., - JIANG P., - CHEN T., - LUO X., - WEN Q, *op. cit.,* 2

sempre più difficile creare ramificazioni fraudolente) e più sarà difficile "minare" un blocco: questo comporta un sistema che al diminuire dei soggetti disposti ad investire risorse, diminuirà anche la difficolta del *mining*, incentivando altri soggetti a tentare di risolvere l'indovinello[92]. Inoltre, la variazione della difficoltà è calibrata in modo tale che ogni blocco venga minato circa ogni 10 minuti, aumentando e diminuendone la difficoltà in base alla velocità con cui vengono "minati" i nuovi blocchi.

Il *mining* è ciò che rende peculiare il protocollo *bitcoin*, ossia un meccanismo di sicurezza decentralizzato quale base per una valuta virtuale *peer to peer*.

Il numero finito e la prestabilita diminuzione di emissione di valuta che caratterizza i *bitcoin* garantiscono, poi, l'impossibilita di fenomeni inflattivi come può invece accadere con i sistemi di moneta fiat dove le banche centrali possono stampare, volendo, illimitata moneta. Però, la prestabilita limitazione[93] del numero di *bitcoin* che vengono "coniati"[94] con il *mining* comporta una progressiva deflazione[95], ossia aumento del potere di acquisto dei *bitcoin*, potendo causare l'effetto di accrescere l'accumulo di moneta piuttosto che spenderla per acquisire beni o servizi[96]. Ciò potrebbe portare ad un uso sempre più limitato dei *bitcoin* e inficiare la sua funzione di riserva di valore specialmente in relazione alla volatilità del prezzo degli stessi.

Ulteriore aspetto da considerare riguardo il *mining*, è la sostenibilità ambientale dei *bitcoin*[97]. L'energia elettrica utilizzata per alimentare le macchine adibite al *mining* di tutto il mondo, ha raggiunto circa 70Twh, più del consumo di Repubblica Ceca,

---

[92] «*il crescere della potenza elaborativa complessivamente spesa nel network e il conseguente incremento della difficoltà dei calcoli richiesti per aggiungere nuovi blocchi, rende, parallelamente, sempre più sicuro il sistema, aumentandone nel contempo l'attrattività per investitori e pubblico, in quello che può essere definito un circolo virtuoso*», RINALDI G., *op. cit.*, 264

[93] «*[…] simula, in un certo modo, il progressivo esaurimento (o per meglio dire il costante aumento della difficoltà estrattiva) dell'oro, conferendo a bitcoin una natura intrinsecamente deflattiva.*», RINALDI G., *op. cit.*, 265

[94] Il verbo "*to mine*" afferendo all'estrazione di metalli preziosi, si focalizza più sulla ricompensa che al suo scopo primario, ossia quello di garantire la sicurezza del sistema *Bitcoin* e di contribuire alla formazione di un consenso distribuito su tutto il *network* senza un autorità centrale[94], ANTONOPOULOS A., *op. cit.* 178

[95] «*il delicato equilibrio tra pesi e contrappesi si completa con alcuni elementi a cavallo tra scienza computazionale e politica monetaria: l'offerta complessiva di* bitcoin *è predeterminata ab origine, risultando, dunque, totalmente inelastica rispetto alla domanda*» RINALDI G., *op. cit.*, 264

[96] LEMME G.- PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin* in *Rivista di diritto bancario*, n. 11/2016, 19

[97] OECD, *op. cit.,* 111

Svizzera o Colombia[98]. Poiché la corrente elettrica utilizzata è in prevalenza derivante da fonti di energia non rinnovabili[99] ed inquinanti, l'attività di *mining* contribuisce all'inquinamento che già affligge il nostro pianeta[100]. Sarebbe auspicabile quindi, trovare metodi di funzionamento alternativi alla *proof of work* che siano soprattutto più sostenibili in termini di energia utilizzata per far funzionare la *blockchain*, come ad esempio la *proof of stake*.

1.7.3 (*Segue*) La *proof of stake* e altre soluzioni tecniche per il sistema del consenso

La *proof of work* non è l'unico metodo esistente nel panorama delle *blockchain* per garantire le soluzioni ai problemi di affidabilità e sicurezza. Sono state concepite tipologie di sistemi alternativi che assolvono la stessa funzione, soprattutto in virtù della insostenibilità energetica della *proof of work*.

Una di esse è la "*proof of stake*": a differenza della *proof of work*, dove il *miner* che aggiunge il blocco è colui che ha risolto l'indovinello matematico con l'impiego di risorse computazionali ingenti, con la *proof of stake* il nodo che va ad aggiungere un blocco viene scelto in base alla quantità di criptovaluta che possiede, considerando anche (a seconda dei casi) da quanto tempo le detiene[101]. L'ammontare posseduto viene "scommesso" (*put at stake*), e nel caso di azioni fraudolenti, il *miner* perderà ciò che ha messo "*at stake*'', come se fosse un deposito cauzionale. In questo modo, esso sarà incentivato ad agire onestamente per non perdere la somma depositata, che sarà maggiore dei ricavi dell'agire disonestamente. I *miners* dei sistemi che adottano la *PoS* potrebbero essere considerati più dei "*minters*'' (coniatori), piuttosto che "estrattori" di moneta, in quanto non necessitano un impego di risorse ingente ma semplicemente coniano nuova "moneta".

---

[98] Circa il 0,21% dell'consumo totale del pianeta, fonte: *https://digiconomist.net/bitcoin-energy-consumption*

[99] SWAN M., *Blockchain: Blueprint for a New Economy*, Sebastopol, Stati Uniti, 2015, 83

[100] Critico sul punto, Massimo Sala, docente dell'Università di Trento, Direttore del Laboratorio di Crittografia, in un'intervista apparsa su Nòva, Lex 24, reperibile al seguente link: http://goo.gl/PP76Nq

[101] SARZANA DI S.IPPOLITO F. – NICOTRA M., *op. cit.,* 26

Altre declinazioni della *PoS* sono sistemi in cui il nodo che andrà a validare la transazione è eletto in base ad un meccanismo di voto da parte dei possessori di criptovaluta (*Delegated proof of stake*)[102].

Seppur più sostenibile dal punto di vista ambientale, anche la *PoS* ha profili critici[103].

Uno di questi è il fisiologico risultato secondo cui, essendo coloro che possiedono già un cospicuo ammontare di moneta i soggetti che "conieranno" nuova valuta, si arricchiranno proporzionalmente a quanto già posseggono. Tale circostanza è alla base di un secondo rilievo critico, ossia la tendenziale e progressiva centralizzazione del sistema, in virtù di soggetti che avendo sempre più risorse da mettere "*at stake*" potranno di fatto avere controllo della rete, a discapito di un sistema decentralizzato e distribuito *peer to peer* basato sulla completa parità dei soggetti partecipanti alla rete.

Bisogna comunque considerare che a seconda della tipologia di *blockchain* considerata e degli utenti che vi partecipano, corrisponde una più o meno idonea tipologia di sistema di consenso.

Nel caso delle *blockchain* pubbliche, dove i nodi non hanno conoscenza dell'affidabilità degli altri, il sistema della *proof of work* è il più efficace per costruire la fiducia della rete cosi come garantire la sicurezza di attacchi esterni, dato che chiunque può accedervi liberamente.

---

[102] «*DPoS utilises distributed voting to elect delegates and witnesses that participate in the validation process. Every member votes to elect a number of witnesses to generate a block. Each witness is assigned a xed schedule, e.g. every 2 s, to produce a block. The system relies on reputation and dishonest witnesses can be voted out of the system. This deterministic selection of block producers allows very fast con rmation times [69]. Similarly to witnesses, stakeholders elect delegates who are responsible for decisions on protocol rules and system parameters, such as transaction fees, block size, transactions per block etc. The algorithm is described as a shareholder voting consensus scheme, because every single member of the network can decide who can be trusted and va- lidation power is not concentrated to the members with most resources [56], unlike PoS.*» ANDONI M., - ROBU V., - FLYNN D., - ABRAM S., - GEACH D., - JENKINS D., - MCCALLUM P., - PEACOCK A., *Blockchain technology in the energy sector: A systematic review of challenges and opportunities* in *Renewable and Sustainable Energy Reviews*, n. 100, 2019, 150

[103] «*The main vulnerability of PoS systems is known as the 'nothing at stake' problem or in other words that voting/claiming nancial rewards for multiple chains is inexpensive. Several solutions have been proposed such as integrating a punishment mechanism for validators that simultaneously create blocks in multiple chains and automatically deducting coins owned or de- posited.*», ANDONI M., - ROBU V., - FLYNN D., - ABRAM S., - GEACH D., - JENKINS D., - MCCALLUM P., - PEACOCK A, *op. cit.,* 150

Nelle *blockchain* private o ibride, dove i nodi sono fidati o costituti da soggetti autorevoli, un sistema come la *proof of work* può rivelarsi eccessivo, dovendo preferire un modello meno dispendioso come la *proof of stake* o la *proof of autority*[104] o *proof of existence*. La seconda si basa sull'identità del nodo, dando il potere di validare le transazioni solo a determinati soggetti; essa si presta ad utilizzi nell'ambito della Pubblica Amministrazione; l'ultima basa la facoltà di validare le transazioni in base al possesso da parte del nodo di specifici documenti o autorizzazioni.

In conclusione, a seconda dell'uso e dagli obiettivi di una determinata *blockchain* è auspicabile utilizzare un sistema di consenso appropriato, e col tempo verranno certamente implementati e migliorati i metodi di convalida in virtù del progresso tecnologico e alle *blockchain* che verranno concepite *ad hoc* per determinati utilizzi.

1.8 I *token*

I *token*, nell'ambito della sicurezza informatica, sono un insieme di informazioni sostitutive di altre che si desiderano mantenere non visibili a soggetti terzi. In relazione alla *blockchain* e alle criptovalute, il *token* è considerato un contenitore di informazioni e dati appartenenti a colui che ne risulti il "proprietario" in base alle transazioni tracciate sulla *blockchain*[105]. Tecnicamente, esso è l'*hash* della transazione, ossia una stringa di valori che si riferisce solo e soltanto ad una specifica transazione e può essere scambiato liberamente e condiviso. Pertanto, esso certifica la titolarità della transazione da parte del soggetto a cui il *token* è "intestato", il quale può essere scambiato sulla *blockchain* o anche conferire diritti eterogenei eseguibili automaticamente grazie al funzionamento degli *smart contract*.

---

[104] «*essentially, PoAu can be seen as a modi ed PoS algorithm, where validators' stake is their own identity. Network members put their trust into authorised nodes and a block is accepted if the majority of authorised nodes signs the block. Any new validators can be added to the system via voting*», ANDONI M., - ROBU V., - FLYNN D., - ABRAM S., - GEACH D., - JENKINS D., - MCCALLUM P., - PEACOCK A., *Op. cit.,* 150

[105] FISCH C., *Initial coin offerings (ICOs) to finance new ventures* in *Journal of Business Venturing* n. 34, 2019, 3

Lo scambio e l'emissione di nuovi *token* presentano problematiche di inquadramento giuridico[106], pertanto è necessario distinguere tre categorie di *token* in base ai diritti esercitabili grazie attraverso essi, nei confronti o meno di una controparte[107].

La prima categoria di *token* è la criptovaluta strettamente intesa, dove non è presente alcuna controparte e ha l'unica funzione di esplicitare la titolarità dello stesso *token*. Esso non conferisce diritti oltre alla proprietà stessa del *token*, ed esempi tipici di questa tipologia sono i *token Bitcoin*, semplici unità di valore interscambiabili.

La seconda categoria di *token* invece, assegna al titolare diritti esercitabili nei confronti dell'emittente del *token* o di terzi. Essi sono verosimilmente inquadrabili sotto lo stesso schema tipico dei titoli di credito poiché, similarmente, conferiscono a chi dimostra la titolarità del *token* il diritto ad una prestazione in esso indicata (1992 c.c.). Alternativamente, i *token* dove il titolare ha diritto a ricevere un pagamento di un importo specifico, sono inquadrabili come promesse di pagamento (1988 c.c.).

La terza categoria, infine, consiste in *token* che rappresentano una proprietà ma al contempo conferiscono anche determinati diritti, quali diritto di voto, ma non conferiscono al titolare diritti reclamabili verso l'emittente o verso terzi.

Procedendo ad un'analisi giuridica più approfondita, è possibile inquadrare le diverse categorie di *token* in diversi istituti codicistici[108].

I *token* della prima categoria, anticipando quanto verrà più esaustivamente analizzato nei successivi paragrafi, possono essere ricondotti alla definizione di "valuta virtuale" contenuta nel d.lgs. 21 dicembre 2007, n. 231 (normativa antiriciclaggio) alla lettera *qq*), comma 2 dell'art 1[109].

I *token* appartenenti alla seconda categoria, possono assumere diverse vesti e, in base ad esse, si prestano a un differente inquadramento giuridico.

---

[106] GIUDICI P., *ICO e diritto dei mercati finanziari: la prima sentenza americana* in *Le società* n. 1/2019, 62

[107] SARZANA DI S.IPPOLITO F. – NICOTRA M., *op. cit.,* 44

[108] SARZANA DI S.IPPOLITO F. – NICOTRA M. *op. cit.,* 44

[109] «*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*»

Nel caso di *token* che garantiscono un pagamento di una somma determinata, possono essere considerati alla stregua dei valori mobiliari, strumenti finanziari[110] o azioni. In questo caso, sarebbero applicabili le norme in tema di diritto societario, la direttiva MIFID 2, la disciplina degli emittenti del TUF come anche il regolamento CONSOB 11971/1999.

Qualora presentino tratti essenziali comuni con gli strumenti partecipativi al capitale di rischio, è da considerare la possibilità di applicare le norme in tema di *equity crowfunding*.

Infine, resta da considerare l'ipotesi che il *token* non configuri uno strumento finanziario, ma comunque la relativa emissione sia assimilabile all'attività, riservata alle banche, di raccolta del pubblico risparmio.

I *token* non configuranti uno strumento finanziario, o che conferiscono un diritto a prestazioni di servizi o beni, sono difficilmente inquadrabili in un singolo istituto, dando vita a negozi misti, disciplinati dall'autonomia contrattuale delle parti. Possono rientrare nella fattispecie di cui all' art. 1992 c.c. dei titoli rappresentativi di diritti di credito, rappresentativi di merci o documenti di legittimazione.

Riguardo i *token* della terza categoria, essi conferiscono diritti di comproprietà non rivolti all'emittente alla quale è possibile ricollegare l'istituto della comunione[111].

Dal versatile utilizzo che caratterizza i *token* ne consegue che non è possibile inquadrarli sotto un'unica disciplina giuridica. A seconda di come è configurato il funzionamento del *token* variano anche i possibili utilizzi distorti da parte degli

---

[110] BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto e informatica*., 2017, 34

[111] È stata anche teorizzata la possibilità di ricondurre i *token* e le criptovalute alla stregua di *bene* giuridico ma «*l'ostacolo principale rispetto a questa ricostruzione è costituito dalla concezione tradizionalmente "corporale" attribuita al termine «cosa» di cui all'art. 810 c.c. Secondo tale consolidata interpretazione, le entità immateriali non rientrano nel novero delle "cose" in quanto, appunto, prive del requisito della corporeità. Per conseguenza, i diritti di esclusiva (ivi compreso il diritto di proprietà) sulle entità diverse dalle "cose" sono regolati da un sistema sostanzialmente tipico: l'attribuibilità di tali diritti resta subordinata a un esplicito riconoscimento da parte dell'ordinamento. Ne discende che un'entità o risorsa incorporale può essere qualificata come «bene» in senso giuridico soltanto in presenza di una positiva statuizione normativa e non, semplicemente, sulla base del riferimento all'art. 810 c.c.*», RINALDI G., *op. cit.*, 290; sul punto anche BOCCHINI R., *op. cit.* 33, il «*nostro ordinamento, ancora troppo legato ad una nozione di cosa corporale e di bene materiale; e ciò, a nostro parere, rischia di non consentire una sicura e piena inclusione del* Bitcoin *nella sfera del diritto proprietario a causa della sua intrinseca natura, talmente immateriale da rimanere addirittura diffusa all'interno di una rete di comunicazione elettronica ad architettura distribuita.*».

individui, con la conseguente applicazione di un differenziato regime giuridico e sanzionatorio; ma tutto ciò a patto che nell'ambito applicativo delle norme attualmente in vigore rientri l'utilizzo dei *token*. Nei prossimi paragrafi verrà approfondita l'applicabilità di determinati reati nel caso in cui vengono utilizzate valute virtuali e si vedrà come non sempre le norme vigenti riescano a punire e prevenire efficacemente le condotte commesse attraverso tali tipologie di *token*.

1.9 Le ICO e i relativi profili giuridici. La casistica statunitense

Con l'avvento della *blockchain* e delle criptovalute sono state sviluppate forme di raccolta di capitale caratterizzate dall'offerta al pubblico di *token* in corrispettivo di denaro o criptovaluta con l'obiettivo di finanziare progetti o servizi, chiamate "ICO" o "*initial coin offerings*"[112]. A differenza del *crowfunding*, le ICO utilizzano la *blockchain* per emettere i *token*, rappresentando un innovativo metodo per finanziare *start up* o imprese innovative[113].

Questo fenomeno, seppur poco conosciuto e diffuso tra i comuni risparmiatori tradizionali, ha raggiunto volumi di affari considerevoli. Basti pensare che solo nel mese di gennaio 2019 sono stati raccolti circa 300 milioni di dollari[114] in progetti ICO, e da marzo a giugno 2018 sono stati raccolti più di 13 miliardi di dollari[115].

Le ICO permettono specialmente a piccole imprese di raccogliere capitale utile per realizzare i propri progetti e correlativamente di dare impulso all'economia e alla crescita attraverso forme di investimento alternative a quelle impiegate normalmente nella prassi[116]. Esse, però, sono caratterizzate da una forte asimmetria informativa[117],

---

[112] FISCH C., *Initial coin offerings (ICOs) to finance new ventures* in *Journal of Business Venturing* n. 34, 2019, 1

[113] Il fenomeno delle ICO «*ha sostanzialmente soppiantato il* crowdfunding *tradizionale e, per i progetti legati al mondo blockchain, ha ormai largamente superato anche il venture capital»; l concetto di base delle ICO è analogo al* crowdfunding*, ma ulteriormente sviluppato. «Nel* crowdfunding *il soggetto che abbisogna di fondi per lanciare una qualche attività attribuisce dei diritti, per es., sul futuro godimento di quell'attività*», GIUDICI P., *op. cit.,* 62

[114] Fonte dati: *https://www.coinschedule.com/stats*

[115] Fonte dati: v. nota precedente

[116] «*A mechanism used by new ventures to raise capital by selling tokens to a crowd of investors*», FISCH C., *op. cit.,* 22

[117] GIUDICI P., *op. cit.,* 63

poiché le imprese sono nella maggior parte dei casi solo agli inizi del proprio sviluppo, e vi è anche un forte rischio di cadere in operazioni truffaldine[118], in quanto nessuno garantisce il successo del progetto o prima ancora la veridicità di quanto esplicato come obiettivo del finanziamento[119]; tali circostanze rendono manifesta la necessità di approntare una disciplina a tutela del consumatore/investitore che, nel vigente quadro normativo, è rimessa a disposizioni di settore difficilmente applicabili all'offerta di strumenti valutari virtuali.

Un altro fattore critico è che spesso l'impresa che offre *token* è poco incentivata a svelare nel dettaglio il proprio progetto, preferendo l'anonimità dei propri partecipanti, offrendo poche o nulle garanzie[120] agli investitori delle qualifiche possedute da detti soggetti.

Inoltre, bisogna considerare che non tutti i comuni investitori possiedono le capacità e competenze necessarie per comprendere e valutare il progetto e la tecnologia proposta dall'impresa da finanziare, anche se viene solitamente sottolineato che chi è disposto a investire in questo settore si presume che abbia determinate conoscenze; però, l'avvento di piattaforme sempre più *user-friendly,* coadiuvate da campagne di *marketing* senza controllo sulle piattaforme dei *social media* potrebbe portare investitori poco esperti ad esplorare il mondo delle ICO, assoggettandosi cosi a tutti i rischi che esse possono comportare agli investitori non professionali[121].

Pertanto, in virtù del fatto che le ICO interessano cospicue somme di denaro e che un loro uso poco accorto da parte degli investitori o fraudolento da parte degli offerenti[122] può causare danni ingenti, necessitano una regolamentazione adeguata per scongiurare abusi di mercato e nuove forme di riciclaggio.

Attualmente il panorama normativo delle definizioni e delle discipline applicabili alle ICO è frammentato, discordante e non armonizzato specialmente a livello europeo.

Di fatto, le imprese che lanciano una ICO raccolgono denaro presso il pubblico alla pari di una offerta pubblica iniziale (IPO), senza però essere obbligate a presentare un

---

[118] FISCH C., *op. cit.,* 23

[119] FISCH C., *op. cit.,* 23

[120] IBBA S., - PINNA A., - LUNESU M. L., - MARCHESI M., - TONELLI R., *Initial coin offerings and agile practices* in *Future internet*, 10, 2018, 2

[121] CROSSER N., *Initial coin offerings as Investment Contracts: are a blockchain Utility tokens securities?* in *The University of Kansas Law Review*, dicembre 2018, 1

[122] IBBA S., - PINNA A., - LUNESU M. L., - MARCHESI M., - TONELLI R., *op. cit.*, 3

capitale minimo come garanzia degli investitori, rispettare obblighi di trasparenza e i requisiti di onorabilità o professionalità. Pertanto, le autorità di vigilanza del mercato hanno cercato di inquadrare le ICO in determinate cornici definitorie per poter applicare anche ad esse le normative in materia di mercati finanziari.

Il primo caso che ha dato il via a numerosi provvedimenti da parte delle autorità di controllo di diversi stati[123] è il caso "The DAO", acronimo di "*Decentralized Autonomous Organization*" (organizzazione anonima decentralizzata, ossia una organizzazione "virtuale", senza una struttura, operante tramite *smart contracts* sulla *blockchain* di *Ethereum*)[124].

Gli sviluppatori di TheDAO avevano come obiettivo quello di raccogliere capitali emettendo "DAO Tokens" per poter finanziare progetti che venivano sottoposti al voto dei rispettivi titolari, decidendo in tal modo quali progetti sarebbero stati finanziati con il capitale raccolto. Il capitale raccolto sotto forma di *Ether* (la criptovaluta usata sulla *blockchain* di *Ethereum*) aveva raggiunto circa 150 milioni di dollari[125], senonché nel giugno 2016 un attacco al *wallet* che custodiva i fondi raccolti ha sottratto circa 50 milioni di dollari[126], suscitando l'attenzione della SEC (*Security and Exchange Commission*, autorità di controllo del mercato e della borsa statunitense), la quale provò a ricondurre la pratica di emettere *token* correlati alla *blockchain* in cambio di diritti di voto e/o proprietà, alla disciplina del collocamento di strumenti finanziari, ossia la "*Securities law*". A tal fine, la SEC utilizza il cosiddetto "*Howey Test*"[127], ossia segue i criteri interpretativi elaborati in una decisione della corte suprema statunitense del

---

[123] «*È un tema che sta interessando tutti i regolatori nazionali, ma come sempre lo sguardo di tutti - in primo luogo, proprio dei promotori di ICO - è rivolto agli Stati Uniti. Le ragioni sono molteplici. Ovviamente si tratta del mercato dove operano gli investitori più importanti del mondo e dove le imprese del settore tecnologico hanno un maggior peso*», GIUDICI P., *op. cit.*, 63

[124] Consultabile al seguente link: https://www.sec.gov./litigation/investreport/34-81207.pdf

[125] Fonte dati: v. nota precedente

[126] Ciò portò al "*fork"* della *blockchain* di *Ethereum*, ossia una ramificazione di essa, dando vita alla distinzione tra *Ethereum* Classic (la *blockchain* più antica) ed *Ethereum* (il nuovo ramo della *blockchain*)

[127] Secondo l'*howey test*, un contratto di investimento è caratterizzato da "[…]*an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others*", ossia da un investimento di denaro in una impresa con una ragionevole aspettativa di profitti derivanti da sforzi imprenditoriali o manageriali di altri; i criteri interpretativi pertanto sono quattro: 1) investimento in denaro; 2) impresa collettiva; 3) aspettativa di profitti; 4) profitti ottenuti da sforzi imprenditoriali o manageriali altrui. GIUDICI P., *op. cit.*, 64

1946[128] (SEX v. W.J. Howey Co., 328 U.S 293, 301, 1946) appunto per determinare se l'ICO di TheDao sia un contratto di investimento e quindi sottoposto alle norme sulle *securities*[129].

Il risultato dell'analisi ha portato la SEC a ritenere applicabile la *Securities Law*, in seguito alla riconduzione dei *tokens* TheDAO alla fattispecie degli strumenti finanziari. Importante sottolineare come sia necessario un approccio "*case by case"*, ossia bisogna valutare il caso concreto per determinare l'applicabilità o meno della *Securites Law Act*. Il suddetto approccio però, comporta notevoli difficoltà nel predeterminare se una ICO sarà assoggettata alle norme sugli strumenti finanziari, andando così a generare incertezza sia da parte di chi vuole raccogliere capitali e finanziari per progetti e *start up* innovative, sia per chi desidera investire in questo settore. Infatti, la SEC è arrivata a qualificare come *Securities* anche una ICO lanciata nel 2017[130] che si presentava come emittente di "*utility tokens*", ossia *token* che

---

[128] «*La Corte Suprema degli Stati Uniti già nel 1946 nel caso Howey abbracciò l'interpretazione funzionale, non formalistica, del concetto di contratto di investimento che si era consolidata nelle leggi statali che avevano preceduto la legislazione federale (*"blue sky laws*"), leggi in cui - come notava la Corte Suprema - sin da subito* "la forma era stata abbandonata a favore della sostanza e l'enfasi era stata posta sulla realtà economica*"*», GIUDICI P., *op. cit.*, 64

[129] In relazione al caso concreto, la SEC ha precisato al terzo capitolo, lett. B, par. 2, del "*Report of Investigation Pursuant to Section* 21(a) *of the Securities Exchange Act of 1934*: The DAO" che anche se si parla di "*money*'' (denaro), non è necessario che l'investimento sia "monetario", ma può anche essere rappresentato sotto un'altra forma di valore. Nel caso di specie, gli investitori avevano conferito *Ether*, i quali hanno un valore di mercato, in cambio dei DAO Tokens; pertanto il primo requisito è rispettato; non vi è dubbio, poi, che si tratti di una impresa gestita da più persone. Riguardo il terzo requisito, è chiaro dai materiali promozionali e dalle dichiarazioni fatte dai creatori di TheDAO che l'investimento avrebbe dato diritto a "*rewards*" (ricompense), andando a configurare, quindi, una impresa con scopo di lucro. Tutto questo comporta che l'investitore medio è certamente motivato, seppur parzialmente, dalla prospettiva di profitto dell'investimento dei propri ETH (*Ether*) in *tokens* TheDAO. Il quarto ed ultimo requisito riguardante la provenienza dei profitti dallo sforzo manageriale altrui è soddisfatto nel caso di specie in quanto l'attività dei creatori di TheDAO era essenziale per lo sviluppo e la continuità del progetto. Infatti, essi continuamente monitoravano le operazioni, salvaguardavano gli investitori e sceglievano quali dei contratti proposti dovevano essere ammessi al voto. Perciò, l'esperienza e le qualifiche dei creatori del progetto, ma soprattutto la loro gestione e cura del successo di esso non lasciava altro spazio agli investitori se non di affidarsi completamente alla loro competenza.

[130] La ICO in questione prendeva il nome di Munchee, che raccolse circa 15 milioni di dollari per finanziare lo sviluppo di un *app* per dispositivi *Iphone*. Nel "*white paper*" di Munchee gli sviluppatori fanno riferimento al caso TheDAO e dichiarano che il loro progetto è *compliant* con l'*Howey Test*, non configurandosi i *tokens* da loro emessi come *Securities* poiché configuranti per l'appunto *utility tokens* e non *security tokens*. Nonostante la previa verifica di *compliance* con le norme vigenti negli Stati Uniti riguardo l'emissione di strumenti finanziari, la SEC ha analizzato nel dettaglio le condotte tenute dagli sviluppatori di Munchee e ha concluso per la configurazione dello schema giuridico dei contratti di investimento sempre facendo riferimento all'*Howey Test*. Nel caso concreto, l'obiettivo di Munchee era

conferiscono il diritto di usufruire di servizi digitali determinati, e perciò ritenuta fuori dall'area di applicazione della *Securities Law Act* del 1933.

La SEC afferma che apponendo l'etichetta di "*utility token*" agli *asset* emessi in seguito ad una ICO, non preclude la loro configurazione come *securities*, essendo fondamentale l'analisi della realtà economica sottostante la transazione, e quindi privilegiando la sostanza sulla forma (in linea con i nostri principi di diritto privato riguardo il *nomen iuris* assegnato ad un determinato schema contrattuale che non pregiudica l'applicazione di una disciplina differente in base alla sua vera ed effettiva natura giuridica).

Per tentare di aggirare l'*Howey Test*, è stata teorizzata una diversa tipologia di *token* chiamata "SAFT" (*Simple Agreement for Future Tokens*)[131] dal giurista statunitense Marco Santori che, nella categoria degli *utility tokens*, distingue tra "*pre-functional tokens*" e "*already-functional tokens*"; i primi, sono *tokens* offerti al pubblico prima ancora che gli sviluppatori abbiano realizzato il progetto, e che con estrema probabilità andranno a configurare una *security* secondo i principi dell'*Howey Test* in quanto l'aspettativa del profitto sovrasterà l'aspettativa dell'utilizzo del *token*. I secondi, ai quali appartengono i SAFT, sono distribuiti solo dopo che il *network* è stato sviluppato e realizzato. Se essi sono realmente utilizzati in un *network* funzionante ed operativo, non possono rientrare nei requisiti *dell'Howey Test* in quanto il loro reale utilizzo prevale sullo scopo di lucro, cosi come non sarà basato sullo sforzo "altrui", in quanto esso è già stato utilizzato per la realizzazione del *network*, avvenuta prima dell'emissione dei *token*. Seppure essi vengano scambiati sul mercato secondario, non saranno comunque configurabili come *securities* in quanto il loro prezzo è determinato

---

quello di creare un "ecosistema", dove Munchee avrebbe pagato in MUN token per ogni recensione rilasciata. Nel *paper* si fa espresso riferimento al fatto che l'incremento della partecipazione all'ecosistema avrebbe fatto aumentare di valore i *token* emessi, e viene enfatizzato come la società avrebbe amministrato il proprio *business* in modo tale da aumentare il valore dei propri *tokens*. Inoltre, viene anche esplicitata la possibilità di togliere dalla circolazione un numero determinato di *tokens*, in modo tale da far aumentare il valore dei *tokens* ancora in circolazione. Altri argomenti a favore della qualificazione come *securities*, sono la circostanza che Muchee ha evidenziato a dovere l'esperienza, le capacita manageriali e le qualifiche tecniche derivanti anche da precedenti impieghi professionali dei propri dipendenti, inducendo gli investitori a credere e sperare che gli sforzi degli sviluppatori avrebbero da soli comportato il successo o il fallimento dell'azienda, come nel caso TheDAO.

[131] BATIZ-BENET J., - SANTORI M., CLAYBURGH J., *The SAFT Project: Toward a Compliant Token Sale Framework*, ottobre, 2017, 2

esclusivamente dall'incontro della domanda e dell'offerta e non sullo "sforzo altrui" come richiesto dall'*Howey Test*[132]. Pertanto, l'intento lucroso sarà determinato da fattori diversi e prevalenti rispetto agli sforzi altrui, in quanto il progetto è già stato sviluppato e realizzato in precedenza.

Il tentativo di Santori, quello di aver creato uno schema contrattuale che si incastri nelle norme senza violarle, con l'intenzione di favorire il proliferare delle raccolte di capitali per finanziare progetti e *start up* è senz'altro da lodare per le intenzioni più che l'effettiva l'utilità pratica dello stesso. Di fatto, è necessario non limitare l'innovazione tecnologica ingabbiandola nel fitto schema di fattispecie giuridiche esistenti, ma è ancor più necessario proiettarsi verso nuove definizioni e fattispecie che meglio si prestino ai risultati del progresso tecnologico. Lo sforzo interpretativo necessario per rendere malleabili le norme non sempre porta a risultati soddisfacenti e pertanto solo nuove iniziative del legislatore potrebbero contemperare esigenze di regolamentazione ed esigenze di favoreggiamento dell'innovazione tecnologica in continua evoluzione.

In tempi recenti, proprio in virtù dell'incertezza riguardo l'inquadramento giuridico di queste nuove forme di raccolta di capitale, stiamo assistendo alla proliferazione delle cosiddette STO, ossia le *Secuity Token Offering*. A differenza delle ICO, con le quali venivano emessi sostanzialmente *security tokens* senza però rispettare le norme applicabili, le STO emettono anch'esse *security tokens* ma rispettano la disciplina dell'emissione di strumenti finanziari; probabilmente è stato compreso che tentare di aggirare le norme in tema di strumenti finanziari porta solo a sanzioni e multe da parte delle autorità di controllo e pertanto la via della *compliance* è quella più sicura e da preferire.

Il legislatore dovrà tener conto che le norme da implementare non dovranno andar a discapito dell'innovazione tecnologica e degli investimenti nel settore delle *start up* innovative. Norme troppo repressive e adempimenti che rendono macchinoso il lancio di una ICO potrebbero scoraggiare investimenti e sviluppi di progetti dedicati al progresso tecnologico. Inoltre, normare in Italia in maniera chiara e comprensibile, sia per le imprese che per investitori, porterebbe anche ad una cospicua affluenza di capitali esteri, in quanto si è constatato che le imprese sono più incentivate a lanciare

[132] CROSSER N., *op. cit.,* 3

ICO dove la regolamentazione è chiara senza temere di essere sanzionati per inquadramenti giuridici arbitrari *ex post* che comportano l'applicazione di norme e sanzioni non considerate applicabili dall'impresa al momento del lancio dell'ICO.

1.9.1 (*Segue*) Le casistiche europee: le linee guida della FINMA

Nonostante le autorità di controllo del mercato di diversi stati europei si sono pronunciate riguardo i rischi e gli obblighi derivanti dall'uso delle criptovalute e delle ICO, le linee guida della FINMA[133] (autorità di controllo del mercato finanziario svizzera) pubblicate il 16 febbraio 2018 spiccano per il loro risultato classificatorio e di orientamento tra le norme applicabili nei riguardi dell'emissione dei *tokens*.

L'autorità svizzera adotta un approccio collaborativo, cercando di far chiarezza sulle informazioni da fornirle per ottenere un parere preventivo sulla disciplina applicabile e correlativamente esplica i principi attraverso i quali andrà a valutare le richieste di parere. Viene prima di tutto messo in chiaro, in linea con quanto enunciato della SEC, che indicazioni generali compatibili con qualsiasi tipo di ICO non possono essere fornite, dovendo andare a considerare il caso concreto in base al reale funzionamento e configurazione dell'operazione di raccolta di capitale. Inoltre, in virtù dell'assenza di una generale classificazione delle tipologie di *token* a cui attenersi né in Svizzera, ne in altri paesi, la FINMA dichiara di seguire un approccio «orientato alla funzione economica»[134], e propone di classificare i *tokens* i tre tipologie: 1) *token* di pagamento; 2) *utility token*; 3) *token* di investimento.

I primi, sono *token* che «*effettivamente o nelle intenzioni dell'organizzatore, sono accettati come mezzi di pagamento per l'acquisto di beni o servizi oppure sono finalizzati al trasferimento di denaro e di valori*» e non conferiscono alcun diritto nei confronti dell'emittente.

I secondi, sono invece *token* «*che permettono di accedere a un'utilizzazione o a un servizio digitale forniti su o dietro utilizzo di un'infrastruttura blockchain.*»

---

[133] Consultabili al seguente link*: https://www.finma.ch/it/news/2018/02/20180216-mm-ico-wegleitung/*

[134] V. *Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offering (ICO)*, edizione del 16 febbraio 2018, FINMA

I *token* di investimento rappresentano valori patrimoniali, come ad esempio un credito nei confronti dell'emittente o un diritto sociale rispettivamente ai sensi del diritto delle obbligazioni e societario; quindi, secondo la loro funzione economica possono essere inquadrati come azioni, obbligazioni o strumenti finanziari derivati.

Infine, è da considerare la configurazione di *token* "ibridi" tra *token* di pagamento e *utility token* o di investimento. In questo caso, il *token* viene classificato cumulativamente come valore mobiliare e mezzo di pagamento.

Scendendo nel dettaglio, la FINMA dichiara che la funzione economica dei *token* di pagamento, non permette di classificarli come valori mobiliari non applicandosi così la rispettiva disciplina. I *token* di utilizzo, invece, sono considerati valori mobiliari solo se sussiste la funzione economica di investimento, anche soltanto parzialmente. I *token* di investimento invece sono a tutti gli effetti valori mobiliari nel caso in cui «*rappresentano un diritto valore e i token sono standardizzati e idonei a essere negoziati su vasta scala*».

In seguito alla classificazione, la FINMA esplicita la necessità della richiesta dell'autorizzazione e della sottoposizione alla vigilanza prudenziale nei seguenti tre casi: i *token* configurano derivati finanziari; i *token* non sono derivati ma sono rilevati da terzi ed offerti stabilimenti o su commissione sul mercato primario; i *token* conferiscono, similarmente ai depositi bancari, diritto di rimborso del capitale.

Riguardo l'applicazione della normativa svizzera in tema di riciclaggio (LRD) del denaro, la FINMA chiarisce che essendo i *token* trasferibili utilizzando la *blockchain*, una ICO di *token* di pagamento costituisce una emissione di mezzi di pagamento, dalla quale deriva l'obbligo assoggettamento alla vigilanza prudenziale. L'applicazione della suddetta normativa impone obblighi di diligenza e l'obbligo di affiliazione ad un organismo di autodisciplina (OAD) o di sottoporsi alla vigilanza della FINMA; ma tale obbligo è considerato assolto nel caso in cui i *token* di pagamento vengano gestiti attraverso un intermediario già sottoposto alla normativa antiriciclaggio. In ultima analisi, la conversione di criptovalute in valute avente valore legale o con altre criptovalute comporta, secondo la FINMA, anch'essa la sottoposizione alle norme in materia di riciclaggio[135].

[135] SARZANA DI S. IPPOLITO F., - NICOTRA M., *op. cit.,* 50

Considerando nell'insieme le linee guida sopra esposte, esse hanno il pregio di delineare con chiarezza le tipologie di *token* e di ricollegare con precisione e senza lasciare spazi grigi le normative applicabili ai singoli casi concreti.

1.9.2 (*Segue*) Le norme riguardanti le ICO della Repubblica di Malta

Il 4 luglio 2018, sono stati emanati ben tre atti legislativi da parte del governo maltese riguardanti la *blockchain* e le *distributed ledger technologies*. Uno di questi, il "*Virtual financial assets act*", disciplina le "*Virtual financial asset*" (VFA), ossia qualsiasi forma di registrazione digitale il quale viene usato come mezzo di scambio, unita di conto, o deposito di valore. Esso inoltre, non è moneta elettronica, strumento finanziario[136] o un *token* virtuale (strumento digitale registrato, la cui utilità, valore o applicazione è ristretta soltanto all'acquisto di beni o servizi all'interno della piattaforma DLT o che se emesso possa essere scambiato con fondi solamente sulla piattaforma e direttamente dall'emittente).

La parte centrale della normativa è costituita dall'obbligo di redigere un *white paper* che rispetti determinati requisiti indicarti nell'art. 4 e che sia registrato presso le autorità competenti. È prevista, inoltre, la nomina di un "VFA agent", registrato ed autorizzato ad esercitare attività di consulenza, contabilità e revisione legale dei conti.

Viene sancita la responsabilità per i danni sopportati dagli acquirenti di VFA in caso di false informazioni contenute nel *white paper*, così come viene regolata l'attività di pubblicizzazione della ICO, prescrivendo che l'*advertinsing* debba essere chiaramente identificabile come tale e che siano rispettosi di quanto riportato nel *white paper*.

Nel secondo allegato alla legge, disciplina i cosiddetti "*VFA services*", riguardanti la trasmissione, esecuzione di ordini, gestione portafogli ecc. correlati ai VFA, predisponendo un obbligo di licenza e il relativo registro dei titolari, sottoposti alla vigilanza dell'autorità emittente.

---

[136] «*Nonostante la nomenclatura utilizzata possa far sembrare diversamente, il testo specifica espressamente che i* virtual financial asset *non devono essere considerati strumenti finanziari*», RINALDI G., *op. cit.*, 274

Infine, a tutela del mercato sono state predisposte norme penali nella sezione 4 intitolata "prevenzione di abusi di mercato". Viene qualificato come reato la condotta di "*insider dealing*", verosimilmente corrispondete alle condotte del art. 184 TUF, compresi il *tipping* e *tauytage* (art.184 comma 1 lett a e b, TUF); all'art. 36 vengono inoltre qualificate come reato le condotte di manipolazione di mercato, sempre in linea con la disciplina italiana, in questo caso l'art. 185 del TUF.

In conclusione, la Repubblica di Malta è stata lungimirante nell'ambito delle norme appositamente dedicate alla *blockchain* e alle ICO, emanando leggi che, sul solco delle normative in ambito finanziario e di tutela del mercato, mirano a regolare ciò che l'innovazione tecnologica produce senza cercare (attraverso impervi sforzi interpretativi) di renderlo compatibile con le norme già in vigore ed emanate prima che il fenomeno della *blockchain* e delle criptovalute prendesse piede. L'emanazione di questo tipo di norme, inoltre, favorisce l'afflusso di capitali esteri e il fenomeno del cosiddetto "*forum shopping*"[137], in quanto gli interessati al lancio di una ICO sceglieranno molto verosimilmente il paese dove è chiara e certa la legge applicabile, gli obblighi da adempiere e le relative sanzioni.

Seppur lodevole lo sforzo del legislatore maltese, è auspicabile il predisporre discipline uniformi che coinvolgano il maggior numero di stati possibili, in quanto il fenomeno della *blockchain* e delle nuove tecnologie è transazionale, che richiede un grado di tutela uniforme per tutti i cittadini, a prescindere dalla loro provenienza geografica.

Il cyberspazio non tiene conto dei confini nazionali[138], pertanto gli operatori nel settore delle nuove tecnologie dovrebbero essere confortati da ordinamenti giuridici quanto più uniformi possibili per permettere loro di svolgere le proprie attività senza essere limitati dai confini territoriali, categoria sconosciuta o quanto meno irrilevante per il cyberspazio. Ovviamente l'omogeneità delle norme deve riguardare anche la qualificazione di determinate condotte come reati o sanzioni amministrative; se i diversi stati europei fossero liberi di scegliere alternativamente se istituire sanzioni penali o amministrative, il fenomeno del *forum shopping* non sarebbe comunque

[137] SARZANA DI S. IPPOLITO F., - NICOTRA M., *op. cit.,* 35
[138] RINALDI G., *op. cit.*, 260

debellato.

1.9.3 (*Segue)* Le pronunce dell'Agenzia delle Entrate, CONSOB e Banca D'Italia in tema ICO e *tokens*

Nel nostro Ordinamento non sono ancora state introdotte norme volte a regolare la disciplina dei *tokens* e delle ICO come hanno provveduto a fare stati come Svizzera e Malta. Ad oggi, pronunce riguardanti i suddetti temi provengono dalla Agenzia delle Entrate con la Risposta n.14/2018 dalla CONSOB con la delibera n. 20660 del 31 ottobre 2018.

Il quesito sottoposto all'agenzia delle entrate riguarda la promozione di una ICO avete ad oggetto l'emissione di *utility tokens* cedibili a terzi, e il relativo trattamento fiscale ai fini delle imposte dirette (IRES e IRAP) e indirette (IVA) specificatamente riguardo le operazioni di cessione dei *token* e di conversione delle criptovalute (*bitcoin* o *Ethereum*) in valuta corrente. Fa notare l'Agenzia delle Entrate che bisogna tener conto, per meglio apprezzare l'efficacia della risposta all'interpello, che l'istante non ha prodotto il *white paper* descrittivo del progetto, e pertanto la risposta si esprime con specifico riferimento a *token* rappresentativi unicamente del diritto di acquistare beni e servizi del soggetto emittente (*utility token*), con espressa esclusione di finalità di natura monetaria, speculativa e partecipativa.

Vengono preliminarmente definiti, in linea con la pronuncia della FINMA (ma senza considerare i *token* di pagamento) due categorie di *token*: *security token*, rappresentativi di diritti economici legati all'andamento dell'iniziativa imprenditoriale e/o di diritti amministrativi, e *utility token*, rappresentativi di diritti diversi, legati alla possibilità di utilizzare il prodotto o il servizio che l'emittente intende realizzare[139].

Riguardo l'applicazione delle norme in tema di IVA, le ICO della suddetta tipologia vengono semplicemente considerati come *voucher*, strumenti che conferiscono al detentore il diritto di beneficiare di determinati beni e/o servizi, e quindi come una «*mera movimentazione finanziaria, non rilevante ai fini IVA, la cui esigibilità si avrà solo al momento in cui i beni saranno ceduti o i servizi prestati con*

[139] SARZANA DI S. IPPOLITO F., - NICOTRA M., *op. cit.,* 50

la spendita dei token.». Questa dunque è la posizione della agenzia delle entrate riguardo la natura delle ICO, ma essendo una risposta ad un interpello, non ha efficacia *erga omnes* e pertanto ha validità solo riguardo il caso concreto, ossia ICO di *utility token* (che nelle pronunce della SEC sono state quelle per le quali è stata prestata maggior attenzione in quanto sono *utility token* che sebben nominati come tali, in realtà nascondono logiche di profitto che li assimilano alle *securities*).

La delibera della CONSOB, invece, concerne la sospensione ai sensi dell'articolo 99, comma 1, lett. b), TUF, di un'offerta al pubblico di criptovalute promossa da una società di diritto inglese in Italia.

Secondo la CONSOB, le *Initial Coin Offering* sono suscettibili di configurare offerte al pubblico di prodotti finanziari ex art. 1, comma 1, lett. t), del TUF; riguardo la classificazione dei *token* alla stregua di "prodotti finanziari" *ex* art. 1, comma 1, lett. u), del TUF, la CONSOB prende in considerazione le caratteristiche dei *token* emessi nel caso sottoposto alla sua attenzione e rileva che vi sono: l'impiego dell'aderente all'offerta del proprio capitale; lo scopo di ottenere un rendimento predefinito compreso tra un minimo e un massimo espresso in misura percentuale e calcolato sul capitale conferito dall'investitore; il potenziale rischio finanziario. Considerati nell'insieme questi elementi, la CONSOB qualifica quindi la ICO in questione come un investimento di natura finanziaria, e la conseguente violazione delle norme riguardanti la suddetta materia giustifica la sua sospensione[140].

Infine, per fornire una panoramica completa delle pronunce delle autorità italiane, è da tener presente quanto pubblicato dalla Banca D'Italia nel marzo 2019 riguardo le «*cripto-attività*»[141].

In particolare, viene fornita una dettagliata classificazione delle diverse tipologie di *token* basati sulle *distributed ledger technologies*. La prima, le «*valute virtuali*», ricomprendono i *token* privi di diritti incorporati, negoziabili e convertibili con moneta legale o con altre valute virtuali. Alla seconda categoria appartengono i *payment tokens,* con cui si replicano le funzionalità della moneta mantenendo con essa un valore fisso

[140] Per approfondimenti consultare il seguente link: https://www.chiomenti.net/approfondimenti/delibera-consob-in-materia-di-initial-coin-offering-ico-

[141] CAPONERA A., - GOLA C., *Aspetti economici e regolamentari delle «cripto-attività»* in *Occasional Papers*, Banca D'Italia, n.484

(in alcuni casi possono anche essere considerati come valuta elettronica se ne rispettano puntualmente i requisiti).

I *security tokens* sono *tokens* simili a titoli dematerializzati che vengono scambiati tramite le DLT, tipicamente a seguito di una ICO; il relativo *status* giuridico è «*incerto*» e non vi è uniformità di opinioni né a livello europeo né nelle altre giurisdizioni.

Infine, gli *utility tokens* sono caratterizzati dal fatto che non sono negoziabili e che offrono unicamente diritti amministrativi o licenze d'uso, come l'accesso ad una piattaforma o un *network* di persone.

Gli autori precisano poi che se nel corso del loro uso diventassero *tokens* portatori non solo di un diritto ma anche pienamente trasferibili e negoziabili su un mercato negoziato, allora diventerebbero *security tokens*, da cui deriverebbe l'applicazione delle norme in materia di strumenti finanziari.

Riassumendo, nonostante non siano numerose le pronunce delle corti o autorità italiane, comunque specialmente in seguito all'attenzione dedicata alle criptovalute da parte delle autorità europee (approfondite nel corso del successivo paragrafo) e non, anche in Italia si è cercato di inquadrare con precisione e senza ambiguità l'istituto giuridico più adatto per ogni tipologia di *token* in modo tale da non creare incertezza e vuoti di tutela.

1.9.4 (*Segue)* Il report dell'ESMA sulle ICO e i "*Crytpo-Assets*"

Il 9 gennaio 2019 l'ESMA (*European Securities and Market Authority*), ha pubblicato un *report*[142] riguardante le criptovalute, *token* e in particolare le ICO e le discipline di rango comunitario orientativamente applicabili.

Nelle premesse iniziali, l'ESMA riconosce che il diffondersi dei "*crypto-asset*"[143] comporta notevoli difficoltà per il legislatore e i partecipanti al mercato in quanto non

[142] ANNUNZIATA F., Distributed Ledger Technology *e mercato finanziario: le prime posizioni dell'ESMA, in* Fintech, 2019, 1

[143] La definizione di *cryptoasset* presente nel glossario del report ESMA del 9 gennaio 2019: "*a type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT) or similar technology as part of their perceived or inherent value. Unless otherwise stated, ESMA uses the term to refer to both so-called 'virtual currencies' and 'digital tokens'. Crypto-asset additionally means an asset that is not issued by a central bank.* »

vi è chiarezza sulle cornici normative applicabili; e se fossero applicabili, ci potrebbero essere casi in cui è necessario una differente interpretazione o riconsiderazione dei requisiti di applicazione di suddette norme. L'approccio nel creare o riconsiderare le norme, auspicato dalla ESMA, è definito «*technology-neutral approach*», ossia non focalizzato sul tipo di tecnologia utilizzata, in modo tale da assicurare una portata applicativa nelle norme più ampia possibile a prescindere da come vengono configurati tecnicamente di volta in volta i *crypto-assets*. Non esiste, pertanto, una soluzione alla problematica della qualificazione giuridica dei *cripto-assets* su misura per ogni di *token* o criptovaluta.

Nonostante l'autorità europea non consideri, attualmente, il fenomeno dei *crypto-assests* come effettivamente dannoso per la stabilità finanziaria, essa si preoccupa di evidenziare i rischi a cui gli investitori e l'integrità del mercato sono esposti: truffe, "*cyber-attacks*", riciclaggio e abusi di mercato; non dimentica di sottolineare però anche l'altra faccia della medaglia, ossia tutti i benefici che le ICO e la "tokenizzazione" comporta. Ad esempio, le ICO configurano un'utile alterativa alla raccolta di fondi per *start-up* basate sulla *blockchain* o per altri progetti innovativi che avrebbero difficoltà ad ottenere finanziamenti tramite i metodi tradizionali; ancora, esse danno la possibilità anche ai piccoli investitori di partecipare a finanziamenti di imprese nella loro fase embrionale. I benefici della «*tokenisation*» invece, riguardano sia i partecipanti al mercato, sia gli investitori: aumento della liquidità di azioni non quotate o di prestiti sindacati ottenuti da un più semplice e veloce trasferimento, cosi come l'implementazione di *smart contracts* che riducono rischi e costi di esecuzione delle obbligazioni contrattuali.

Viene poi ripresa la classificazione dei *crypto-assets* sul solco lasciato dalla pronuncia della FINMA (*token* di investimento, *utility token* e *token* di pagamento) ma viene anche data una definizione di *distributed ledger tecnlogy* e di *blockchain* a livello europeo[144], che può essere di stimolo per una uniforme definizione delle stesse nelle norme dei singoli paesi dell'unione europea.

---

[144] «*Blockchain: a form of distributed ledger in which details of transactions are held in the ledger in the form of blocks of information. A block of new information is attached into the chain of pre-existing blocks via a computerised process by which transactions are validated; Distributed ledger technology (DLT): a means of saving information through a distributed ledger, i.e., a repeated digital copy of data available at multiple locations. DLT is built upon public-key cryptography, a cryptographic system that*

Riguardo la questione della qualificazione giuridica dei *crypto-asset*, l'ESMA premette che non vi è ancora una definizione giuridica degli stessi nel panorama delle norme europee dei mercati finanziari, e pone la propria attenzione sulla possibilità di qualificarli alla stregua di strumenti finanziari rientranti nella direttiva MiFID II. A tal fine, l'ESMA ha condotto nell'estate del 2018 uno studio interrogando le autorità del controllo del mercato degli stati membri riguardo la possibile qualificazione giuridica dei *crypto-assets*. I risultati del sondaggio hanno rivelato che la maggior parte delle autorità nazionali considera gli stessi come rientranti appieno nei requisiti richiesti dalla direttiva riguardo la qualificazione di strumenti finanziari, e una parte di esse propongono modifiche alla leggi esistenti in modo tale da creare norme su misura tenendo in considerazione la natura peculiare dei *crypto-assets*; le autorità che non li considerano come strumenti finanziari, invece, sono quelle appartenenti a paesi dove vi è stato un approccio più restrittivo in sede di trasposizione della direttiva MiFID II nell'ordinamento nazionale.

Se quindi è possibile qualificarli come strumenti finanziari[145], diverse sono le normative che di conseguenza sarebbero applicabili. Le soluzioni adottate dall'ESMA comprendono tra le tante la direttiva prospetto 2003/71/EC (e il relativo regolamento 2017/1129), la Direttiva Trasparenza 2013/50/EU, la direttiva MiFID II e il regolamento MiFIR, il regolamento MAR riguardante gli abusi di mercato e infine la quinta direttiva in tema antiriciclaggio e finanziamento del terrorismo. Pertanto, ai fini regolamentari l'emissione di *crypto-assets* al pubblico sarà accompagnata dall'obbligo di redigere il prospetto informativo (in realtà la maggior parte delle ICO già vengono spontaneamente accompagnate da un *white paper*[146], dove viene esposto e divulgato il progetto da finanziare) con la conseguente applicabilità del reato di falso in prospetto *ex* art. 173-*bis* TUF; anche obblighi di trasparenza scaturiranno dall'emissione di strumenti finanziari sotto forma di *crypto-assets* nei confronti degli emittenti, e che potenzialmente metteranno fine a ciò che avviene frequentemente nella prassi, ossia

uses pairs of keys: public keys, which are publicly known and essential for identification, and private keys, which are kept secret and are used for authentication and encryption. »

[145] Riguardo le criptovalute, invece, BOCCHINI R., *op. cit.*, 34, propende per l'esclusione della qualifica di strumenti finanziari, «*Le cosiddette monete virtuali restano, dunque, fuori dall'ambito di applicazione non solo del T.U.F., ma sono escluse anche dall'applicazione, ad esempio, del c.d. "sistema MiFI", previsto dalla omonima Direttiva 2004/39/CE relativa ai mercati degli strumenti finanziari.*»

[146] FISCH C., *op. cit.,* 23

ICO truffaldine di soggetti o organizzazioni anonime che dopo aver raccolto il capitale fanno perdere le loro tracce. Il regolamento MiFIR e la direttiva MIFID II comportano il rispetto di specifici requisiti e l'obbligo di autorizzazione per l'emissione di *security tokens* o l'esercizio di attività o servizi di investimento, cosi come il regolamento MAR comporterebbe la configurazione di reati come *insider trading* e manipolazione di mercato. Infine, con la V Direttiva Antiriciclaggio, gli *exchange* che permettono la conversione di valuta "fiat" in criptovaluta e viceversa rientrano tra i "soggetti obbligati" sottoposti agli obblighi della direttiva; l'ESMA precisa però, che i servizi "*crypto-to-crypto*" (conversioni tra *crytpo-assets*) sono in prevalenza e pertanto si auspica una revisione della direttiva antiriciclaggio in modo tale da far rientrare tra i soggetti obbligati anche ai provider di servizi *crypto-to-crypto* e di servizi finanziari correlati alle ICO.

Alla luce del contenuto del report dell'ESMA, è possibile pertanto rilevare come il fenomeno delle ICO e delle criptovalute, seppur di dimensioni ridotte, comunque necessita l'applicazione di normative volte a tutelare gli investitori e il mercato dai diversi pericoli astrattamente configurabili alla stregua degli strumenti finanziari.

Inoltre la tendenza dell'ESMA, in linea con l'approccio dei vari paesi membri, è quella di forzare le norme attualmente in vigore per renderle applicabili ai *crypto-assets*. L'ideale, per aver certezza degli obblighi a cui sono sottoposti i soggetti che operano nel mondo delle criptovalute, è dar vita a definizioni giuridiche di ampio respiro cosi come anche promuovere modifiche volte a far rientrare nelle cornici normative di rango comunitario i *crypto-assets*, le ICO e le relative attività e servizi.

1.10 La *blockchain* come veicolo di valuta: il *bitcoin*. Il suo inquadramento giuridico e profili penali

A parte l'utilizzo della *blockchain* per la notarizzazione dei documenti o per la creazione e scambio di *token*, l'applicazione senza dubbio più conosciuta e diffusa della tecnologia *blockchain* è rappresentata dalle criptovalute, quali *bitcoin* ed *Ethereum*.

In particolare, il *bitcoin* è stato specificatamente concepito come sistema di pagamento basato sulla crittografia indipendente da qualsiasi ente terzo "fidato" che ne garantisse l'integrità e il funzionamento, in alternativa a quello tradizionale

rappresentato dal sistema bancario[147]. Quindi, il motivo fondante del concepimento del *bitcoin* era quello di dar vita ad una "valuta", ossia un mezzo di scambio di valore da utilizzare per transazioni economiche. Seppur chiamate criptovalute, la soluzione del problema della loro qualificazione come valuta vera e propria non è così immediata[148] e di semplice soluzione[149].

È difficile equiparare il *bitcoin* alla moneta, in quanto per essere tale deve essere capace di assolvere alle funzioni di mezzo di scambio, unità di misura e riserva di valore[150]. Senza dubbio il *bitcoin* non ha valore legale[151], in quanto non ha efficacia solutoria e liberatoria garantita dalla legge[152]. L'accettazione di criptovaluta è lasciata all'autonomia delle parti, ma il creditore ha la facoltà di rifiutare una *solutio* in criptovaluta. Oltre a non essere considerabile come mezzo di scambio, le criptovalute a causa dell'instabilità del loro "prezzo", non sono idonee ad assolvere la funzione di unità di conto. Infine, considerate come riserve di valore, si ripropone quanto già osservato sui *token* e sul loro inquadramento come *securities* e quindi di strumenti di

---

147 «*What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party*». NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 1. Consultabile al link seguente: *https://bitcoin.org/bitcoin.pdf*

148 «*La sua natura giuridica, tuttavia, risulta ben lungi dall'essere definita in modo pienamente soddisfacente e si presenta, quanto meno alla stregua delle norme del nostro ordinamento, come una questione ancora aperta, in cui la verità più si avvicina e più sfugge, al punto da divenire, come le macchie d'inchiostro del test di* Rorschach*, un tema in cui il criterio che anima i giudizi non è la contrapposizione giusto-sbagliato, ma ogni opinione sembra avere diritto di cittadinanza.*», GASPARRI G., *op. cit.*, 1

149 «*La natura poliforme che connota dal punto di vista tecnico il fenomeno criptovalutario si riverbera, inevitabilmente, anche sul versante del diritto. A livello internazionale, legislatori, autorità di vigilanza e regolamentazione, dottrina e giurisprudenza oscillano nel collocare le cripto-monete all'interno della categoria dei mezzi di pagamento, degli strumenti o dei prodotti finanziari, dei beni.*», RINALDI G., *op. cit.*, 267

150 DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti,* in Diritto penale contemporaneo, 26, consultabile al seguente link: https://www.penalecontemporaneo.it/upload/6425-divizio2018a.pdf

151 «*può ritenersi che la moneta virtuale non possa essere ricompresa tra le "monete regolamentate" e che il suo utilizzo possa trovare fondamento esclusivamente sulla base consensuale degli utilizzatori, ricadendo nei mezzi di scambio liberamente scelti dall'autonomia*», BOCCHINI R., *op. cit.*, 33

152 «*La sola, parziale, eccezione è costituita dal Venezuela, che ha recentemente coniato la prima criptovaluta di Stato, il petro. La Repubblica venezuelana si è contestualmente impegnata ad accettare questa nuova criptomoneta come forma di pagamento per un'ampia serie di rapporti che intercorrono tra cittadino e pubblica amministrazione (*"national taxes, fees, contributions and public services"*).*», «*che in ogni caso non sembra, almeno per il momento, voler attribuire al petro efficacia liberatoria ex lege in ordine ai pagamenti tra privati*», RINALDI G., *op. cit.,* 268

investimento.

Si potrebbero far rientrare le criptovalute nell'ambito delle monete elettroniche, ma in realtà in comune con esse hanno solo la dematerializzazione del contante[153]. Infatti, le monete elettroniche vengono emesse in relazione a valuta reale corrisposta, e sono per legge riconvertibili o rimborsabili in valuta reale (direttiva 110/2009/CE). Il *bitcoin* non presenta questi requisiti, non viene emesso dietro corresponsione di valuta reale, ma viene "estratto" dai *miners* quale ricompensa per il loro servizio prestato alla rete. Pertanto neanche alla categoria di moneta elettronica è possibile inquadrare le criptovalute.

Riguardo le monete complementari, esse sembrano essere la tipologia di moneta che più si avvicina alle criptovalute, in quanto sono caratterizzate dall'essere prive di valore legale, emesse da privati ed accettate in via consensuale; pero, non è possibile convertirle in moneta legale, o scambiarle sul mercato secondario come fossero riserve di valore come invece è possibile fare con i *bitcoin*. Neanche la soluzione delle monete complementari pertanto sembra convincente.

Diverse sono state le pronunce delle autorità di vigilanza europee e non a riguardo. La Banca Centrale Europea nel "*Virtual currency scheme*[154]" pubblicato nel 2012 distingue le criptovalute in tre tipologie di «schemi»: 1) schemi di valuta virtuale chiusi, dove non c'è diretto contatto con l'economia reale[155], spendibili solo per acquistare beni virtuali e servizi offerti nell'ambito della *community* virtuali *online*[156]; 2) schemi di valuta virtuale unidirezionale che può essere acquistata con valuta reale ma non può essere riconvertita in tale forma[157]; 3) schemi di valuta virtuale bidirezionale, che può essere acquistata anch'essa con valuta reale ma può essere convertita in valuta reale e

---

[153] Per le «*palesi difformità di carattere tecnico e sostanziale, deve necessariamente ritenersi inapplicabile nei confronti delle valute virtuali la disciplina europea prevista in materia di moneta elettronica.*», RINALDI G., *op. cit.*, 270

[154] Consultabile al link: *https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf*

[155] «*non è previsto il suo acquisto o la sua la conversione in denaro reale e può, dunque, essere acquisita unicamente tramite attività "on-line" e può essere spesa solo per acquisti di beni virtuali o servizi offerti all'interno di una comunità virtuale*», BOCCHINI R., *op. cit.*, 35

[156] DANIELLI A., - DI MAIO D., - GENDUSA M., - RINALDI G., *bitcoin e criptovalute, funzionalità e rischi delle monete virtuali, InDiritto*, 2018, Milano, 20

[157] «*Esempi sono gli Amazon Coin, ma anche i punti delle carte fedeltà, per i quali è previsto anche l'acquisto con denaro corrente*», BOCCHINI R., *op. cit.*, 35

viceversa[158]. Quest'ultima è la tipologia più problematica in quanto il suo uso è identico a quello della valuta avente corso legale[159]. Nel 2015 sono stati pubblicati degli aggiornamenti al dossier del 2012, dove la BCE ha qualificato le valute virtuali come «*digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money*», ossia rappresentazioni digitali di valore non emessa da una banca centrale, istituiti di credito o istituti di moneta elettronica, che in alcuni casi possono essere usati come alternativa al denaro. Anche l'EBA, nel 2014[160] ha condotto un dossier definendo le valute virtuali similarmente a quanto affermato dalla BCE, soffermandosi specialmente sui rischi derivanti dal loro utilizzo e detenzione da parte dei consumatori, investitori e commercianti.

All'interno dei confini nazionali, la Banca d'Italia si è espressa nel 2015 sulla scia della pronuncia della BCE. A parte l'identica definizione di valuta virtuale nella parte riguardante la "rappresentazione digitale di valore", l'autorità di vigilanza italiana non manca di elargire una serie di raccomandazioni al pubblico. Essa infatti avverte come le valute virtuali non sono strumenti di pagamento elettronici[161], non hanno corso legale e non devono essere per legge accettate per l'estinzione delle obbligazioni pecuniarie.

---

[158] «*Esempi sono* Linden Dollars, Bitcoin*, e le valute complementari locali. Le monete virtuali del Tipo 3 possono essere distinte in due macrogruppi con differenti impatti sulla economia reale: le monete globali, con una circolazione "*worldwide*" e le monete locali, legate all'economia di comunità locali (dall'ambito comunale a quello nazionale*)», BOCCHINI R., *op. cit.*, 37

[159] MANCINI N., Bitcoin*: rischi e difficoltà normative*, in *Banca impresa società*, 2016, 127

[160] Consultabile al seguente link: *https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf*

[161] Vi sono opinioni contrastanti la posizione della Banca d'Italia, «*Tale impostazione è accolta nella risoluzione 72/E del 2016 dell'Agenzia delle Entrate, relativa al trattamento fiscale applicabile alle operazioni di acquisto e cessione di* bitcoin *ai fini dell'IVA e delle imposte dirette, nonché nel parere del Consiglio Nazionale del Notariato n. 3- 2018/B, concernente il quesito se il pagamento del prezzo di un immobile in* bitcoin *o in altra criptovaluta configuri una violazione delle norme in materia di limitazione all'uso del contante e/o di quelle in materia di indicazione analitica dei mezzi di pagamento. Entrambe le determinazioni, pur evidenziando le difficoltà di un inquadramento giuridico della fattispecie e riscontrando una eterogeneità di vedute, attribuiscono valore dirimente alle indicazioni contenute nella sopra ricordata.*», «*Tale paragone non può che suscitare forti perplessità. Si è visto infatti come tra moneta e criptovalute sussistano differenze di ordine sia giuridico, sia economico, che ostano ad una assimilazione di queste ultime al concetto di moneta. Questa è la posizione cristallizzata dal legislatore europeo che, giova ripetere, si è preoccupato di sancire espressamente che le valute virtuali non possiedono lo status giuridico di valuta o moneta, con la conseguenza per cui esse non possono essere ricomprese tanto nella categoria della moneta legale, quanto in quella della moneta estera.*», RINALDI G., *op. cit.*, 285

Inoltre, avverte come è possibile configurare la violazione di norme penali riguardanti l'esercizio abusivo di attività riservate ai soggetti individuati nel Testo Unico Bancario e nel Testo Unico Finanza (artt. 130, 131 TUB l'attività bancaria e l'attività di raccolta del risparmio; art. 131-*ter* TUB la prestazione di servizi di pagamento; art. 166 TUF, per la prestazione di servizi di investimento).

La V Direttiva antiriciclaggio 2018/843, pubblicata il 19 giugno 2018, è la fonte normativa più recente che fornisce una definizione di valuta virtuale, regolandone i prestatori di servizi di cambio valute e di portafoglio digitale. Si legge nel testo normativo che per valuta virtuale si intende «*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 definizione rappresenta una evoluzione di quella formulata nel 2015 dall'EBA.

Innanzitutto, viene ripresa la qualificazione di "rappresentazione digitale di valore", non emessa o garantita da una banca centrale o da un'autorità pubblica, ma viene anche specificato che non possiede la stessa valenza giuridica della moneta emessa da uno stato[162] (effetto liberatorio e solutorio delle obbligazioni). Inoltre, accuratamente viene definita come «*non necessariamente legata a una valuta legalmente istituita*», ricomprendendo cosi anche le cosiddette "*stable coins*" (monete stabili, dal prezzo stabile), criptovalute il cui valore viene associato ad una valuta fiat (in genere al dollaro statunitense) o anche ad una diversa criptovaluta.

Infine, a differenza della definizione dell'EBA dove viene posto in risalto che «*in alcune circostanze può essere usata come alternativa al denaro*», nella V Direttiva viene esplicitato che essa è accettata dai consociati come mezzo di scambio, e può essere trasferita e contabilizzata elettronicamente; non vi è uno specifico riferimento alla *blockchain* come mezzo di trasferimento e memorizzazione, pertanto non solo le criptovalute rientreranno nella definizione di moneta virtuale ma anche anche le diverse rappresentazioni di valori che non utilizzano la tecnologia *blockchain* per il loro funzionamento.

[162] SARZANA DI S.IPPOLITO F. – NICOTRA M, *op. cit.*, 158

Se usate e considerate come "monete", diversi sono i reati astrattamente configurabili soprattutto mediante la prestazione di servizi professionali relativi alle criptovalute. I reati di riciclaggio[163] e autoriciclaggio sono probabilmente quelli che più sono favoriti dalle criptovalute in virtù della loro anonimità e facilità di far disperdere le proprie tracce sulla *blockchain*[164]. Potrebbero essere anche configurabili come avvertito dalla Banca d'Italia nel 2015 reati relativi alla abusiva prestazione di servizi analoghi a quelli offerti da banche e prestatori di servizi di investimento.

Riguardo alla possibilità di configurare i reati di riciclaggio e autoriciclaggio descritti agli articoli 648-*bis* e 648-*ter* 1 c.p., il d.lgs. 25 maggio 2017, n. 90, modificante la precedente normativa antiriciclaggio e del contrasto del terrorismo del d.lgs. n. 231/2007, ha anticipato di fatto la V direttiva fornendo anch'esso una definizione di criptovaluta che ricalca quasi nella sua totalità quella presente nella direttiva europea. L'attenzione però, viene posta sull'estensione di determinati obblighi già gravanti sugli operatori del settore finanziario ai prestatori di servizi correlati alle valute virtuali ma anche alla modifica della disciplina riguardante i cambiavalute. I prestatori di servizi relativi all'utilizzo di criptovaluta vengono definiti come «*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*». Pertanto rientrano sia i cosiddetti *wallet provider*, che custodiscono le chiavi private che permettono la spendita delle criptovalute, sia gli *exchange*, piattaforme online (e anche *offline*, in quanto esistono dei veri e propri bancomat fisici) che permettono il cambio tra valute reali e non, e che spesso forniscono anche servizi di *wallet*.

L'art. 8 del d.lgs. n. 90/2017 ha modificato l'art. 17-*bis* (riguardante la disciplina dell'esercizio dell'attività di cambiavalute in via professionale), commi 8-*bis* e *ter* prevedendo l'obbligo di iscrizione in una sezione speciale registro dei cambiavalute ed estendendo di fatto le norme riguardanti la regolamentazione dell'attività dei cambiavalute. Così facendo il legislatore senza distinzioni in base al tipo di attività svolta, ha determinato l'applicazione delle stesse norme per tutti i prestatori di servizi

[163] «*i* Bitcoin *e le criptovalute potrebbero consentire ai riciclatori di spostare fondi illeciti in maniera più veloce, più economica e più discreta*», BOCCHINI R., *op. cit.*, 47

[164] DANIELLI A., - DI MAIO D., - GENDUSA M., - RINALDI G., *bitcoin e criptovalute, cit.,* 34

relativi all'utilizzo di valuta virtuale.[165]

Questa presa di posizione del legislatore con le sopra citate novità normative, fanno propendere per la tesi che considera le criptovalute alla stregua della "moneta" e di valuta vera e propria, in quanto l'estendere la normativa dedicata alla configurazione di reati relativi al cambio o alla decezione di denaro proveniente da illeciti si giustifica solo col considerare le criptovalute e il loro utilizzo alla pari con quello del denaro.

Ma non solo i reati sopra citati sono rilevanti, in quanto è possibile configurare reati relativi all'abusivismo di attività riservata a soggetti autorizzati[166]. L'abusiva attività bancaria e finanziaria (rispettivamente art. 131 e 132 d.lgs. 385/1993), però, sono di difficile configurazione in quanto i soggetti operanti nei servizi relativi alle valute virtuali non erogano finanziamenti, ma servizi di gestione di portafoglio digitale. Neanche l'art. 130 dello stesso Testo Unico è di semplice applicazione, poiché è richiesto dalla norma come definizione di "raccolta di risparmio", «*l'acquisizione di fondi con obbligo di rimborso*», escludendo quindi dal raggio applicativo della norma l'attività prestata dagli *exchange* che si limita a permettere il cambio di valuta virtuale in reale e viceversa. Ancora, i reati prescritti agli art. 131-*bis* e 131-*ter* del TUB, ossia l'abusiva emissione di moneta elettronica e l'abusiva attività di prestazione di servizi di pagamento, non sono di immediata applicazione per i prestatori di servizi. D'ostacolo alla loro configurazione vi è la mancata qualificazione delle criptovalute in moneta elettronica[167], pertanto i *miners* che nella pratica "coniano" le valute virtuali non sarebbero soggetti alla norma in questione. Inoltre, anche la definizione di servizio di pagamento permetterebbe di tener fuori dall'applicazione della norma gli *exchange* di criptovalute. Infatti, caratteristica fondante delle criptovalute è proprio la totale disintermediazione delle transazioni, le quali vengono gestite e validate dai partecipanti

---

[165] D'AGOSTINO L., *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del d.lgs. 90/2017*, in *Rivista di Diritto Bancario*, 1/2018, 14

[166] «*Si richiama, tuttavia, l'attenzione sul fatto che le attività di emissione di valuta virtuale, conversione di moneta legale in valute virtuali e viceversa e gestione dei relativi schemi operativi potrebbero invece concretizzare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati (artt. 130, 131 T.U.B. per l'attività bancaria e l'attività di raccolta del risparmio; art. 131-ter T.U.B. per la prestazione di servizi di pagamento; art. 166 T.U.F., per la prestazione di servizi di investimento)".*». BOCCHINI R., *op. cit.,* 35

[167] D'AGOSTINO L., *op. cit.*, 14

alla *rete peer to peer*. Come già ribadito, gli *exchange* si limitano a far confluire domanda e offerta di criptovaluta oppure a cambiare in valuta reale, ma in alcuni casi forniscono servizi di *wallet* semplicemente custodendo le chiavi pubbliche e private degli utenti, non potendosi cosi qualificare la loro attività come prestazione di servizi di pagamento. Si potrebbe obiettare che comunque i prestatori di servizi di *wallet* abbiano comunque un ruolo nell'invio e nella ricezione delle transazioni, ma in realtà proprio per come è strutturata e ideata una criptovaluta (come *bitcoin*), non necessita di un intermediario che autorizzi e gestisca i pagamenti; c'è anche da tener presente che attualmente appare forzato andare a considerare gli *exchange* e i *wallet provider* alla stregua di soggetti quali i prestatori si servizi di carte di credito o di valuta elettronica.

Per lo stesso motivo, infine, è problematica l'applicazione l'art. 166 del Testo Unico Finanza in quanto le definizioni che determinano l'ambito applicativo della norma non permettono di farvi rientrare le valute virtuali. Essendo elemento oggettivo della fattispecie la prestazione di servizi o attività di investimento di strumenti finanziari (definiti quest'ultimi all'art. 1, secondo comma T.U.F.) e non rientrando le valute virtuali in quest'ultima categoria, permetterebbero di tenere fuori dall'art. 166 gli operatori professionali nell'ambito delle criptovalute.

In conclusione, anche volendo considerare le valute virtuali come valuta, comunque non troverebbero immediata applicazione le norme a tutela del mercato monetario e dei risparmiatori. Urgerebbe una riforma legislativa solo se l'attività prestata dagli operatori professionali raggiungesse volumi consistenti e coinvolgesse interessi equivalenti a quelli che ispirano le attuali fattispecie penali del TUB e TUF. Infatti, nel caso del riciclaggio, l'intervento del legislatore è andato verso la direzione di inclusione delle valute virtuali nell'ambito applicativo delle norme già esistenti perché le lesioni ai beni giuridici tutelati dalle stesse a causa di determinati (ab)usi delle valute virtuali è diventata ormai pari a quelle determinate dallo scorretto uso di valuta reale.

A parte le fattispecie penali astrattamente configurabili, le valute virtuali comportano utilizzi illeciti anche a fini fiscali e sono senza dubbio sfruttabili da organizzazioni terroristiche. Ricevere e inviare pagamenti in *bitcoin* potrebbe essere

una semplice modalità di evasione fiscale[168], in quanto sarebbe ancora più comodo effettuare operazioni "in nero" sfruttando l'anonimato (pseudonimia) delle criptovalute. Inoltre, proprio a causa della transnazionalità e della difficile tracciabilità, organizzazioni criminali e terroristiche sicuramente utilizzano i *bitcoin* per acquistare e vendere merce di cui è proibito il commercio, anche attraverso i *market place* del *deep web*, dove è possibile acquistare merci illegali nella più totale riservatezza.

Riassumendo, la *blockchain* nella declinazione di moneta è quella che più ha applicazioni pratiche e ha avuto un grande sviluppo e diffusione tra gli individui. Essa però è anche l'uso della *blockchain* che più comporta problematiche criminogene su vari fronti, derivanti tuttavia, dal cattivo uso fatto dall'uomo e non dalla tecnologia in quanto tale. Anche l'Euro e il Dollaro vengono utilizzati per evadere le imposte, riciclare denaro e acquistare armi o droghe, ma di fatto nessuno ha mai pensato di rendere le attuali valute illegali. Basterebbe integrare le attuali normative in modo tale da non lasciar fuori queste nuove "valute" e di continuare a perseguire il contrasto al riciclaggio e terrorismo semplicemente tenendo in considerazione queste nuove modalità di configurazioni di tali reati e non.

1.11 Oltre i *bitcoin*: *Ethereum* e le altre criptovalute

Sebbene la criptovaluta più diffusa e conosciuta sia il *bitcoin*, nel corso degli ultimi anni sono proliferate decine di nuove criptovalute ognuna con caratteristiche peculiari. Tra queste, la criptovaluta "*Ether*" e la relativa *blockchain* chiamata "*Ethereum*" è la più utilizzata dopo i *bitcoin*[169]. Nata grazie ad una campagna di *crowfunding* nel 2014[170]

---

[168] «*la natura decentralizzata delle reti di valute virtuali e l'assenza di regolamentazione fanno sì che il trattamento fiscale delle valute virtuali possa presentare incertezze e lacune, a cominciare dall'individuazione dello Stato beneficiario, dando vita a implicazioni imprevedibili per i soggetti coinvolti.*», BOCCHINI R., *op. cit.*, 47

[169] «*Ethereum is an innovative blockchain-based virtual machine and Cloud 2.0 platform that comes with an embedded programming language that allows users to create their own applications that run on top of blockchain architectures. Ethereum enables user-created smart contracts and aims to build an all- purpose technology platform, on which transaction-based application concepts may be built. According to a recent report by Eurelectric, the Union of the electricity industry, more than 1000 projects are currently using Ethereum. Many startups are using Ethereum-based coins and cryptocurrencies for Initial Coin Offerings (ICOs), as a means to raise funding*» ANDONI M., - ROBU V., - FLYNN D., - ABRAM S., - GEACH D., - JENKINS D., - MCCALLUM P., - PEACOCK A., *op. cit.*, 147

[170] *https://blog.ethereum.org/2016/02/09/cut-and-try-building-a-dream/*

lanciata dal suo creatore Buterin, deve il suo successo alla circostanza che la *blockchain* di *Ethereum* è specificatamente progettata per far funzionare gli *smart contracts*, e gli *Ether* sono le "monete" scambiabili sulla piattaforma e che permettono l'esecuzione dei "contratti". Similarmente alla *blockchain* di *bitcoin*, è anch'essa una *blockchain permissionless*, *open source*, e distribuita che utilizza la *proof of work* per il *mining*. Tra le diverse differenze prettamente tecniche vi è il tempo di creazione dei blocchi quindi della loro conseguente validazione molto più rapido (circa 12 secondi contro i 10 minuti di *Bitcoin*), ma come già anticipato ciò che sostanzialmente rende *Ethereum* innovativo rispetto al *bitcoin* è la possibilità che offre ai programmatori di dar vita a *smart contracts* sfruttando la *blockchain* e le garanzie di certezza e automaticità dell'esecuzione del "contratto".

Un'altra criptovaluta che presenta profili interessanti e che di discosta dai principi teorici alla base dei *bitcoin* è *Ripple*. Essa è una criptovaluta gestita da una società privata (è dunque non decentralizzata), concepita per essere utilizzata da banche e da intermediari finanziari per la gestione dei pagamenti effettuata dai propri clienti, in pieno contrasto con l'idea di creare un sistema di pagamento sicuro in assenza di ente garante. Più che rappresentare, nella mente dei suoi creatori, un sistema di pagamento alternativo a quello gestito dalle banche, essa è un *upgrade* dell'attuale sistema finanziario[171]. *Ripple*, pertanto, è un esempio di come sia fondamentale focalizzarsi su come viene utilizzata e concepita una nuova tecnologia; pur discostandosi dai principi teorici che hanno portato alla creazione di sistemi di pagamento alternativi, essa rappresenta una valida declinazione della *blockchain* che essendo garantita da enti autorevoli, potrebbe garantire più controllo e sicurezza del sistema e prevenire usi per scopi illeciti.

Una criptovaluta che per come è stata progettata sembra prestarsi meglio dei

[171] *https://coincentral.com/ripple-vs-bitcoin/*

bitcoin ad usi illeciti è *Monero*[172]. Creata nel 2014[173], essa viene pubblicizzata enfatizzando l'attenzione per la *privacy* e la sicurezza. Infatti, è una criptovaluta non tracciabile e anonima, non potendo in alcun modo determinare se una transazione è stata realmente effettuata o tra chi è stata effettuata. Questo risultato viene ottenuto tramite adozioni tecnologiche differenti rispetto al *bitcoin*, dove le transazioni sono tracciabili ed è possibile almeno in linea teorica, risalire all'identità dei soggetti della transazione. *Monero* quindi è un esempio di come, a differenza di *Ripple*, sia stato sviluppato il funzionamento della *blockchain* per finalità comunque non trasparenti, seppure giustificate dall'esaltazione dei valori della *privacy* e della sicurezza delle transazioni.

La panoramica delle criptovalute non si esaurisce con quelle esposte in questo contesto in quanto sono più di duemila quelle attualmente "circolanti"[174], ma in linea di massima ognuna presenta caratteristiche analoghe al *bitcoin* da cui si differenziano o per la velocità delle transazioni, o per la minor dimensione dei dati o per il minor costo del *mining*. Nel proseguo della trattazione si farà riferimento a *Bitcoin* e al suo funzionamento, ma è bene tenere in considerazione l'esistenza di altre criptovalute che assolvono nella maggior parte dei casi la stessa funzione del *bitcoin* ed *Ethereum* (rispettivamente mezzo di pagamento e piattaforma per l'esecuzione di *smart contracts*).

1.12 Conclusioni

Nel corso dei precedenti paragrafi sono state analizzate diverse questioni riguardo la tecnologia *blockchain* e l'inquadramento giuridico dei suoi eterogenei utilizzi.

---

[172] Oltre ai possibili utilizzi illeciti, *Monero* presenta delle caratteristiche addirittura vantaggiose per quanto riguarda la conformità delle disposizioni contenute nel GDPR (Regolamento UE 2016/679), infatti «*Attualmente, le uniche criptomonete ad apparire potenzialmente conformi alle disposizioni del GDPR sono le c.d.* privacy coin *(come ad esempio Monero), che sembrano in grado di garantire un effettivo anonimato agli utilizzatori, in quanto non conservano all'interno della propria* blockchain *alcuna "*personally identifiable information*" (vale a dire informazioni che consentono di individuare l'utente all'interno del sistema)*», RINALDI G., *op. cit.,* 267

[173] *https://ww.getmonero.org/resources/about/*

[174] *https://coinmarketcap.com/*

I *token*, distinti nelle varie tipologie, rappresentano probabilmente la declinazione della blockchain più incerta dal punto di vista della funzione economica e delle norme ad esse applicabili. Non è ancora possibile con certezza determinare *ex ante* la regolamentazione rilevante per ogni tipo di *token* ma le autorità nazionali, europee ed extra-europee stanno cercando di delineare dei criteri di inquadramento giuridico per non lasciare il fenomeno della diffusione dello scambio e utilizzo dei *token* completamente privo di norme a tutela del mercato e dei consumatori.

Le criptovalute, in virtù della loro attitudine ad essere utilizzate come strumento alternativo alla moneta avente corso legale, si prestano a diversi utilizzi illeciti. Nei *dark markets* il *bitcoin* e in generale le criptovalute sono le uniche "monete" scambiate per la vendita e acquisto di merci illegali poiché garantiscono anonimità (*recitus,* pseudonimità) e riservatezza; il riciclaggio di denaro è anch'esso favorito dalle caratteristiche intrinseche delle criptovalute, soprattutto da quelle progettate appositamente per assicurare un livello di riservatezza ulteriore rispetto comune protocollo *Bitcoin* (*Monero* su tutte). Riguardo l'attività dei prestatori di servizi nell'ambito delle criptovalute, le attuali norme penali contenute nel TUB e TUF non sono abbastanza capienti tali da ricomprendere nell'elemento oggettivo anche l'utilizzo di valute virtuali.

Infine, l'apprezzabile tentativo del legislatore italiano di dare validità giuridica ai registri distribuiti e agli *smart contracts* è di per sé da accogliere con favore ma con l'auspicio di una ragionato e coscienzioso emendamento alle attuali norme in vigore.

CAPITOLO II

LE CRIPTOVALUTE E PROFILI DI RILEVANZA PENALE

SOMMARIO: 2. Le caratteristiche delle criptovalute e il loro utilizzo a fini illeciti. - 2.1 Il "*cyber*-criminale", aspetti criminologici. - 2.2 I c.d. "*criminal smart contracts"*. - 2.3 Il c.d. "*cyberlaundering*". - 2.3.1 (*Segue)* Il c.d. *"mixing"*. - 2.4 I reati contro il patrimonio: I delitti di Riciclaggio, Impiego di denaro, beni o altra utilità di provenienza illecita e l'autoriciclaggio (Artt. 648-*bis*, *ter*, *ter*.1 c.p.). - 2.4.1 (*Segue)* Il riciclaggio mediante criptovalute e le relative problematiche di diritto penale parte generale. - 2.5 La V Direttiva antiriciclaggio e il D.lgs. 25 maggio 2017, n. 90. - 2.6 L'abusivismo bancario e finanziario. - 2.7 I reati tributari. - 2.8 Conclusioni.

2. Le caratteristiche delle criptovalute e il loro utilizzo a fini illeciti

Le criptovalute, in virtù delle loro caratteristiche intrinseche di funzionamento e di struttura, possono facilmente essere strumentalizzate per finalità illecite.

Le soluzioni tecnologiche adottate in occasione dell'ideazione del protocollo *Bitcoin* per garantirne la *privacy* e la sicurezza sono state di fatto strumentalizzate per perseguire finalità diverse da quelle che hanno ispirato il concepimento di una valuta decentralizzata basata sulla tecnologia *blockchain*: si pensi ad esempio alla crittografia, che nasce per garantire la riservatezza delle comunicazioni e che viene utilizzata nel protocollo *Bitcoin* per assicurare la sicurezza delle transazioni (ma anche dai sistemi di *home banking* e *Paypal*[175]), e per impedire interventi abusivi o intercettazioni[176].

Sennonché, individui malintenzionati possono benissimo sfruttare la crittografia e la anonimità delle transazioni per occultare il contenuto delle transazioni sia a terzi che alle autorità investigative (non svelando, ad esempio, la chiave privata del proprio *address,* oppure l'identità dei soggetti coinvolti nello scambio di criptovaluta).

[175] Servizio online di metodo di pagamento di moneta elettronica

[176] PICOTTI L., *Profili penali del* cyberlaundering*: le nuove tecniche di riciclaggio* in *Rivista trimestrale diritto penale economia*, n. 3-4/2018, 606

Infatti, nonostante i sostenitori del *bitcoin* affermino che nel protocollo non ci sia anonimità ma una "pseudo-anonimità", dal momento che ogni *address* bitcoin è rappresentato da una stringa alfanumerica, può fondatamente sostenersi che una delle caratteristiche peculiari delle criptovalute è l'anonimità sostanziale perché non comporta una sicura tracciabilità della persone coinvolte nella transazione[177].

Non a caso, alcuni Autori[178] già nel 1992 prevedevano che l'uso di valuta anonima avrebbe dato vita ai c.d. "crimini perfetti".

La sostanziale anonimità del sistema *Bitcoin* è favorita dall'assenza di un ente centrale: se normalmente le banche verificano l'identità dei propri clienti e correntisti, nel caso delle criptovalute non è necessario la previa identificazione degli utenti per ricevere o inviare *bitcoin*.

È pur vero che attualmente la maggior parte degli *exchangers,* in linea con le normative in tema antiriciclaggio, hanno adottato procedure di previa verifica della clientela, ma, essendo espletate interamente online, tali procedure sono facilmente eludibili.

Non mancano, invero, obiezioni secondo cui l'intero registro della *blockchain*, essendo lo storico delle transazioni pubblico e difficilmente modificabile, sarebbe un sistema di tracciamento ineccepibile. Tali obiezioni non tengono tuttavia conto del fatto che di pubblico vi è solo la *transaction chain* degli importi e degli *address* che hanno inviato e ricevuto i *bitcoin* (nel caso di *Monero* o di altre criptovalute come *Dash* o *Zcash,* viene occultato anche l'importo[179]), ma non è possibile risalire facilmente alla vera identità degli utenti, tenuto anche conto che è possibile utilizzare un numero illimitato di *addresses* e che vi sono dei servizi di *mixing* che non fanno altro che far perdere le tracce delle transazioni sulla *blockchain*.

Da non dimenticare, poi, che vi sono ulteriori *escamotage* che permettono l'utilizzo delle criptovalute in maniera tale da eludere le investigazioni da parte delle autorità competenti. Tra questi merita una particolare menzione l'uso dei VPN[180] (*virtual private network)* e del *browser* TOR.

---

[177] STURZO L., *Bitcoin e riciclaggio 2.0* in *Diritto penale contemporaneo*, n. 5/2018, 21

[178] SOLMS S., - NACCACHE D., *On blind signatures and perfect crimes* in *Computer Security* n.11, 1992, 583

[179] V. *Supra* cap. 1, § 1.11

[180] «*Chiunque sia in possesso di un computer e di una connessione internet, può navigare in rete*

Come sappiamo, ogni volta che ci connettiamo ad *internet* il nostro *device* viene "identificato" e localizzato attraverso l'indirizzo IP. Le connessioni VPN sfruttano la crittografia per mascherare il proprio indirizzo IP e proteggere i dati trasmessi, permettendo cosi una ancor più difficile identificazione e tracciabilità del soggetto che invia o riceve *bitcoin*. Il *browser* TOR ("*the Onion Router")*, invece, utilizza un tipo di cifrazione "a strati", in modo tale da garantire la completa riservatezza dei dati inviati, protetti dai vari *layers* di cifratura[181].

Tali caratteristiche delle valute virtuali hanno attratto l'attenzione dei criminali, a causa delle elevate potenzialità di movimentare ingenti quantità di denaro in modo anonimo e sicuro: uno strumento formidabile per la ripulitura dei proventi illeciti. La strumentalizzazione per fini di riciclaggio è, invero, soltanto uno dei possibili impieghi per fini criminosi, dovendosi infatti dar conto anche di altri utilizzi quali ad esempio a fini di scambio sui *marketplace online*[182] adibiti alla vendita di beni il cui commercio è vietato (droga, armi, materiale pedopornografici e *virus* informatici *in primis*), o per eludere la normativa fiscale.

Di conseguenza, è possibile affermare che vengano utilizzate tutte le volte in cui vi sia la necessità dell'utilizzo di un mezzo di scambio anonimo che non sia il denaro

---

utilizzando il proprio indirizzo IP, ossia un indirizzo numerico che serve ad identificare e localizzare in maniera univoca ogni computer o dispositivo connesso ad una rete. Sebbene sia impossibile navigare senza un indirizzo IP, è possibile trovare nel web strumenti di navigazione che consentano di camuffare il proprio indirizzo IP, ottenendo un massimo livello di anonimato, in maniera tale che il proprio computer risulti collocato in un'altra città, in un altro Paese o, addirittura, in un altro continente (esempi sono rappresentati dai programmi CyberGhost VPN o TunnelBear)», SIMONCINI E., *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, in *Rivista trimestrale di diritto penale dell' economia*, n. 4/2015, nota n.53, 908

[181] La sua ideazione nasce per poter garantire la *privacy* degli utenti, ma anche la loro sicurezza. Esso viene infatti utilizzato dai giornalisti per poter comunicare con dissidenti e *whistleblowers,* oppure viene utilizzato da organizzazioni non governative per eludere le restrizioni dovute alla censura che ancora esistono in alcuni paesi. Anche TOR quindi è stato concepito ispirato dai migliori propositi (venne inventato dal laboratorio di ricerche navali statunitense), ma oramai viene sfruttata la sua riservatezza per ostacolare in maniera efficace qualsiasi attività di localizzazione o di individuazione del soggetto connesso alla rete *internet*.

[182] Esemplare è il caso di *silkroad* https://www.repubblica.it/tecnologia/2015/05/30/news/ergastolo_per_il_fondatore_di_silk_road-115620536/

avente corso legale (nel caso dei *ransomware*[183] e in particolare di *wannacry*[184] , le criptovalute vengono usate come strumenti sostituitivi del denaro in quanto la loro difficile tracciabilità è garanzia di impunità per i ricattatori). Inoltre, seppur possa sembrare inverosimile, le caratteristiche sovraesposte delle criptovalute hanno portato a sempre più frequenti attacchi da parte dei "*cyber*" criminali nei confronti dei detentori delle valute virtuali. Proprio perché anonime, di difficile tracciabilità e indissolubilmente legate al "possesso" delle chiavi private, l'obiettivo degli attacchi è proprio il furto delle suddette chiavi custodite dagli *exchangers* o dai *wallet providers* per sottrarre i *bitcoin* ai legittimi possessori[185].

Riassumendo, l'anonimità (*recitus,* pseudonimità), la difficile tracciabilità e la riservatezza rendono le criptovalute ideali per essere utilizzate per finalità illecite. Nel corso dei successivi paragrafi verranno meglio analizzate le rispettive caratteristiche in relazione ai reati configurabili attraverso il loro utilizzo.

Il *focus* dell'attenzione verrà posto in particolare sui reati contro il patrimonio e l'ordine economico (riciclaggio in particolare), i reati introdotti a tutela dell'ordine pubblico presenti nel T.U.F e T.U.B.

---

[183] «*Le estorsioni on-line vengono compiute attraverso attacchi DDoS (Distribuited Denial of Service) e consistono nell'interruzione dei servizi telematici offerti dalle diverse agenzie e società (quali siti web, programmi informatici, mail, ecc.) accompagnata da una richiesta di denaro sotto forma di bitcoin per poter ripristinare il servizio e porre fine all'attacco informatico.*», SIMONCINI E., *op. cit,* nota n.59, 909; ACCINNI G., P., *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)* in *Archivio Penale* n. 1/2018, 10, secondo cui l'utilizzo di *bitcoin*, *Monero*, e *ZChash* è in crescita come valore di scambio nell'ambito della commissione di attacchi DDoS, *«la cui peculiarità è quella di far esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai client , ad esempio un sito web, fino a renderlo non più in grado di erogare il servizio al soggetto richiedente*»

[184] ACCINNI G., P., *op. cit*., 9, secondo cui l'attacco c.d. "*WannaCry"*, profusosi a partire dal maggio 2017 e progettato specificatamente per colpire i computer con sistema operativo *Microsoft Windows*, consisteva nella criptazione dei *file* memorizzati sull'*hard disk* con la conseguente richiesta di un "riscatto" in *bitcoi*. I computer infettati ammontano a duecentrotrentamila, sparsi per circa 150 paesi.

[185] A «*mero titolo di esempio è così possibile citare il c.d. caso Bitfinex, un virtual currecies exchanger con sede ad Honk Kong che in data 2 agosto 2016 ha subito il furto di monete virtuali per un controvalore complessivo pari a 72 milioni di dollari. Ancora più eclatante il caso dell'exchanger Mt-Gox, sino al 2014 uno dei maggiori exchanger a livello planetario, a cui gli degli hacker avrebbero sottratto n. 744.408 Bitcoin, equivalenti a 350 milioni di dollari statunitensi. Non meno emblematico anche l'attacco perpetrato ai danni del progetto di raccolta fondi "The Dao", nel corso del quale sono stati sottratti dagli hacker più di 152 milioni di dollari. Il furto è stato perpetrato nel corso di una Ico (Initial coin offering), ossia quell'operazione attraverso cui un'azienda creatrice di una nuova valuta virtuale la offre in vendita al pubblico per la prima volta»,* ACCINNI G., P., *op. cit.,* 10

Infine, verrà affrontata una panoramica dell'inquadramento delle criptovalute ai fini fiscali e la relativa possibilità di considerarle nell'alveo dei redditi imponibili.

2.1 La figura del "cyber-criminale". Aspetti di carattere criminologico

La commissione di reati attraverso l'utilizzo delle criptovalute è facilitato non solo dalle caratteristiche oggettive del mezzo tecnologico – che di per sé rilevano una natura criminogena particolarmente accentuata – ma anche dalla circostanza della assenza di materialità della condotta. Un reato commesso *online* non è criminologicamente sovrapponibile a i crimini commessi interamente *offline*. Vi sono diversi elementi che da un punto di vista criminologico caratterizzano i *cybercrimes,* quali la percepita anonimità, la mancanza di un contatto fisico o quantomeno visivo con le vittime, l'annullamento dei confini geografici, ed anche le differenti norme giuridiche nelle diverse giurisdizioni[186].

La percepita anonimità porta il soggetto agente alla convinzione che la sua identità sarà molto difficilmente scoperta, e questo va ad inficiare la funzione preventiva e dissuasiva delle norme penali. L'individuo nella rete si cela dietro diversi *alter ego*[187] indossando una maschera, o meglio, più maschere a cui corrispondono comportamenti differenziati La sanzione penale incorporata nel precetto normativo non può efficacemente esplicare la propria funzione se l'individuo è convinto di non essere scoperto in tempi rapidi, di non essere sottoposto a processo e di subire la pena.

Sotto un altro profilo la depersonalizzazione delle vittime, invece, comporta che il criminale non venendo a contatto diretto con la vittima, non si renda conto effettivamente del danno causato alla stessa. In questo modo il disvalore sociale del proprio comportamento viene avvertito in misura molto minore rispetto ad un crimine commesso *offline*, e tutto ciò fa sì che la commissione di atti illeciti sia facilitata proprio dall'assenza di remore morali.

Ugualmente rilevante è la transnazionalità degli illeciti commessi in rete. La consapevolezza di agire in danno di vittime locate a migliaia di chilometri di distanza

---

[186] STALANS L. J., - DONNER C., M., *Explaining why cybercrime occurs: criminological and psychological theories* in *Cyber Criminology,* Berlino, 2018, 36

[187] PICOTTI L., *Cybercrime* a cura di CADOPPI A., - CANESTRARI S., - MANNA A., Milano, 2019, 56

aumenta la depersonalizzazione delle vittime ed inoltre induce il criminale a sentirsi immune da qualsiasi forma di repressione, soprattutto se agisce in paesi dove le autorità requirenti sono poco o per nulla efficaci.

Da sottolineare, poi, è lo smisurato bacino di potenziali vittime raggiungibili a bassissimi costi che la rete offre rispetto ai crimini *offline* tanto che si può sostenere che una caratteristica peculiare dei *cybercrime* è la sproporzione tra i costi degli "attacchi" e i danni procurati e i profitti accumulati, il che determina una maggiore appetibilità rispetto alle stesse condotte che l'individuo potrebbe commettere in modo "analogico".

Questo fa sì che la commissione di un reato *online* è molto conveniente, supportata dalla anonimità e dalla difficile tracciabilità. La transnazionalità determina anche difficoltà a livello di cooperazione giudiziaria nei casi in cui gli attacchi vengano sferrati da paesi poco disposti a collaborare, e comunque le lungaggini burocratiche degli *arrest warrant* o di circolazione dei mezzi di prova sono tutte a vantaggio dei criminali[188].

Bisogna tener presente anche le difficoltà che vi sarebbero nei processi contro i "cybercriminali" nel provare «al di là di ogni ragionevole dubbio» la loro colpevolezza. Ammesso che si venga localizzati e identificati, ad esempio dopo aver determinato l'indirizzo IP da cui è partito l'attacco, non vi è la certezza sufficiente per affermare la colpevolezza del soggetto ricollegato a quel determinato indirizzo IP.

Riassumendo, in virtù delle peculiarità dei reati commessi attraverso *internet*, sono altrettanto singolari le questioni criminologiche che ne determinano una più facile commissione di reati soprattutto da parte di persone insospettabili[189], che nella "vita *offline*" non commetterebbero alcun illecito; nel mondo virtuale, però, i suddetti individui sono invece più propensi a porre in essere comportamenti criminogeni in virtù delle ragioni poc'anzi esaminate[190].

---

[188] STURZO L., *Bitcoin e riciclaggio 2.0* in Diritto penale contemporaneo n. 5/2018, 22

[189] *Contra*, «*I delinquenti che popolano tale settore non possiedono caratteristiche psicologiche (anomale) inquadrabili in particolari tassonomie, ma competenze specifiche al passo con il progresso tecnologico*» NADDEO M., N*uove frontiere del risparmio, bitcoin exchange e rischio penale* in *Diritto penale e processo*, n. 1/2019, 100

[190] «*L'incalzare dell'evoluzione tecnologica esercita una penetrante forza attrattiva nei confronti di numerosi comportamenti delittuosi, che, sganciatisi dai contesti sociali tradizionali, ricercano concrete possibilità di attuazione nella realtà virtuale, conservando - peraltro - struttura e finalità identiche*

2.2 I c.dd. "*criminal smart contracts*"

Per un quadro più completo è necessario considerare l'esistenza di particolari modalità di commettere reati sfruttando la *blockchain*. In particolare, peculiare è il divamparsi del fenomeno dei c.d. "*criminal smart contracts*". Come tutte le nuove soluzioni tecnologiche, anche gli *smart contracts* si prestano ad essere utilizzati per fini illeciti; il *focus* dell'attenzione, però, si concerterà in particolare sulla piattaforma di *Ethereum* piuttosto che sul protocollo di *Bitcoin*. Quest'ultimo ha infatti portato alla diffusione dei *ransomware*, del *cyberlaundering* e dei *dark markets*[191], ma *Ethereum* offre funzionalità inedite, ossia quella di implementare gli *smart contracts* nella *blockchain*.

La possibilità della commissione di reati mediante *smart contracts*[192] non è una questione ovvia, ma è importante prima verificare se essi si prestano ad essere utilizzati come mezzo di commissione di atti illeciti. Due sono le questioni da considerare[193]: se l'utilizzo dello *smart contract* garantisca sia la commissione del crimine, sia un pagamento al suo autore; se lo *smart contracts* sia "pratico", ossia se non necessiti per essere eseguito di una notevole quantità di energia computazionale che possa rendere il suo utilizzo non conveniente.

Gli atti illeciti che possono essere messi in atto tramite uno *smart contract* sono la rivelazione e vendita di documenti secretati, il furto delle chiavi private (ad es. di un *wallet* di valuta virtuale), e i c.d. «*Calling card crimes*»[194] ("crimini con biglietto da visita"), che si caratterizzano per la circostanza che la loro esecuzione ha effetto nella realtà *offline*.

Gli *smart contracts* permettono di poter scambiare valute virtuali automaticamente, azzerando così il rischio che una parte del contratto si tiri indietro e annulli il pagamento. Inoltre, comportano una interazione minima tra le parti evitando così il

---

rispetto alle ipotesi di reato «classiche»; ciò non esclude che nella Rete sia individuabile un gruppo di illeciti realizzati con maggiore frequenza statistica in virtù delle potenzialità offerte dal mezzo telematico», RUGGIERO F., *Momento consumativo del reato e conflitti di giurisdizione nel* cyberspazio, in *Giurisprudenza di merito* n.1/2002, 255

[191] JUELS A., - KOSBA A., - SHI E., *The ring of gyges: investigating the future of criminal smart contracts,* 283, *http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf*

[192] V. *Supra* cap. I, § 1.3

[193] JUELS A., - KOSBA A., - SHI E., *op. cit.,* 284

[194] JUELS A., - KOSBA A., - SHI E., *op. cit.,* 285

rischio di essere tracciati o monitorati da parti di terzi. Infine, permettono di utilizzare come *input* del contratto fonti esterne al sistema degli *smart contracts* come ad esempio bollettini meteo o listini ufficiali dei prezzi delle azioni.

Queste funzionalità possono però facilitare la commissione di reati, come nel caso della scarsa interazione delle parti che rende ancora più difficile per le autorità competenti il monitoraggio di comportamenti sospetti. L'utilizzo di dati esterni come *input* degli *smart contracts*, invece, comporta la possibilità di allargare il relativo raggio di azione non solo alla realtà virtuale *online* ma anche alla realtà materiale (omicidi su richiesta, terrorismo, incendi dolosi ecc.).

I *criminal smart contracts* adibiti alla rivelazione di informazioni segrete danno vita a veri e propri mercati di informazioni riservate riguardanti ad esempio segreti governativi o disegni industriali. Lo *smart contracts* viene programmato in modo tale che una volta corrisposto il prezzo, viene automaticamente decriptata l'informazione riservata per un determinato periodo di tempo. Altri tipi di simili *smart contracts* invece sono programmati per decriptare pubblicamente solo una parte delle informazioni a seguito di un previo modesto pagamento, e sole se il contenuto è interessante per gli utenti viene decriptato l'intero messaggio; altrimenti, viene rimborsato il contributo iniziale. Questo tipo di *smart contracts*, pertanto, permette l'efficace rivelazione di informazioni riservate dando la possibilità ai detentori delle stesse di monetizzare la *disclosure* nella più completa anonimità e semplicità.

Un'altra tipologia di *criminal smart contracts* è il c.d. «*key compromise criminal smart contract*»[195], programmato in modo tale da trasferire automaticamente all'autore del furto una prestabilita quantità di criptovaluta a seguito della consegna della chiave privata "rubata" ad un determinato soggetto. È di fatto un contratto che sollecita e commissiona il furto di chiavi private. Una criticità di questo *smart contract* è che la vittima o *target* del furto è visibile pubblicamente, pertanto è possibile intraprendere contromisure efficaci in modo tale da neutralizzarne gli effetti.

Infine, i c.d. *calling card crimes* mediante *smart contracts* sono probabilmente tra i più allarmanti in quanto dal loro utilizzo può scaturire la commissione di reati particolarmente gravi, come gli omicidi su commissione. Il loro funzionamento si basa

[195] JUELS A., - KOSBA A., - SHI E., *op. cit.,* 286

sulla pubblicazione dello *smart contracts* per l'assassinio di un determinato individuo. L'aspirante omicida inserisce come *input* i dettagli dell'omicidio (data, ora e luogo) e l'esecuzione automatica del contratto (e la conseguente corresponsione del compenso pattuito) avrà luogo solo dopo aver verificato sulla base di un *data feed*[196] che effettivamente quel soggetto è stato assassinato con le modalità inserite dall'assassino come *input*. È interessante notare che dopo aver pubblicato il contratto, nessuna interazione prende luogo tra il (futuro) assassino e chi l'ha commissionato; ciò rende estremamente difficile tracciare i due soggetti in base al loro traffico di dati (in questo caso inesistente). Nelle altre possibili applicazioni di questo tipo di *smart contracts* rientrano la commissione di aggressioni, rapimenti, sabotaggi e attacchi informatici o terroristici; praticamente tutto quello che può essere verificato e contenuto in un *data feed* può essere designato come obiettivo dello *smart contract*.

Una contromisura che può efficacemente contrastare il funzionamento automatico di questi *software* è quello di alterare i dati contenuti nei *data feed* in modo tale da provocare l'automatica esecuzione del contratto senza che sia accaduto realmente l'evento. Inoltre, a differenza delle semplici transazioni sulla *blockchain* che non rivelano nulla di per sé illecito, i *calling-card crimes* di fatto sono auto-incriminanti, e per essere efficaci debbono essere adeguatamente pubblicizzati e portati a conoscenza. Si è pertanto ipotizzato di dar vita a *community* volte a vigilare sulla natura degli *smart contracts* pubblicati e affinché vengano eliminati dalla rete. Oppure, è stato proposto di affidare ai *miners* il compito di omettere le transazioni quando queste sono state segnalate come scaturenti da contratti illeciti. Infatti, nel caso in cui il *miner* fosse pienamente a conoscenza dei contenuti e dei propositi degli *smart contracts* da lui inseriti nella *blockchain*, si potrebbero configurare ipotesi di concorso nel reato altrui, sotto forma di agevolazione.

Infine, è stata anche prospettata la possibilità di stabilire che una determinata autorità o un numero sufficiente di utenti abbia la discrezionalità di rimuovere uno specifico *smart contract* dalla *blockchain*. Questa soluzione è la più problematica in quanto potrebbe non essere pacificamente accettata dagli utenti partecipanti alla rete

[196] *https://it.wikipedia.org/wiki/Feed*

blockchain in quanto l'idea di fondo della *blockchain* e del principio del consenso è che non vi è nessun ente sovraordinato ma la fiducia è riposta negli stessi utenti.

Vi è da considerare, per una trattazione più completa, non solo i casi in cui gli *smart contracts* vengano programmati con l'esplicita finalità di commettere o facilitare reati, ma anche i casi in cui, dopo aver elaborato uno *smart contract* senza l'intenzione di commettere alcun delitto, un crimine venga effettivamente commesso in seguito ad un errore di programmazione o di risultati inaspettati o non previsti. Infatti, gli *smart contracts* sono auto-eseguibili, pertanto una volta attivato non vi è più la discrezionalità dell'uomo sull'esecuzione del contratto. In questi casi saranno particolarmente rilevanti le questioni sulla previsione dell'evento e l'incidenza del dolo nella forma eventuale.

In conclusione, anche gli *smart contracts* permettono la commissione di attività illecite che possono configurare reati estremamente gravi, e l'utilizzo delle criptovalute per lo scambio di riserve di valore permette di agire nel pieno anonimato e ne facilita l'esecuzione rispetto ai tradizionali metodi di pagamento in valuta avente corso legale.

2.3 Il c.d. "*cyberlaundering*"

Il *cyberlaundering* è un fenomeno che ha preso piede negli ultimi anni, e rappresenta la «*nuova frontiera del riciclaggio*»[197] in quanto sfrutta la «*polverizzazione*» del denaro via *internet* e la conseguente possibilità di trasferirne ingenti somme sotto la protezione dell'anonimità e la difficile tracciabilità[198].

---

[197] SIMONCINI E., *op. cit.*, 897

[198] «*Tale fenomeno esplose a livello internazionale verso la fine degli anni '90 inseguito al crescente utilizzo delle nuove tecnologie dell'informazione e della comunicazione (ICT-Information and Communication Technology) nel settore dell'attività bancaria e finanziaria, che consentirono di compiere trasferimenti di ricchezza a carattere transfrontaliero eliminando l'intervento dei tradizionali intermediari istituzionali. Operazioni che prima potevano essere effettuate solamente recandosi fisicamente presso una banca, ora possono essere disposte stando comodamente seduti sul proprio divano attraverso i servizi di home banking. Oltre all'evidente risparmio di tempo, aspetto ancor più rilevante è il completo abbattimento dei costi di gestione della transazione bancaria, ridotti del 98% se effettuata on-line, indipendente- mente dal luogo in cui si trova il correntista*», SIMONCINI E., *op. cit.*, nota n.1, 897

Anche in questo caso le innovazioni tecnologiche[199] hanno fatto sì che la criminalità organizzata potesse operare, oltre che nel mondo reale *offline*, anche nella rete[200], la quale rappresenta, in realtà, un terreno maggiormente fertile per il perseguimento di finalità illecite[201] tant'è che la criminalità organizzata c.d. del «*terzo millennio*»[202] riesce a generare profitti[203] in misura maggiore rispetto alle tradizionali modalità di riciclaggio soprattutto grazie ai minori costi delle operazioni[204] garantiti dall'utilizzo dei supporti telematici e della rete. Infatti, l'informatica e la digitalizzazione dei valori hanno portato alla transizione da un tipo di società basata sullo scambio materiale di beni o denaro, ad una nuova e diversa economia "virtuale" basata su sistemi di pagamento digitali, monete elettroniche, *e-commerce*[205], dove le

---

[199] ZAGARIS B., - MACDONALD S., *Money Laundering, Financial Fraud, and Technology: The Perils of an Instantaneous Economy* in *George Washington Journal of Law & Economics*, 3/1992

[200] Riguardo del caso dell'utilizzo delle criptovalute, *«Per questo motivo affermare di usare la rete per trasferire del denaro all'estero è in un certo senso fuorviante. Per la rete non esiste il concetto di estero: sono gli scambi commerciali di beni acquistati con il bitcoin che possono avvenire in una nazione o nell'altra, ma la valuta virtuale spedita e ricevuta si troverà sempre e solo sulla rete, registrata simultaneamente su tutti i nodi. Una persona può così ricevere della valuta mentre si trova in Italia, andare negli Stati Uniti, collegarsi alla rete e spendere il proprio denaro elettronico»* CALZONE O., *Servizi di mixing e monero in il mondo dell'inteligence* in Gnosis, 28 luglio 2017, disponibile sul sito internet istituzionale del SISR al seguente link: www.sicurezzanazionale.gov.it, 3

[201] *«In effetti la «Rete» presenta tre fondamentali caratteristiche che lo rendono un luogo ideale per il compimento di attività criminali di ogni genere: «delocalizzazione» (il fatto illecito non è immediatamente individuato nell'ambito di un specifico locus commissi delicti); «dematerializzazione» (dovuta al contenuto digitale delle informazioni, dei servizi e del denaro che circola nella rete); «dispersione» (difficoltà di identificare l'autore dell'illecito ai fini dell'imputazione della relativa responsabilità penale)»*, SIMONCINI E., *op. cit.*, 897;

[202] SIMONCINI E., *op. cit.*, 898

[203] «*Le stime del F.M.I. (Fondo Monetario Internazionale) ritengono che il denaro sporco muova tra il 3% ed il 5% del Pil del pianeta, ossia una cifra che oscilla all'incirca tra i 600 ed i 1500 miliardi di dollari solo negli USA. Per avere un quadro di riferimento a noi più vicino, basti pensare che in Italia il riciclaggio dei proventi illeciti produce 410 milioni di euro ogni giorno, 17 milioni l'ora, 285 mila euro al minuto, 4.750 euro al secondo*», SIMONCINI E., *op. cit.*, nota n.5, 898

[204] «*gli scambi finanziari che utilizzano la rete come strumento di contatto, offrono alle organizzazioni criminali e terroristiche numerosi canali di riciclaggio estremamente innovativi rispetto a quelli tradizionali.*» RAZZANTE R., *La regolamentazione antiriciclaggio in Italia*, Torino, 2007, 56

[205] «*New technologies, which are currently in various stages of development and testing, will make it easier for launderers to place money into the financial system, to manipulate these funds in order to hide their origins, and then to make use of the funds without raising any suspicions. These new methods include electronic cash, also known as "e-cash" or "cybercash," stored value cards (SVC), smart cards, and the Internet generally.* », SAXENA R., *Cyberlaundering: the next step for money launderers?* in *St. Thomas Law Review Spring*, 1998, 2

transazioni vengono elaborate in pochissimi secondi e con il minimo sforzo da parte dell'individuo[206].

Il «*lavaggio virtuale/cibernetico*» o "*cyberlaundering*"[207], evoluzione del riciclaggio tradizionale, ricomprende tutte le attività dirette ad occultare la provenienza delittuosa di capitali, beni, valori o altre utilità, utilizzando sistemi informatici e utilizzando la rete, comprensiva sia del *web* che del *dark*[208] e *deep web*[209]. Esso, fa parte dei c.d. *cybercrimes*, ossia i reati commessi a distanza tramite l'utilizzo della connessione *internet* e dei sistemi informatici o elettronici, e in particolare è qualificato tra i c.d. «*computer facilitated crimes*», reati facilitati dall'utilizzo dei computer, contrapposti ai «*computer crimes*», reati nei quali i computer costituiscono l'obiettivo materiale della condotta criminosa[210].

Generalmente, il riciclaggio "tradizionale" da un punto di vista criminologico viene suddiviso in più fasi[211], ed anche nel *cyberlaundering* sono presenti le stesse caratteristiche. In particolare, però, se per la prima fase (il collocamento del denaro di origine delittuosa) nel caso del riciclaggio così come viene generalmente inteso è necessario un trasferimento materiale del denaro sporco nell'economia legale, nel del *cyberlaundering* ciò non è necessario. Pertanto, il *cyberlaundering* risolve «*uno dei più grandi problemi del riciclaggio, ovvero la movimentazione fisica dei grandi flussi di denaro*»[212], in quanto il "denaro" da riciclare è già dematerializzato (o sotto forma di moneta elettronica o di criptovaluta).

---

[206] SIMONCINI E., *op. cit.*, 900

[207] «*Il termine Cyberlaundering deriva dalla fusione di due concetti profonda- mente differenti: il termine cyber, nato agli inizi degli anni '80 nell'ambito della letteratura fantascientifica, ed il termine laundering («lavanderia o lavaggio»), normalmente utilizzato nei paesi anglosassoni per definire il riciclaggio di denaro sporco (c.d. money-laundering)*», SIMONCINI E., *op. cit.*, 898

[208] «*il dark web (in italiano: web oscuro o rete oscura) è la terminologia che si usa per definire i contenuti del World Wide Web nelle darknet (reti oscure) che si raggiungono via Internet attraverso specifici software, configurazioni e accessi autorizzativi. Il dark web è una piccola parte del deep web, la parte di web che non è indicizzata da motori di ricerca, sebbene talvolta il termine deep web venga usato erroneamente per riferirsi al solo dark web»,* fonte: https://it.wikipedia.org/wiki/Darkweb

[209] PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio* in Rivisita trimestrale di diritto penale dell'economia, n. 3-4/2018, 592

[210] SIMONCINI E., *op. cit.*, 899

[211] «*Placement* (piazzamento materiale dei proventi), *layering* (stratificazione tramite operazioni volte a separare il capitale dalla sua origine, ed *integration* (integrazione dei circuiti legali con investimenti leciti)», PICOTTI L., *Profili penali del cyberlaundering, cit.*, nota n. 5, 592

[212] SIMONCINI E., *op. cit.*, *op. cit.*, 899

È utile menzionare che dai più si suole distinguere tra «*riciclaggio digitale strumentale*» e «*riciclaggio digitale integrale*». Il primo, è caratterizzato dall'uso della rete *internet* per «*migliorare e/o favorire*»[213] le operazioni di "ripulitura del denaro sporco" e si snoda nelle tre tradizionali fasi[214]. La fase più critica è di certo la prima, quella di collocamento dei capitali di origine delittuosa, poiché comporta il trasferimento fisico del denaro da ripulire negli istituti finanziari. Questi, sono obbligati dalla legge a sottoporre i clienti a determinate procedure di verifica, controllo e segnalazioni, le quali possono essere aggirate solo se vi sia un previo sodalizio criminale tra controllore e controllato o tramite corruzioni efficaci. Le successive fasi di stratificazione (*layering*) e di integrazione (*integration*), consistono nel compiere un numero consistente di transazioni finanziare frammentando il capitale da ripulire in tante minute porzioni[215] e infine rimpiegarlo in attività formalmente lecite come esercizi commerciali di vario genere (ristoranti, sale scommesse, compro oro ecc.)[216].

Il riciclaggio digitale integrale (la vera innovazione del riciclaggio), invece, è caratterizzato dal fatto che tutte le fasi descritte precedentemente avvengono interamente *online* e coperte dall'anonimità. A differenza del riciclaggio digitale strumentale, nella fase del collocamento non è necessario interfacciarsi materialmente con banche o intermediari finanziari, in quanto il denaro di provenienza illecita è già in «*formato digitale*»[217]. Addirittura, ciò rende superflue le ulteriori due fasi, in quanto è semplicemente necessario appoggiarsi ad una testa di legno (c.d. *Money mule*), la quale può anche benissimo essere una «*identità virtuale fittizia, creata mediante la produzione di un documento*»[218]. Infatti, è ben possibile aprire un conto online, senza sottostare ai controlli imposti alle banche al momento della registrazione di un nuovo cliente[219].

---

[213] SIMONCINI E., *op. cit.,* 900

[214] RAPUANO S., - CARDILLO M., *Le criptovalute: tra evasione fiscale e reati internazionali* in *Diritto e pratica tributaria*, n.1/2019, 58

[215] PICOTTI L., *Profili penali del cyberlaundering, cit.,* nota n. 5, 592

[216] SIMONCINI E., *op. cit.,* 901

[217] MULINARI S., *Cyberlaudering: riciclaggio di capitali, finanziamento del terrorismo e crimine organizzato nell'era digitale*, Torino, 2003, 62

[218] SIMONCINI E., *op. cit.,* nota n. 21, 901

[219] *«Tra i numerosi siti che consentono di aprire conti on-line ed effettuare trasferimenti in assoluta libertà, possiamo ricordare: www.paypal.com, www.paycash.ru, www.ecash.com, www.e-gold.com, www.e-dinar.com. Si tratta di banche virtuali che sfuggono ad ogni control- lo. Il sito www.e-dinar.com,*

Vi sono diverse modalità pratiche di configurazione del riciclaggio digitale integrale, come ad esempio la costituzione di società fittizie (c.d. *shell companies*), la creazione di *hotline* telefoniche[220], false fatturazioni e il c.d. *loan back*[221], il gioco d'azzardo *online* e non solo. Le *shell companies*, in particolare, sono società che sostanzialmente non esercitano alcuna attività commerciale, e vengono costituite col solo fine di farvi depositare il capitale illecito per essere poi reintrodotto nell'economia reale, tutto con l'accordo di un prestanome[222]. Generalmente vengono costituite nei c.d. paradisi fiscali (*tax heavens*[223]), in quanto le norme in suddetti paesi garantiscono l'anonimato attraverso il segreto bancario e molto spesso sono poco interessate o invogliate a cooperare con le autorità inquirenti estere.

Una breve disamina merita la questione riguardante il gioco d'azzardo *online*, una delle attività più redditizie per la criminalità organizzata[224]. Esso, grazie anche agli

---

in particolare, permette di effettuare tutte le operazioni in pieno rispetto della legge islamica, basandosi su una valuta virtuale (e-dinar) che corrisponde a 4,25 grammi d'oro 24 carati», SIMONCINI E., *op. cit.* nota n. 22, 901

[220] «*possibile, inoltre, costituire una hot-line telefonica verso cui far migrare i capitali tramite l'apparente fruizione del servizio telefonico o, ancora, aprire un sito di raccolta di donazioni per scopi benefici*», SIMONCINI E., *op. cit.*, 902

[221] «*il loan back rappresenta una tecnica di riciclaggio mediante la quale un soggetto (spesso un prestanome) si indebita chiedendo un prestito per avviare attività produttive o commerciali oppure per rilevare delle aziende, offrendo in cambio delle garanzie personali. Tali garanzie sono rappresentate da fondi di origine illecita o da certificati di deposito al portatore spesso detenuti presso istituti bancari o finanziari esteri. Di conseguenza, quando l debito non viene onorato, l'erogatore del finanziamento escute la garanzia rappresentata dai fondi di provenienza illecita perfezionando inconsapevolmente l'operazione di riciclag- gio*», SIMONCINI E., *op. cit.,* nota n. 92, 902

[222] «*nello specifico, la ripulitura del denaro sporco avvien tramite il c.d. mirror image trading, ossia «operazioni commerciali caratterizzate dall'acquisto e dalla vendita di beni e servizi fittizi tra società apparentemente diverse, ma riconducibili ad uno stesso soggetto, il cui unico scopo è quello di ripulire denaro attraverso transazioni apparentemente lecite*», SIMONCINI E., *op. cit*, 902 ed anche RICHARDS *Transnational Criminal Organizations, Cybercrime and Money Laundering: a Handbook for Law Enforcement Officers, Auditors and Financial Investigations*, New York, 1998

[223] «*Deriva da «haven», ossia rifugio/asilo, e non da «heaven», ovvero paradiso. Solitamente si tratta di territori, spesso di natura insulare ed ex-coloniale, amministrativamente indipendenti, con risorse economiche e finanziarie limitate, che al fine di attirare risorse finanziarie estere hanno deciso di incentrare il loro core- business sulla fornitura di servizi finanziari protetti da un rigido segreto bancario e su di una quasi totale assenza di imposizione fiscale»,* SIMONCINI E., *op. cit.*, 902

[224] «*In Italia l'industria del gioco d'azzardo rappresenta attualmente la terza impresa più redditizia, con un fatturato di oltre 84 miliardi di euro nel 2014, pari al 4% del PIL nazionale. Nel medesimo anno gli italiani hanno perso al gioco d'azzardo circa 17,2 miliardi di euro, potendo contare su circa 414 mila slot machine (una slot ogni 143 abitanti) e 51.000 VLT (videolottery), un terzo di quelle in funzione in tutto il mondo (circa 160.000). Nei primi nove mesi del 2015 si stima che il denaro puntato dagli italiani nel gioco d'azzardo sia pari a 4 miliardi.»,* SIMONCINI E., *op. cit.*, 910

ingenti volumi di denaro che coinvolge, comporta non solo il proliferare della commissione di attività di riciclaggio[225], ma anche usura, estorsione ed esercizio abusivo del credito. Poiché digitalizzato, il gioco d'azzardo *online* si presta sia come attività rientrante nel riciclaggio digitale strumentale, sia come attività di vero e proprio *cyberlaundering* in quanto è possibile movimentare grandi quantità di capitali illeciti in breve tempo senza che sia necessario alcun contatto fisico con le sale giochi. Inoltre, bisogna considerare che l'operare *online* permette di utilizzare i VPN (TOR, *tunnelbear*[226] e simili), che mascherano il proprio indirizzo IP, rendendo ancor più arduo la identificazione e localizzazione dell'utente nella rete. Se vengono, poi, utilizzate le criptovalute quali *bitcoin*[227] o *CasinoCoin*[228], allora l'identificazione sarà ancora più difficoltosa, anche perché è possibile ulteriormente ripulitore le criptovalute illecite tramite l'acquisto di beni o servizi o la conversione in moneta fiat[229].

Esempi di *cyberlaundering* ancor più semplici nella pratica sono l'utilizzo carte di pagamento elettroniche, o "*smart cards*"[230]: esse sono quotidianamente utilizzate dalla criminalità organizzata in alternativa al contante per effettuare transazioni telematiche

---

[225] «*secondo quanto riportato nel rapporto 2014 predisposto da McAfee Labs "Jackpot! Money laundering through online gambling", il gioco d'azzardo on-line, tra cui in particolare il poker e il casinò, consente facili opportunità di riciclaggio. Ciò è stato confermato anche dall'U.I.F. (Unità di Informazione Finanziaria) che nel 2014 ha ricevuto 71.661 segnalazioni di operazioni sospette in materia di riciclaggio, di cui 1.053 provenienti dai gestori di giochi e scommesse individuati ai sensi dell'art. 14 d. lgs. 231/2007. Tali segnalazioni nel 2015 sono arrivate a quota 82.428, di cui 1.466 da parte degli operatori del gioco e delle scommesse*». SIMONCINI E., *op. cit.*, 910

[226] *https://www.tunnelbear.com*

[227] «*Nel mercato del gioco on-line, una delle forme più diffuse di pagamento sia per le diverse case da gioco che per i giocatori sembra essere proprio il bitcoin, il quale viene generalmente accettato come principale strumento di pay-in e pay-out*», SIMONCINI E., *op. cit*, 909

[228] Una criptovaluta nata appositamente per essere utilizzata dai siti *online* di scommesse e gioco d'azzardo, la quale si basa sulla esistente criptovaluta *Ripple*, https://casinocoin.org/doc/CasinoCoin_Presentation_en.pdf

[229] SIMONCINI E., *op. cit.*, 911

[230] «*"carte intelligenti" (c.d. smart cards), tessere simili a carte di credito con- tenenti un micro-chip in grado di immagazzinare denaro in formato elettronico, spendibile come comune contante ed utilizzabile quale alternativa alla circola- zione delle banconote e delle monete aventi corso legale*», SIMONCINI E., *op. cit.*, 903

con cui vengono acquistati beni o servizi scambiando moneta elettronica[231] o anche moneta virtuale[232].

Bisogna considerare che l'utilizzo delle *smart cards*, in quanto mezzo di circolazione del denaro alternativo al contante, è fortemente incentivato proprio dalle discipline antiriciclaggio di diversi ordinamenti in virtù della possibilità di tracciare elettronicamente le movimentazioni di denaro di qualsiasi importo[233]. Detto ciò, si potrebbe asserire che le *smart cards* elimino del tutto i rischi del riciclaggio, ma così non è: la tracciabilità delle transazioni è un ottimo strumento di controllo, ma sarebbe davvero possibile tracciare e individuare il soggetto attore delle transazioni solo se siano riferibili ad un conto corrente intestato ad un soggetto previamente identificato. Inoltre, è possibile duplicare o alterare abusivamente i *chip* di memorizzazione dei dati delle *smart cards*, intervenendo sia sui dati identificativi che sulla somma disponibile; è possibile anche modificare i limiti di spesa giornalieri (imposti per finalità antiriciclaggio), cosi come far figurare transazioni da provenienza fittizia[234]. Ma le possibilità di eludere i controlli non finiscono qui, in quanto è possibile sfruttare le *defaillances* nelle normative antiriciclaggio dei paesi più permissivi, e in tal modo riuscire ad aprire anche conti correnti bancari ed entrare in possesso di *smart cards* tramite la presentazione di documenti falsi o la creazione di identità fittizie (o i c.d. prestanome).

Infine, vi sono dei casi in cui per entrare in possesso di una *smart card* non è necessario aprire un conto corrente bancario[235] (e quindi passare attraverso i controlli antiriciclaggio alla cui effettuazione sono obbligate le banche), e non è neanche

---

[231] «*un valore monetario rappresentato da un credito nei confronti dell'emittente che sia memorizzato su un dispositivo elettronico, emesso previa ricezione di fondi di valore non inferiore al valore monetario emesso e accettato come mezzo di pagamento da soggetti diversi dall'emittente*» (art. 55, lett. *h ter* della legge 1 marzo 2002, n. 39, attuativa della Direttiva 2000/46/ce).»

[232] Sono diversi gli *exchange* di criptovalute che offrono la possibilità di scambiare criptovalute con il supporto di una *smart cards* appoggiandosi al circuito *MasterCard* o *Visa*. In alcuni casi, come nel caso del noto exchange *Coinbase* è possibile acquistare beni o servizi in euro o in altra valuta fiat e pagare convertendo istantaneamente i propri *bitcoin* o *ethereum* al momento del pagamento. Per ulteriori approfondimenti, https://support.coinbase.com/customer/portal/articles/2969910-coinbase-card-faq

[233] PICOTTI L., *Profili penali del cyberlaundering, cit.,* 594

[234] PICOTTI L., *Profili penali del cyberlaundering, cit.,* 595

[235] «*most importantly for launderers, "many of today's SVC products are issued by non-bank issuers." As a result, launderers need not be as concerned with strict oversight when making transactions.*», «*Given the current situation, using a smart card is almost as anonymous and efficient as using cash*» SAXENA R., *Cyberlaundering, cit,* 10

indispensabile entrare in contatto con l'emittente specialmente nel momento del deposito iniziale del capitale[236]. Vi sono infatti distributori automatici di carte prepagate che permettono di convertire il contante in denaro "digitale" senza una previa identificazione, o di ricaricare *smart cards* già emesse[237]. Ciò facilità la fase del "*layering*", in quanto sarà sufficiente entrare in possesso di dette *smart cards* emesse dai suddetti distributori automatici e ricaricarle con il denaro da ripulire. L'ultima fase, quella dell'integrazione, verrà messa in atto semplicemente spendendo il denaro "*memorizzato*" nelle *smart cards* in beni e servizi leciti.

Merita anche di essere citata la possibilità di aprire un *account* sulla piattaforma *Paypal*, la quale richiede solo un indirizzo *e-mail* e un numero di cellulare. La caratteristica di *Paypal* è che permette di ricevere e inviare pagamenti senza alcun previo deposito di denaro, di fatto cosi posticipando i controlli antiriciclaggio solo nella fase successiva ed eventuale accredito su un conto corrente bancario[238]. Pertanto, *Paypal* si presta ad essere utilizzato in maniera efficace per operazioni di «"piazzamento" ed anche "occultamento"»[239] (*layering*) del denaro sporco, specialmente se accompagnate da identità digitali false o sottratte abusivamente a terzi[240]

Però, l'utilizzo di carte prepagate emesse da emittenti autorizzati e quindi l'uso della moneta elettronica, o l'esecuzione di bonifici bancari realizzati tramite false identità o le c.d. teste di legno, non sono affatto paragonabili all'utilizzo dei nuovi

---

[236] SIMONCINI E., *op. cit.*, 904

[237] «*Specialmente nei paesi dove le norme sul segreto bancario sono assai stringenti, è possibile ottenere smart cards anonime anche richiedendole online*» GHILARDUCCI D., *Criminalizzazione globale*, in *www.terrelibere.it*, gennaio 2003.

[238] «*consente l'immediata possibilità di effettuare o ricevere pagamenti nel web, senza previo deposito di valori o somme di denaro, né loro custodia da parte del prestatore del servizio, fermo solo il conteggio del "dare" ed "avere" (c.d. balance), che deve restare entro certi limiti di pareggio o sbilancio, alle condizioni e nei termini temporali contrattualmente prefissati*», PICOTTI L., *Profili penali del cyberlaundering, cit.* 598

[239] PICOTTI L., *Profili penali del cyberlaundering, cit.,* 593

[240] «*deve destare qualche preoccupazione la creazione del portafoglio elettronico di google, il c.d. google wallet, un nuovo servizio per semplificare i pagamenti, utilizzando uno smarthphone al posto delle carte di credito. Consente di memorizzare i dati di pagamento nel proprio account in modo da non dover inserire i dati di fatturazione e di spedizione ogni volta che si procede ad acquisti online*», RAZZANTE R., *il riciclaggio come fenomeno transnazionale: normative a confronto,* Milano, 2014

"sistemi di pagamento" non regolamentati e il cui funzionamento non è gestito da un ente centrale autorizzato quali sono le criptovalute[241].

Tali operazioni sono completamente al di fuori dal sistema finanziario e bancario[242], la loro emissione e circolazione non è centralizzata[243] e pertanto è ancor più arduo opporre dei controlli alle movimentazioni di denaro in entrata e in uscita dal "virtuale". Il controllo sull'autenticità delle transazioni non è deputato ad un intermediario o un ente garante, ma è tutto basato sul sistema del consenso e pertanto nella reciproca fiducia dei partecipanti alla rete. Per inviare e ricevere bitcoin non è necessario aprire un conto corrente, né l'utilizzo di carte di credito o di effettuare depositi e prelievi. È necessario semplicemente o scaricare il *client* ufficiale della criptovaluta, ossia un portafoglio elettronico che custodisce e permette di scambiare la criptovaluta, oppure è necessario acquistarle tramite un *exchange* (prestatori di servizi che operano alla stregua dei cambiavalute) e trasferirle poi su un *wallet* (la maggior parte degli *exchange* fornisce anche un servizio di *wallet*)[244]; nel primo caso gli utenti potrebbero non venire mai in contatto con il sistema bancario o finanziario, mentre nel secondo caso gli utenti dovrebbero interfacciarsi con gli *exchange*, ed infatti essi sono stati i nuovi soggetti obbligati ad essere *compliant* con le prescrizioni in tema antiriciclaggio da parte della V Direttiva[245]. Ciò non rende le criptovalute

---

[241] «*La differenza sostanziale tra le comuni carte di credito ed i sistemi di pagamento che si basano sulla moderna moneta virtuale, è rappresentata essenzialmente dalla differente normativa applicabile: mentre le prime sono emesse e gestite da istituti di credito e società finanziarie, sottoposte a leggi, regolamenti ed accordi internazionali che ne disciplinano le modalità operative e di funzionamento, le seconde sono direttamente gestite da società private che operano nel cyber-spazio, non riconducibili ad organismi istituzionali operanti nel contesto transnazionale.*», SIMONCINI E., *op. cit.*, 905

[242] «*Le criptovalute prescindono da collegamenti vincolanti con il valore delle monete aventi corso legale e quindi non possiedono di per sé un valore di scambio ufficiale giuridicamente garantito da istituti emittenti, che come detto non esistono, come è invece basilare nei sistemi di pagamento bancari e finanziari tradizionali, in cui sono regolati e controllati i flussi monetari*», PICOTTI L., *op. cit.*, 603

[243] «*Il denaro virtuale presenta delle peculiarità che lo distinguono nettamente dalla moneta avente corso legale in un determinato Stato: 1) non viene erogato da una banca centrale, essendo una creazione totalmente privata; 2) la sua circolazione non è soggetta ad alcun controllo di tipo politico da parte delle istitu- zioni statali a ciò preposte; 3) costituisce un mezzo di pagamento sicuro ed anonimo.*», SIMONCINI E., *op. cit.*, 905., ed anche Banca d'Italia, *Avvertenze sull'utilizzo delle cosiddette «valute virtuali»*, 30 gennaio 2015, «*le monete virtuali non rappresentano in forma digitale le comuni valute a corso legale (euro, dollaro, ecc.); non sono emesse o garantite da una banca centrale o da un'autorità pubblica e generalmente non sono regolamentate*»

[244] STURZO L., *op. cit.*, 30

[245] A proposito dei *digital wallet*, «*In linea puramente teorica, si potrebbe pretendere che le procedure di adeguata verifica venissero espletate prima dello scaricamento del software, ma questo produrrebbe*

intrinsecamente illegali, ma di fatto agevolano non poco attività criminose di ogni genere, non solo riciclaggio, ma anche estorsioni via web, corruzioni e traffici illeciti[246]. Infatti, l'anonimità, la riservatezza, l'immediatezza e la flessibilità[247] non solo rendono più semplice ripulire il denaro sporco ma costituiscono senza dubbio i motivi per cui lo scambio di criptovalute viene preferito allo scambio di valuta legale nonostante l'estrema volatilità del valore[248], rendendole un vero e proprio «*cyber-heaven*»[249].

L'esempio più immediato di riciclaggio di denaro tramite bitcoin è rappresentato dall'acquisto di *bitcoin* o altre criptovalute con proventi di derivanti da ulteriori reati, di fatto cosi ostacolando la provenienza delittuosa degli stessi. I consistenti profitti generati dai reati economici e i profitti ottenuti sotto forma di contanti (derivanti da traffico di droga, estorsione, prostituzione ecc.) possono essere digitalizzati con le modalità descritte sopra e poi ripuliti con il minimo sforzo con l'acquisto di valuta virtuale, la quale a seguito dei sempre più numerosi individui disposti ad accettarla come corrispettivo, permette la ripulitura dei capitali illeciti con il minimo rischio di essere rintracciati[250]. Ancor più semplicemente, è possibile ripulire i contanti "sporchi"

---

almeno due conseguenza indesiderate: i gestori dei siti che permettono di scaricare il software sarebbero sottoposti a degli oneri tecnici e di sicurezza molto elevati, e gli utenti, temendo per la propria privacy, difficilmente sceglierebbero di usare tali criptovalute.», DANIELLI A., - GENDUSA M., - DI MAIO M., - RINALDI G, *op. cit.,* 37

[246] *In primis,* droga, armi, persone ed organi, PICOTTI L., *Profili penali del cyberlaundering, cit.* 604

[247] «*Per queste sue intrinseche caratteristiche, i bitcoin possano essere utilizzati come straordinario strumento per effettuare transazioni connesse ad attività criminali, tra cui il riciclaggio di denaro sporco*», SIMONCINI E., *op. cit.*, 907

[248] «*Paradigmatico è l'incremento di valore di bitcoin di circa il 500% in un anno, con un crollo poi da 5000 euro a meno di 3000 in un solo giorno, e dopo una successiva risalita, un'ulteriore caduta a circa 4000 euro di valore*», PICOTTI L., *op. cit,* 604.; sempre a riguardo, «*L'anno scorso la paura di perdere il treno dei facili guadagni ha spinto molti risparmiatori sprovveduti a saltare sul carro in corsa, con il rischio concreto di vedere i propri risparmi volatilizzati. Il boom di bitcoin ha trascinato l'intero comparto delle criptovalute cresciute a dismisura. Oggi sono più di 2.000 monete quotate, stando al censimento di Coinmarketcap, con una capitalizzazione complessiva attorno ai 220 miliardi di dollari, la metà dei quali attribuibili proprio al bitcoin, dopo aver toccato un picco di oltre 800 miliardi a inizio anno. Alcune valute hanno perso fino al 90%, altre non esistono più.», https://www.ilsole24ore.com/art/tecnologie/2018-06-10/bitcoin-ricchezza-concentrata-poche-mani-vince-speculazione-breve-150229.shtml?uuid=AEM37p3E.*

[249] «L'*Europol definisce il Bitcoin come la principale moneta utilizzata dalla criminalità organizzata on-line, attraverso la quale vengono compiute numerose attività illecite (riciclaggio, compravendita di droga, commercio di armi, vendita di beni illegali, traffico di organi umani ed estorsioni),* SIMONCINI E., *op. cit.*, 909

[250] «*loro natura anonima e la rapida trasferibilità, rendano i bitcoin uno strumento perfetto per il riciclaggio di denaro, specialmente se associato ai nuovi fenomeni di gioco d'azzardo illegale su piattaforme on-line*» SIMONCINI E., *op. cit.*, 909

contattando dei soggetti detentori di criptovaluta disposti a venderla in cambio, appunto, di denaro contante; basta anche una semplice *app* per *smartphone* ed è possibile effettuare la transazione dal vivo «faccia a faccia»[251], in luogo pubblico, senza dover previamente "digitalizzare" il denaro contante.

2.3.1 (*Segue)* Il c.d. *"mixing"*

Una nuova modalità di *cyberlaundering* che è emersa con l'invenzione della *blockchain* è quella del c.d. *mixing* (o "*tumbling*"[252]). Essa consiste nell'effettuare un numero elevato di transazioni con il risultato di "spacchettare" grandi quantità di criptovalute in modo tale da rendere più difficile la tracciabilità della provenienza delle stesse. Letteralmente, il *mixing* consiste appunto nel "mescolare" o "mischiare" numerosi "frammenti" di criptovaluta distribuendoli su più indirizzi, pertanto « *il pagamento da A ad A verrà perciò dirottato su B, e quello da B a B (di importo corrispondente al primo) verrà dirottato su A, in modo che risultino confusi i nominativi degli ordinanti ed i rapporti in dare e avere tra questi e i riceventi*»[253]. In rete sono diversi i servizi di *mixing* offerti[254], e vengono remunerati con piccoli importi di criptovaluta a titolo di commissioni di servizio[255].

Vi sono due tecniche utilizzate per il *mixing*[256]: la prima consiste nel trasferire frammenti di un iniziale importo di criptovaluta a più indirizzi (chiamati indirizzi "*bounce*", ossia di rimbalzo) in modo tale da rendere notevolmente più intricata la serie di passaggi tra più indirizzi; la seconda tecnica consiste nel "mescolare" più transazioni

---

[251] ACCINNI G., P., *op. cit.*,12

[252] RAPUANO S., - CARDILLO M., *Le criptovalute: tra evasione fiscale e reati internazionali* in *Diritto e pratica tributaria,* n.1/2019, 60

[253] ACCINNI G., P., *op. cit.,* 7

[254] «*I più utilizzati sono Bitmixer (https://bitmixer.io.), Bit Launder (https://bitlaunder.com) Shared Coin http://blockchatvqztbll.onion (indirizzo raggiungibile solo TOR browser), Bitcoin Blender http://bitblendervrfkzr.onion, (anch'esso necessita del browser TOR)*» CALZONE O., *Servizi di mixing e Monero*, in GNOSIS, 28 luglio 2017, disponibile sul sito internet istituzionale del SISR www.sicurezzanazionale.gov.it.; anche, Easycoin (http://easycoinsayj7p5l.onion.pet/, indirizzo TOR) ACCINNI G., P., *op. cit.,* 7

[255] In genere viene applicata una commissione tra 1% e 3%, fonte: NOVETTA, *Survey of bitcoin mixing services: tracing anonymous bitcoins*, Mcleans (Virginia, USA), 2015, https://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf.

[256] CALZONE O., *op. cit.,* 5

dei vari soggetti che si utilizzano il servizio di *mixing* a un indirizzo "*pool*", ossia di raccolta, e solo successivamente trasferirli a più indirizzi.

Può sembrar paradossale pagare per rendere anonima una transazione che lo è già, ma in realtà, come è estato esplicato più volte nei paragrafi precedenti, nella *blokchain* delle criptovalute (ma non tutte) non è garantita l'assoluta anonimità, ma si parla di pseudo-anonimato[257]. Infatti, è vero che di ogni transazione non è dato sapere nome e cognome dei soggetti protagonisti, ma ciò che rimane pubblico sono le transazioni con i relativi importi e indirizzi alfanumerici. Proprio dall'analisi delle transazioni, però, è possibile (seppur non semplicemente), risalire approssimativamente all'identità dei soggetti agenti della transazione: «*è tecnicamente possibile individuare l'indirizzo IP*[258] *del computer usato per spedire e ricevere valuta ed associare poi ad un conto in bitcoin, tramite l'indirizzo IP, i dati comportamentali del proprietario del conto, come i siti web che ha visitato*»[259]. Le informazioni contenute nella *blockchain* possono essere aggregate e associate con informazioni aggiuntive per creare collegamenti a identità reali[260]. Le suddette informazioni aggiuntive sono informazioni riguardanti l'identità personale, il comportamento dell'utente, dati finanziari e la connessione *internet*. In particolare, i primi sono le informazioni che collegano un *account online* o una merce ad una identità reale. Sono dati spesso raccolti in occasione della registrazione dell'*account* e comprendono nome e cognome, indirizzo e-mail, data di nascita ecc. (anche se possono essere falsi, si può risalire alla vera identità tramite account collegati o connessi). I dati finanziari sono gli estremi di conti bancari con cui nel caso sono stati acquistati i *bitcoin* da un *exchange*. Infine, i dati riguardanti la connessione a internet riguardano appunto gli indirizzi IP, cosi come i *cookies*[261] e la

---

[257] CALZONE O., *op. cit.,* 6

[258] «*Tuttavia, incrociando più transazioni effettuate dallo stesso wallet, è possibile risalire al proprietario fisico; spesso, inoltre, le transazioni rivelano dettagli importanti sul computer utilizzato per effettuarle, come ad esempio l'indirizzo IP. Inoltre, tutte le transazioni effettuate nella storia di Bitcoin saranno sempre pubbliche. Pertanto, è più corretto dire che Bitcoin è un sistema "pseudo-anonimo", e non garantisce anonimità.*», CHIRIATTI M., *I nove (falsi) miti più comuni di bitcoin e delle valute virtuali*, in «Il Sole 24 Ore», https://www.ilsole24ore.com/art/tecnologie/2016-02-02/bitcoin-e-anonimo-171022.shtml?uuid=AC45ZDM C, 3 febbraio 2016

[259] CALZONE O., *op. cit.,* 8

[260] NOVETTA, *Survey of bitcoin mixing services, cit., 3*

[261] «*I cookie (più comunemente denominati cookie web, o per antonomasia cookie) sono un tipo particolare di magic cookie (una sorta di gettone identificativo) e vengono utilizzati dalle applicazioni*

configurazione del *browser* (anche se essi sono facilmente mascherabili con TOR e i servizi VPN).

È indubbio che l'utilizzo di questi servizi che permettono di aggiungere un ulteriore strato di anonimità[262] alle transazioni di criptovalute si giustifichi solo in quanto si voglia far perdere completamente le tracce dell'origine delle criptovalute da "mixare"[263], origine che non può che sospettarsi come delittuosa. Anche l'uso del browser TOR per effettuare le transazioni potrebbe destare lo stesso sospetto ma in misura nettamente inferiore, in quanto strumento generico per navigare *online* tra gli elementi non indicizzati dai motori di ricerca. Pero, bisogna procedere con cautela a riguardo, poiché ciò potrebbe condurre a una presunzione di consapevolezza da parte dei gestori dei servizi di *mixing* o degli *exchange* della provenienza delittuosa di determinate criptovalute[264].

Per ottenere il risultato di rendere ancor più difficile tracciare la provenienza di determinate criptovalute, non esistono soltanto i servizi di *mixing* ma sono state sviluppate delle criptovalute che integrano nel loro protocollo di funzionamento un sistema di *mixing*. Infatti, dopo la chiusura del noto *marketplace* di merce illegale operante nel *darkweb* "*The Silk road*"[265], i criminali hanno virato verso l'utilizzo di

---

web lato server per archiviare e recuperare informazioni a lungo termine sul lato client.» Fonte: https://it.wikipedia.org/wiki/Cookie

[262] Inoltre, «*Per aumentare il grado di anonimato e rendere più difficoltosa la tracciabilità degli scambi è però possibile usare: carte prepagate per acquistare i bitcoin direttamente da altri utenti, contattabili ad esempio attraverso il sito LocalBitcoin, riducendo così al minimo la comunicazione dei propri dati personali*», CALZONE O., *op. cit.,* 2. In particolare, *local bitcoin* (https://localbitcoins.com/it/) permette la vendita di bitcoin online collezionando le domande e offerte di bitcoin sul proprio sito.

[263] «I *risultati ottenuti da Novetta [societa specializzata nell'analisi dei dati] evidenziano come i servizi di mixing riescano ad eliminare nella maggior parte dei casi il collegamento, […], fra indirizzi di origine quelli di destinazione. Tuttavia l'analisi descrittiva permette di individuare dei comportamenti tipici di ogni servizio e quindi, nel caso di utilizzo per far perdere le tracce di fondi ottenuti illegalmente, di individuare quello usato per tale scopo».* CALZONE O., *op. cit.,* 6

[264] Infatti, «*L'astratta sussumibilità delle tipologie criminose appena richiamate nella fattispecie di cui all'art. 648 bis c.p. e l'aura di sospetto che avvolge di fatto i servizi di mixing rischia tuttavia di condurre a indebite scorciatoie probatorie, da contrastare con la necessaria ponderazione del "rischio che la natura intrinsecamente opaca ed anomala delle criptovalute presti il fianco a legittimi dubbi di consapevolezza, in capo all'exchanger (o al diverso soggetto che compia l'operazione di conversione di valuta avente corso legale in valuta virtuale), della provenienza illecita dei fondi utilizzati per l'acquisto della virtual currency di volta in volta considerata»,* NADDEO M., *op. cit.*, 106

[265] *https://www.repubblica.it/tecnologia/2014/11/06/news/arrestato_capo_di_silk_road_2-99933316/; «Il caso più celebre di utilizzo di bitcoin per pagare merci la cui vendita era illegale è certamente Silk Road, l'"eBay del vizio", fondata nel 2011 da un utopista libertario, Ross Ulbricht. Il sito è stato*

criptomonete alternative al *bitcoin* (in quanto la sua anonimità è stata dimostrata come non infallibile di fronte alle autorità inquirenti statunitensi).

Come già esposto precedentemente, *Monero* è una delle criptovalute appartenenti a questa tipologia di criptovalute che sta più attirando l'attenzione dei media[266], ed attualmente ha una capitalizzazione di circa un miliardo di dollari[267]. Il suo funzionamento si basa sulla "*unlikeability"* (non associabilità) e sulla "*untreaceability"* (non tracciabilità); la prima non permette di accertare se il destinatario sia un singolo soggetto o più soggetti, la seconda permette di non poter affermare con certezza che tra due indirizzi vi sia stato effettivamente uno scambio di criptomoneta[268]. Pertanto, l'utilizzo di questa criptovaluta piuttosto che il *bitcoin*

---

progettato come un mercato libero, costruito per essere fuori dalla portata del controllo governativo e per dare libertà di scelta ai propri utenti, che potevano decidere le droghe di cui fare consumo senza dover entrare in contatto con pericolose bande di narcotrafficanti o rischiare l'arresto. Simile a eBay, metteva in corrispondenza diretta compratori e venditori, consentendo la vendita solo di prodotti che non derivavano da soprusi e non potevano creare danni eccessivi; […]. I pagamenti erano possibili solo tramite bitcoin e il servizio funzionava su TOR, garantendo comunicazioni quasi completamente anonime. Si stima che nei circa tre anni di vita siano stati venduti beni per un valore complessivo di un miliardo di dollari. L'FBI ha impiegato quasi due anni di lavoro per scoprire l'amministratore del sito, attraverso una paziente attività di infiltrazione, e ha arrestato Ulbricht nell'ottobre del 2013, DANIELLI A., - GENDUSA M., - DI MAIO M., - RINALDI G., *op. cit.*, 46

[266] CALZONE O., *op. cit.*, 7.; a riguardo, «*Monero sta avendo una così rapida diffusione che molti mercati digitali stanno implementando la possibilità di accettare pagamenti in Monero assieme ai pagamenti in bitcoin, rendendo cosı` possibili anche gli scambi tra le due criptovalute. Un esempio è dato dal portale AlphaBay, sul quale si praticava la vendita di stupefacenti: accettando Monero come strumento di pagamento, AlphaBay le ha permesso di quintuplicare il suo valore nel giro di un anno*». RAPUANO S., - CARDILLO M., *op. cit.*, 61

[267] Fonte: https://coinmarketcap.com/currencies/monero/

[268] Nello specifico: *Il primo dei due obiettivi è ottenuto attraverso il concetto di firma digitale one-time. Il secondo grazie alla ring signatures.», «Gli utenti di Monero hanno delle coppie di chiavi private e pubbliche di lungo periodo. L'invio di denaro presuppone però la creazione, per ogni transazione, di chiavi pubbliche e private 'usa e getta' (firma digitale one-time). Per inviare dei fondi ad un'altra persona, un utente di Monero genera una chiave pubblica one-time di questa persona ed una chiave identificativa della transazione. A partire dalla chiave della transazione e della sua chiave privata di lungo periodo, il destinatario è in grado di capire di aver ricevuto dei soldi e di spenderli generando una chiave privata one-time.» «Se una transazione contiene più output, cioè invii a più destinatari, anche se due dei destinatari sono in realtà la stessa persona, i due output avranno comunque chiavi pubbliche one-time diverse. n Monero quindi più invii di denaro ad una determinata persona sono in realtà fatti verso chiavi pubbliche differenti e per questo motivo, a partire dalle informazioni contenute nelle copie del registro contabile di Monero, non si è in grado di stabilire se, dati due invii di denaro, la valuta virtuale sia stata o meno spedita ad un'unica persona (unlinkability);* riguardo le ring signatures, *«obiettivo della non tracciabilità è perseguito attraverso la ring signature. Uno schema di ring signature si basa su tre algoritmi: 1. un algoritmo che crea una una coppia di chiavi, privata e pubblica; 2. un algoritmo che crea una firma digitale di un messaggio a partire dal messaggio stesso, dalla chiave*

garantisce ancor di più la *privacy* e la riservatezza delle transazioni. Per questi motivi, ben si presta ad essere utilizzata come strumento del reato di riciclaggio, in quanto le sue caratteristiche tecniche ne agevolano la commissione e ne impediscono la persecuzione.

Concludendo, il *mixing* offerto da piattaforme *online* o integrato nel funzionamento di criptovalute diverse dal *bitcoin*[269] rappresenta una particolare modalità di *cyberlaundering*, nata con lo sviluppo della *blockchain*, e che può benissimo integrare la condotta residuale delle "altre operazioni" o anche il "trasferimento" della fattispecie di riciclaggio *ex* art. 648-*bis*.

2.4 I reati contro il patrimonio: I delitti di Riciclaggio, Impiego di denaro, beni o altra utilità di provenienza illecita e l'Autoriciclaggio (Artt. 648-*bis*, *ter*, *ter*.1 c.p.)

In seguito alle considerazioni svolte nei paragrafi precedenti, il reato la cui commissione risulta più agevolata dall'utilizzo delle criptovalute è senza dubbio il reato di riciclaggio[270], di cui all'art. 648-*bis*[271] c.p. Anche il delitto di Impiego di denaro, beni o altra utilità di provenienza illecita e quello di Autoriciclaggio rubricati agli articoli 648-*ter* e 648-*ter*.1 sono configurabili attraverso le valute virtuali.

In virtù delle loro caratteristiche strutturali e di funzionamento (anonimato/pseudonimato *in primis*), i *bitcoin* e le specialmente le altre criptovalute progettate per garantire un livello di *privacy* ulteriore[272] sono di fatto estremamente

---

privata di chi firma e da un insieme di chiavi pubbliche (detto ring) di cui fa parte anche la chiave pubblica del firmatario; 3. un algoritmo che, a partire dalla firma, dal messaggio originale e dal ring, restituisce 'vero' solo se la firma è stata creata, a partire dal messaggio, da un membro del ring. L'utilizzo della ring signature permette quindi, ad un osservatore esterno, solo di poter affermare che un messaggio è stato firmato da uno dei membri del ring. Membri che sono scelti di volta per ogni messaggio da firmare.» CALZONE O., *op. cit.*, 7

[269] a cui ci si riferisce con il termine di *Altcoin (alternative coins)* NADDEO M., *op. cit.*, 100

[270] «*Il carattere anonimo o pseudoanonimo dell'impiego della valuta virtuale (come nel caso dei bitcoins) in una operazione di scambio, a basso costo e tra giurisdizioni diverse, ulteriormente aggravato da servizi di mixing, risultano condizioni obiettivamente predisponenti alle operazioni di riciclaggio*» DI VIZIO F., *Le cinte daziarie del diritto penale, cit.,* 57

[271] Inserito dalla l. 18 maggio 1978, n. 191 così come modificato dall'art. 23 l. 19 marzo 1990, n 55 e dall'art. 4 l. 9 agosto 1993, n.328

[272] *Dash, Zcash e Monero in primis*, DANIELLI A., - GENDUSA M., - DI MAIO M., - RINALDI G., *Bitcoin e criptovalute,* Milano, 2018*;* in particolare riguardo *Monero, «il cui protocollo di funzionamento*

appetibili per la criminalità organizzata e gruppi terroristici[273]. Le garanzie delle criptovalute in termini di anonimità e di difficile individuazione e localizzazione delle transazioni conferiscono alle criptovalute potenzialità criminogene consistenti.

Bisogna innanzitutto considerare che con l'ultima modifica della disposizione in questione, la fattispecie del reato di riciclaggio ha assunto qualifica di fattispecie a forma libera[274], in quanto non solo saranno rilevanti le condotte di sostituzione o trasferimento, ma anche le «*altre operazioni*»; il legislatore ricomprendendo quest'ultime, ha reso la fattispecie molto elastica e capace di ricomprendere non solo le tradizionali modalità di riciclaggio ma anche quelle che si svilupperanno di pari passo con l'evoluzione tecnologica[275]. Inoltre, è stato anche aggiunto l'inciso « *in modo tale da ostacolare l'identificazione della loro provenienza delittuosa*»[276], trasformando la disposizione in fattispecie di pericolo concreto. Perciò è necessario accertare se l'utilizzo di *bitcoin* possa concretamente ostacolare la provenienza delittuosa di beni, denaro o altra utilità.

Si potrebbe addure come argomentazione contraria alla concreta idoneità decettiva della provenienza delittuosa che la *blockchain* è un registro pubblico, accessibile da tutti, la cui intera copia è conservata in ogni nodo del sistema; ma bisogna tener conto

---

(denominato CryptoNote) prevede la creazione automatica di nuove coppie di chiavi per ogni operazione e rende visi- bili le informazioni relative alla transazione (ad esempio il suo importo) al solo ricevente ovvero ad un terzo dotato di un'apposita viewkey fornitagli dall'ordinante. Il sistema Monero prevede anche un sistema di mixing auto- matico e garantito indistintamente a tutti gli utenti, con la logica conseguenza che tutte le operazioni risulteranno oscurate e difficilmente ricostruibili nel loro concreto dipanarsi», ACCINNI G., P., *op. cit.*, 7

[273] «*Tanto considerato, al di là delle inevitabili critiche mosse da chi antepone l'innovazione digitale al controllo burocratico, presagendo come l'imposizione di regole muterebbe la ratio stessa di un sistema basato sulla rapidità delle transazioni e sulla totale libertà degli utenti, non può ignorarsi la capacità attrattiva che un sistema del genere, caratterizzato dall'anonimato/pseudonimato delle sue transazioni e dall'assenza di un organismo controllore, provochi nei confronti di chi intenda sfruttare il sistema per perseguire un fine illecito, quale ad esempio quello di ripulitura di proventi delittuosi ovvero di finanziamento di gruppi terroristici tramite un semplice click*», STURZO L., *op. cit.*, 34

[274] FIANDACA G., - MUSCO E., *Diritto penale. Parte speciale*, VII ed., Bologna, 2015

[275] «*esse risultano già formulate con espressioni linguistiche ampie ed elastiche, che si prestano ad abbracciare in via ermeneutica, de jure condito, molteplici fasi od attività riconducibili ai fenomeni nuovi*». PICOTTI L., *Profili penali del cyberlaundering, cit.*, 608

[276] «*In particolare l'elastica clausola di chiusura finale non richiede alcuna specifica modalità tecnica, né alcun univoco risultato finale, dalla condotta punibile, bastandone l'idoneità ad "ostacolare" l'identificazione della provenienza, sia oggettiva, che soggettiva, di valori ed "utilità", senza che occorra un'assoluta impossibilità, né che vi sia un vincolo definitorio alla materialità fisica degli oggetti della condotta stessa*», PICOTTI L., *op. cit.,* 608

che seppur pubbliche le transazioni, è concretamente molto difficile[277] risalire all'identità dei soggetti protagonisti delle transazioni[278], in virtù delle considerazioni esplicitate nei precedenti paragrafi riguardo i possibili utilizzi illeciti derivanti dalle caratteristiche delle criptovalute (l'uso di TOR, i VPN e il c.d. *mixing*)[279].

Se poi consideriamo che le transazioni possono avvenire tra soggetti di cui alcuni di essi risiedono in stati dove le normative antiriciclaggio sono poco stringenti, o comunque sono dotate di autorità inquirenti poco efficaci, il rischio di circolazione di denaro sporco si amplifica fortemente, conferendo alle criptovalute una certa attitudine decettiva.

Analizzando l'elemento oggettivo della fattispecie, e in particolare l'elemento materiale, esso è costituito da «*beni, denaro o altra utilità*». Ricondurre le criptovalute sotto la definizione di denaro è incorretto in quanto le criptovalute non sono riconosciute dallo stato come moneta avente corso legale. La riconducibilità alla categoria dei beni non comporta problemi insormontabili in quanto parte della dottrina ritiene che possa rappresentare sia beni materiali che immateriali, ma comunque possono rientrare senza problemi nel concetto di "altra utilità"[280]. Pertanto, non vi sono

---

[277] «*Nondimeno, la tracciabilità delle singole operazioni non giunge sino al punto di consentire di risalire alla reale identità dei singoli operatori. Vero infatti che in ogni operazione ciascun user è identificato da una chiave pubblica ed una privata. Allorquando si effettui un pagamento, la blockchain registra quindi la chiave pubblica del pagante e l'importo dell'operazione, mentre la chiave privata (la password) non viene pubblicata sulla blockchain, ma rimane nella esclusiva disponibilità del titolare dell'e-wallet. Quanto risulterà visibile sulla blockchain non sarà quindi mai il reale nominativo di chi effettui un'operazione, ma un mero numero identificativo corrispondente alla chiave pubblica dei soggetti coinvolti*, ACCINNI G. P., *op. cit.,* 5

[278] V. *Supra* § 2; LA ROCCA L., *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, in *Analisi Giuridica dell'economia*, 2015 n.1, 209

[279] «*È fuorviante, dunque, ritenere che la ricostruibilità storica, dunque a posteriori, delle transazioni e dei loro protagonisti di digitali costituisca un impedimento assoluto all'integrazione del reato di riciclaggio; nel caso delle valute virtuali a non essere assicurato infatti è proprio legame tra indirizzi delle transazioni e identità di chi realmente li controlla; onde la possibilità che il trasferimento e le sostituzioni valgano a complicare l'identificazione della provenienza delittuosa è assai sviluppata*» STURZO L., *op. cit.*. 58

[280] «*le condotte hanno quale elemento di origine (provento) o di trasformazione (prodotto) la componente delle utilità, contenutisticamente assai ampia. In particolare, per la giurisprudenza di legittimità, con il progressivo ampliamento dei reati presupposto, della condotta incriminabile e dell'oggetto del reato, il legislatore, utilizzando la locuzione «altre utilità», ha inteso colpire con il delitto di riciclaggio «ogni vantaggio derivante dal compimento del reato presupposto». Una clausola di chiusura rispetto al denaro ed ai beni impiegata proprio per evitare che sfuggano alla repressione penale utilità (qualunque esse siano) derivanti dal reato presupposto e delle quali l'agente, grazie all'attività di riciclaggio*

dubbi sulla configurabilità del reato di cui all'art. 648-*bis* c.p. con l'utilizzo delle criptovalute e in particolare con la conversione del denaro contante in valuta virtuale[281].

Discorso analogo vale anche per il reato rubricato all'art. 648-ter (Impiego di denaro, beni o utilità di provenienza illecita) inserito nel codice penale dall'art 24 della l. 19 marzo 1990, n 55. Infatti, l'ambito assai ampio delle «*attività economiche e finanziare*» e il riferimento alle «*altre utilità*» riescono a ricomprendere qualsiasi attività di trasferimento o scambio di criptovalute[282].

Riguardo il reato di autoriciclaggio (art. 648-*ter*.1 introdotto dall'art. 3 della legge 15 dicembre 2014, n.186), è necessaria qualche ulteriore precisazione.

È senza dubbio configurabile attraverso l'uso delle criptovalute (in quanto la fattispecie è formulata in modo tale da ricomprendere anche il *cyberlaundering* mediante criptovalute)[283], ma è necessario far attenzione al requisito imposto dalla norma riguardo al contesto in cui i *bitcoin* di origine delittuosa vengono impiegati, sostituiti o trasferiti, ossia «attività economica, finanziaria, imprenditoriale o speculativa». È da escludere che lo scambio o conversione di criptovaluta possa essere qualificata come attività economica[284] o imprenditoriale[285], ma si potrebbe invece ritenere possibile[286] la configurazione di attività speculativa[287] in quanto a seguito dell'elevata volatilità dei prezzi delle criptovalute, è molto frequente che vengano acquistate e scambiate per attività di speculazione, piuttosto che per essere utilizzate come corrispettivo di beni o servizi[288]. Inoltre, in dottrina si suole identificare l'attività

---

realizzata da un terzo, possa usufruire. Le utilità, dunque, quali valori economicamente apprezzabili, comprendono non solo gli elementi che incrementano il patrimonio dell'agente ma anche il frutto delle attività fraudolente a seguito delle quali si impedisce l'impoverimento del patrimonio», DI VIZIO F., *op. cit.* 57

[281] «*Non è quindi, un problema di astratta tipizzazione, che richieda sul punto concrete modifiche normative […]*», PICOTTI L., *Profili penali del cyberlaundering, cit.*, 608

[282] PICOTTI L., *op. cit.,* 609

[283] PICOTTI L., *op. cit.,* 609

[284] «*per attività economica deve intendersi, ai sensi del 2082 c.c, una attività organizzata al fine della produzione o dello scambio di beni o servizi*», ANTOLISEI F., *Manuale di diritto penale. Parte speciale – I.* XVI ed., Milano 2016

[285] è «*una delle forme in cui si manifesta l'attività economica*», ANTOLISEI F., *op. cit.*

[286] *Contra*, STURZO L., *op. cit.,* 25

[287] «*una qualsiasi operazione intesa ad ottenere un vantaggio avvelandosi di situazioni favorevoli*», ANTOLISEI F., *op. cit.*

[288] Riguardo le tecniche di cyberlaudering descritte nei paragrafi precedenti, quella del gioco d'azzardo *online* sembra non destare alcun problema riguardo la configurazione del delitto di autoriciclaggio. Sul punto,«*Ad es. se si opera attraverso un gambling on line illegale, si ha certamente un "impiego", in*

finanziaria anche con l'attività di cambiavalute[289], pertanto la conversione di criptovaluta in moneta legale o con altre criptovaluta potrà concorrere a configurare la fattispecie del delitto di autoriciclaggio.

Si potrebbe obiettare che quando il reato presupposto venga commesso *online*, ed anche la successiva operazione di riciclaggio, non si possa ammettere la configurazione del reato di autoriciclaggio in quando manchi qualsiasi attività volta a convertire la valuta virtuale o ad impiegarla in attività speculative. Infatti, non vi sarebbe una «*contaminazione del circuito economico lecito*»[290] senza che le criptovalute di origine delittuosa non vengano convertite con altre valute virtuali o con valute legali. Secondo alcuni autori[291], nonostante la mancanza della destinazione degli impieghi, il delitto di autoriciclaggio si configurerebbe ugualmente. Il bene giuridico tutelato dalla norma non sarebbe, secondo questa opinione[292], la tutela dell'ordine economico, in realtà è la «tracciabilità dei flussi finanziari»; pertanto, un soggetto che «muove proventi illeciti virtuali tra i nodi della rete, sarebbe comunque concretamente idonea a dissimularne la provenienza delittuosa, integrandosi così pienamente il delitto di autoriciclaggio.»[293].

È pacifico, poi, che ove il reato presupposto avvenga *online*, e la successiva fase

---

qualsiasi forma, dunque anche tramite pagamenti o trasferimenti elettronici del denaro o delle utilità di provenienza illecita via web, in un'attività che resta solo da stabilire se sia da qualificare come "economica" o "speculativa" (dovendosene escludere prima facie il carattere "finanziario" o "imprenditoriale") o se invece sia da considerare quale "mera utilizzazione o [...] godimento personale" per cui è prevista la non punibilità`, ai sensi del controverso comma 4. Ma a ben vedere i problemi interpretativi che si pongono non sono diversi da quelli che si presentano con riferimento a corrispondenti condotte tradizionali nel mondo reale (nella fattispecie: di fronte all'impiego in un comune gioco d'azzardo), non essendo la formulazione tecnico-giuridica della fattispecie incriminatrice ad impedirne di per sé ´ l'applicazione anche al cyberlaundering.», PICOTTI L., *op. cit.,* 609

[289] «*è da ritenersi finanziaria l'attività così qualificata dalle disposizioni del Testo Unico in materia (nella specie il riferimento è all'art. 106 del TUF) ovverosia "l'assunzione di partecipazioni (acquisizione e gestione di titoli su capitale di imprese), la concessione di finanziamenti sotto qualsiasi forma, la prestazione di servizi di pagamento (incasso e trasferimento di fondi, esecuzione di ordini di pagamento, emissione di carte di credito o debito), l'attività di cambiovalute"*» GULLO A., *Il delitto di autoriciclaggio al banco d prova della prassi: i primi (rassicuranti) chiarimenti della Cassazione* in *Diritto penale e processo*, n. 4/2017, 482

[290] STURZO L., *op. cit.*, 26

[291] STURZO L., *op. cit.*, 26

[292] «*eguali perplessità ricorrono sulla natura del bene giuridico tutelato dalla norma in questione: seppur, prima facie, la tutela dell'ordine economico, che troverebbe riscontro nella descrizione delle attività destinatarie dei proventi illeciti, sembrerebbe essere l'oggetto privilegiato di tutela del complesso art. 648 ter.1 c.p., in verità la tracciabilità dei flussi finanziari deve continuare ad essere ritenuto il bene giuridico tutelato dalla norma.*» STURZO L., *op. cit.*, 26.

[293] STURZO L., *op. cit.,* 26

di riciclaggio avvenga *offline*, necessitando cosi di essere convertito il provento del reato presupposto in valuta virtuale, allora si avrà realizzata perfettamente la fattispecie di riciclaggio o di autoriciclaggio in quanto condotta concretamente idonea a dissimulare la provenienza da reato del profitto.

Riassumendo, il *cyberlaundering* mediante criptovalute è idoneo ad integrare le tre distinte fattispecie trattate poc'anzi, ma ciò che è interessante è che il fenomeno del riciclaggio cibernetico non si risolve soltanto in suddette fattispecie. Infatti, vi sono nuovi reati presupposto e nuovi reati strumentali. L'innovazione tecnologica e la conseguente possibilità di commettere in rete o attraverso la rete ha infatti dato vita a nuovi reati presupposto

Riguardo i primi, un caso particolare è quello del c.d. *phishing*[294], con cui viene indotto un soggetto[295] a comunicare propri dati personali, come codici d'accesso o password di servizi home banking, per poi essere fraudolentemente utilizzati per generare profitti ai "*phishers*" con ingiusto danno della vittima. Ciò comporta la realizzazione di più condotte criminose quali, frodi informatiche (anche aggravate dal furto di identità digitale (ex art. 640-ter, comma 3, c.p.), truffe ex art. 640 c.p., acquisizione e cessione illecite di password (ex art. 615-quater c.p.), accessi abusivi a sistemi informatici o telematici (ex art. 615-ter, c.p.) ed altri delitti simili che diventano quindi reati presupposto dei delitti di riciclaggio, ovvero di impiego od anche di autoriciclaggio[296]. Infatti, i proventi dei suddetti reati possono ben essere oggetto materiale delle condotte descritte nei delitti di riciclaggio. La casistica giurisprudenziale a riguardo è piuttosto ampia[297], la quale ha ritenuto integrato il delitto di riciclaggio in seguito al *phishing*. Dopo aver carpito e utilizzato abusivamente le

---

[294] «*a sua volta non delinea di per sé un singolo reato, ma un complesso insieme di comportamenti illeciti nel Cyberspace, che possono integrare una pluralità di reati cibernetici ed, infine, sfociare nel cyberlaundering*», PICOTTI L., *op. cit.*, 611; il «*phishing può essere definito come una tecnica di social engineering, in quanto è una metodologia di comportamento sociale indirizzata a carpire informazioni personali oppure abitudini e stili di vita. L'etimologia del termine ne indica un'origine dubbia, derivante dall'unione delle parole "harvesting" con "password", ovvero "password" con "fishing" o, ancora, quest'ultima con "phreakin"*», FLOR R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Rivista italiana di diritto e procedura penale*, 2007, n. 2-3, 892

[295] «*inviando una falsa e-mail che appaia provenire dall'istituto bancario presso cui è appoggiato un suo conto corrente gestibile on line*», PICOTTI L., *op. cit.*, 611

[296] PICOTTI L., *op. cit.*, 611

[297] In specie GUP Milano, 29.10.2008, in Riv. giur. ec. az., 2009, n. 5, 111 s., nota di FLOR R.

credenziali d'accesso del servizio di *home banking* della vittima, viene effettuata una transazione indirizzata ad un terzo, il quale provvede con ulteriori trasferimenti a "ripulire" e quindi dissimulare la provenienza delittuosa dei proventi del *phishing*. Questo soggetto, pertanto, risponderà del delitto di riciclaggio se venga dimostrata la sua consapevolezza della provenienza delittuosa. A riguardo, la giurisprudenza della suprema corte di cassazione a Sezioni unite[298] in tema di dolo nella ricettazione, ritiene sufficiente il dolo eventuale; la rappresentazione del delitto presupposto, però, deve andare «al di la del mero "sospetto"»[299], che potrebbe manifestarsi con commissioni di importo inusualmente esagerato o dalla scarsa limpidità delle informazioni ricevute riguardo lo scopo della transazione o la provenienza dei fondi. Al *phisher*, invece, si potrebbe ascrivere la responsabilità per il delitto di autoriciclaggio ex art. 648-ter.1 nel caso in cui egli stesso effettui operazioni sulle somme derivanti dai reati commessi nell'attività di *phishing* o concorra con il terzo (ciò però potrebbe destare problematiche riguardo la violazione del principio del *ne bis in idem*).

Un altro reato presupposto di recente configurazione è rappresentato anche dalla frode informatica ex art. 640-ter (nel caso aggravata dal furto di identità digitale, comma 3 dello stesso articolo), che può ritenersi integrata nel caso di manipolazione delle *smart cards* trattate nei paragrafi precedenti[300]. Infatti, come già riferito, è possibile sia manipolare i dati memorizzati nei *chip* delle *smart cards*, sia l'identità del titolare. Integrando queste condotte «alterazione del funzionamento» o l'intervento «senza diritto» (e il conseguente ingiusto profitto con altrui danno), la frode informatica può ben assurgere a rango di reato presupposto ove il profitto venga impiegato, sostituito o trasferito con modalità concretamente idonee ad ostacolarne la provenienza delittuosa.

Accanto agli inediti reati presupposto, vi sono da considerare anche i nuovi reati «strumentali»[301], ossia reati il cui disvalore non viene assorbito dai reati di riciclaggio. Emblematico è il caso di utilizzo di *smart cards* contraffatte o alterate in precedenza

---

[298] Cass. Sez. un., 26.11.2009 (dep. 30.3.2010), n. 12433, Nocera

[299] PICOTTI L., *op. cit.*, 612

[300] «*la frode informatica ex art. 640-ter c.p. è prospettabile nel caso di avvenuto utilizzo di carte di credito, falsificate mediante modificazione della banda magnetica, grazie ad acquisizione illegittima dei codici di accesso segreti (PIN)*», Cass., sez. II, 15.4.2011, n. 17748

[301] PICOTTI L., *op. cit.*, 613

per effettuare operazioni di "lavaggio" di denaro sporco. In questo caso, il delitto configurabile[302] è quello di cui all'articolo 493-ter c.p.[303], ed è considerato come strumento, non come presupposto del reato di riciclaggio. Infatti, l'alterazione dei *chip* è già stata effettuata da terzi, e il mero utilizzo della carta «clonata» rappresenta un fatto diverso e distinto dalla falsificazione della *smart card*. Pertanto, la condotta di indebito utilizzo delle *smart cards* è punibile autonomamente (sotto il vincolo della continuazione col delitto di riciclaggio)[304] ed ascrivibile ad un altro soggetto, che si è servito delle suddette *smart cards* per compiere le operazioni di riciclaggio.

Riassumendo, sono considerati autonomi il reato informatico in senso stretto dell'art 493-ter e quello di riciclaggio mediante l'utilizzo di sistemi informatici o telematici (reato informatico in senso lato)[305].

Infine, ulteriori ipotesi di reati strumentali al riciclaggio "cibernetico" possono considerarsi l'art 494 c.p.[306], rubricato furto di identità digitale, ed anche l'art. 615-ter c.p., ossia il reato di accesso abusivo a sistema informatico o telematico, se la sua commissione permette di trasferire i proventi illeciti dopo aver abusivamente effettuato l'accesso a sistemi di *home banking*.

Concludendo, possiamo affermare come attualmente le norme del codice penale riescano a ricomprendere esaustivamente le nuove modalità di riciclaggio e di impiego

---

[302] «*Occorre, in proposito, considerare che la migliore giurisprudenza propende per la qualificazione nei termini di delitto di frode informatica (e non di indebita utilizzazione di carte di credito o equiparate) della condotta di colui che, servendosi di una carta di credito falsificata e di un codice diaccesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi*» Cass., Sez. 2, sent. n. 26229 del 09/05/2017 – dep. 25/05/2017, Rv. *contra* Cass., Sez. 6, sent. n. 1333 del 04/11/2015 – dep. 14/01/2016

[303] «*Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi*». Primo comma dell'articolo 493-ter c.p.

[304] «*nel caso di riciclaggio di carte di credito provenienti da delitto, perché rubate o clonate, l'indebita utilizzazione delle stesse non costituisce il reato presupposto del riciclaggio, ma un reato strumentale alla commissione del riciclaggio medesimo, ai sensi dell'art. 55, comma 9, d.lgs. 21 novembre 2007, n. 231*», Cass., sez. II, 24.10.2013, n. 47147

[305] PICOTTI L., *op. cit.*, 613

[306] Cass., sez. V, 8.6.2018 (dep. 19.7.2018), n. 33862

di profitti di provenienza delittuosa, ma ovviamente la persecuzione e repressione dei suddetti reati non è facilitata dall'utilizzo della rete e dei sistemi informatici. Infatti più che concentrarsi sulla persecuzione dei reati di riciclaggio sarebbe opportuno focalizzarsi sui sistemi di prevenzione e di contrasto. Nel corso dei paragrafi seguenti verranno analizzate le misure di contrasto al riciclaggio portate avanti dal legislatore di rango comunitario.

2.4.1 (*Segue)* Il riciclaggio mediante criptovalute e le relative problematiche di diritto penale parte generale

Le rivoluzioni tecnologiche determinano l'esigenza da parte del diritto di adeguarsi costantemente alle nuove e differenti manifestazioni fenomenologiche dei reati. Ciò avviene attraverso interpretazioni estensive delle norme esistenti (fino ad arrivare ad un pericoloso utilizzo dell'analogia), la creazione di nuove norme o la modifica di quelle vigenti[307].

Le ideologie alla base le rivoluzioni tecnologiche sono spesso ispirate dal desiderio di creare realtà senza diritto e senza controllo da parte dello stato, tutto nella più piena libertà e riservatezza; i principi ispiratori del protocollo *Bitcoin* scaturiscono, infatti, dai movimenti crittoanarchici che pongono al centro dell'attenzione la *privacy* e l'assenza dell'ingerenza del potere statale.

Per poter continuare a fornire lo stesso livello di protezione degli individui e dei beni giuridici tutelati è necessario che il diritto si evolva e stia al passo con la rapida evoluzione degli strumenti tecnologici[308]e i relativi comportamenti dell'uomo[309]. Un approccio conservatore che pretenda di far confluire la duttile realtà tecnologica nelle

---

[307] PICOTTI L., *Cybercrime* a cura di CADOPPI A., - CANESTRARI S., - MANNA A., Milano, 2019, 36 ss.

[308] SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tutela penale l'incriminazione dei "dual-use software*" in *Rivista Italiana di Diritto e Procedura Penale*, fasc. 2, 1 giugno 2017, 750

[309] «*Evidenti ragioni di interesse scientifico per il tema in esame discendono dalla dimensione ontologicamente sovranazionale ed aterritoriale di quell'ambiente immateriale denominato ciberspazio, che, oltre a rendere impervio il cammino di ricerca del materiale probatorio ed arduo l'accertamento dei fatti criminosi, suggerisce riflessioni critiche in ordine ai consueti criteri di determinazione del momento consumativo del reato e della legge penale applicabile*», RUGGIERO F., *Momento consumativo del reato e conflitti di giurisdizione nel* cyberspazio, *cit.,* 255

già esistenti categorie dogmatiche del diritto penale rischia di essere limitante ed impreciso. Infatti, in generale i reati commessi mediate l'utilizzo di sistemi informatici presentano nei propri elementi oggettivi peculiarità che li differenziano nettamente dagli illeciti così come siamo abituati a teorizzarli e interpretarli.

Innanzitutto, a proposito della struttura del reato e in particolare della nozione di "atti", "azione" ed "evento", è necessario evidenziarne le caratteristiche in relazione ai crimini commessi nel cyberspazio. L'azione nel cyberspazio si sovrappone e si confonde con l'evento, il quale viene da sempre considerato dalla dottrina come «*risultato esteriore, nettamente distinto dall'atteggiamento muscolare del reo e definibile a prescindere da esso*»[310], in quanto l'individuo con la propria azione mette in moto un processo articolato in più "azioni" il cui risultato è difficilmente percepibile "naturalisticamente"; è arduo qualificare l'azione dell'uomo come attività di carattere esteriore[311], in quanto essa ha effetti percepibili in senso logico-informatico (in forma di codice binario). L'azione dell'individuo nella maggior parte dei casi non è quella descritta dal "fatto" del reato, ma sarà l'esecuzione automatica da parte dei sistemi informatici ad essere rilevante per la tipicità della norma incriminatrice. Ciò determina anche che l'evento del reato perde la sua connotazione materiale, intesa come modificazione della realtà esteriore, fondendosi con l'evento[312].

Inoltre, ulteriori problematiche sorgono in relazione l'applicazione spaziale della legge penale e il *tempus commissi delicti*.

Riguardo la prima questione, la sua soluzione è rilevante per la determinazione della giurisdizione e competenza. È ormai indubbio che il cyberspazio non ubbidisce alla logica territoriale dei confini nazionali, a differenza degli ordinamenti statali che

---

[310] GROSSO F., C., - PADOVANI T., - PAGLIARO A., *Trattato di diritto penale,* Milano, 2007

[311] MARINUCCI G., - DOLCINI E., - GATTA G., L., *Manuale di diritto penale – Parte generale*, Milano, 2018

[312] «*Sul piano tecnico, la Rete si pone come un articolato sistema di elaboratori elettronici in collegamento telematico, diffuso in tutto il mondo e capace di annullare qualsiasi distanza di tempo e di luogo, rendendo accessibili informazioni ad una sfera illimitata di persone in brevi scansioni cronologiche ed a basso costo. A differenza degli altri mass-media Internet presenta uno spazio di operatività geografica preventivamente non delimitabile, una struttura aperta ed uno sterminato numero di connessioni; mancando una forma di organizzazione gerarchica, la Rete risulta "anarchica", «acefala» e decentralizzata: si fonda, in definitiva, soltanto su un protocollo unitario relativo alla tecnica di trasferimento dei dati, che garantisce il collegamento a tutti i computers aderenti alla suddetta procedura»,* RUGGIERO F.*, op. cit.,* 255

richiedono uno «*spazio sul quale esercitare la propria sovranità esclusiva*»[313]. Inoltre, la rete permette la deterritorializzazione dell'individuo, che può agire ed essere presente in più "luoghi informatici", come anche la detemporalizzazione delle azioni, ossia programmare e automatizzare complesse operazioni senza il necessario e simultaneo "contatto fisico" tra uomo e sistema informatico[314] (si pensi alla realizzazione di *criminal smart contracts* dove è possibile pianificare a monte il *software*, la cui esecuzione causerà l'evento rilevante per la norma incriminatrice solo successivamente e al verificarsi di determinate condizioni previamente stabilite ed automaticamente eseguite).

Le norme del codice penale rilevanti in questo caso sono gli artt. 3 e 6 c.p., riguardanti l'obbligatorietà della legge penale e i reati commessi nel territorio dello stato; fondamentale pertanto è determinare quando un reato commesso mediante l'uso della rete *internet* sia considerato come commesso nel territorio italiano e quando chi lo commette è considerato alla luce del codice come presente all'interno dei confini nazionali. È alquanto arduo riuscire a rispondere con certezza a tali quesiti, soprattutto tenendo presente la struttura decentralizzata delle *blockchain*.

Diverse sono le soluzioni prospettabili, poiché il registro dove vengono conservate le transazioni non è custodito in un solo luogo, ma ogni copia è conservata in ogni singolo nodo della rete, sparsi in tutto il pianeta[315].

Essendo il registro della *blockchain* ubiquitario e rappresentato in più copie, probabilmente l'unico elemento che distingue un blocco dagli altri è il *miner* che ne ha permesso la concatenazione. Una soluzione potrebbe essere quella di considerare una transazione avvenuta nel luogo in cui il *miner* ha risolto l'indovinello crittografico e ha "agganciato" il blocco alla *blockchain*. Questa soluzione, però, comporterebbe una perenne incertezza sul "dove" la transazione è stata aggiunta al registro. Inoltre,

---

[313] «*In particolare, al fine di inquadrare il tema della giurisdizione e della competenza in rapporto agli illeciti commessi per mezzo di Internet, occorre porre a raffronto due elementari constatazioni: la prima è che Internet ignora i confini territoriali e, dunque, la territorialità degli ordinamenti giuridici; la seconda è che gli ordinamenti giuridici necessitano invece di uno spazio sul quale esercitare la propria sovranità esclusiva e ulteriormente tendono ad allargare i propri confini applicativi sulla base di valutazioni legate alla qualità del soggetto attivo o del soggetto passivo o alla natura del reato commesso*.» SEMINARA S., *Locus commissi delicti, giurisdizione e competenza del cyberspazio,* 1, in http://informaticagiuridica.unipv.it/convegni/2012/SEMINARA%2023-11-2012.pdf

[314] FLOR R., *Phishing, identity theft e identity abuse, cit.,* 930

[315] ANTONOPOULOS M. A., *Mastering bitcoin, cit.,* 4

bisogna anche non dimenticare che una transazione affinché venga considerata come stabilmente inserita in un blocco valido, sia necessario che vengano aggiunti successivamente ad esso più blocchi, circa sei[316]; può capitare infatti in caso di *fork* che una transazione venga aggiunto in un blocco che poi, in virtù del principio della catena più lunga, diventi un blocco "orfano" con il conseguente confluire delle transazioni in coda per essere aggiunti ai nuovi blocchi (che verranno aggiunti al ramo della catena più lunga)[317]. Quindi può accadere che seppur una transazione viene inserita in un blocco valido "minato" da un *miner* situato in un determinato paese, si considererà come stabilmente inserita nella *blockchain* nel momento in cui un altro *miner* vada ad aggiungere il sesto blocco successivo. Inoltre, in tutto ciò vi è un lasso di tempo (circa ogni 10 minuti viene aggiunto un nuovo blocco), che crea cosi uno scollamento temporale tra quando il soggetto agente ha effettivamente trasmesso la transazione e quando la stessa venga considerata come avvenuta. Ovviamente è impensabile un reato consumato che poi venga "annullato", pertanto è bene considerare con attenzione anche quando è possibile affermare che una transazione sia effettivamente conclusa.

Un ostacolo alla verificazione del luogo geografico dell'individuo che trasmette la transazione al *miner* è, come esposto nei paragrafi precedenti, l'utilizzo di VPN e di *browsers* con crittografia stratificata. Dal punto di vista informatico, anche se fisicamente il soggetto agente agisce da un *computer* situato in Italia, risulterà come connesso a dei *server* ubicati in altri paesi, creando cosi notevoli difficoltà anche dal punto di vista probatorio e dell'effettiva applicazione della giurisdizione italiana.

Per quanto riguarda il *locus* ed *il tempus comissi delicti* del delitto di riciclaggio, considerando che esso è un reato istantaneo[318], la soluzione preferibile sarebbe quella di considerare il luogo e il momento in cui il soggetto trasmette la transazione[319], in quanto, seppur di difficile accertamento in virtù dei motivi di cui sopra, per lo meno non rimane in balia della ubiquità del sistema di *mining* con tutte le sue insite incertezze riguardo dove e quando iscriverà la transazione in un blocco. Inoltre, questa soluzione

[316] V. *supra* § 1.7.1
[317] V. *supra* § 1.7.1
[318] GAROFOLI R., *Manuale di diritto penale parte speciale*, Molfetta, 2017
[319] «*è abbastanza pacifico sostenere che si ha perfezione nel momento e nel luogo della realizzazione della sostituzione, del trasferimento o delle altre operazioni costituenti ostacolo alla identificazione*» FIORE S., *I reati contro il patrimonio*, Milano, 2010

dovrebbe essere la più efficiente in termini di persecuzione del reato in quanto la giurisdizione sarebbe così affidata allo stato in cui il soggetto agente fisicamente opera ed agisce.

Nel caso degli *exchange*, che permettono scambio di criptovalute detenute tra gli utenti registrati alla piattaforma, o la conversione di valuta fiat con valuta virtuale, si potrebbe sostenere che il reato si consumi nel luogo dove essi hanno sede in quanto essi permetto e gestiscono le transazioni. Questa soluzione però non potrebbe convincere in quanto l'*exchanger* opera solo come intermediario tra l'utente che desidera convertire la valuta in suo possesso e coloro i quali vorrebbero vendere le valute in loro possesso, venendo iscritta la transazione alla *blockchain* di *bitcoin* con le stesse modalità di qualsiasi altra transazione avvenuta senza l'intermediazione di terzi, ossia attraverso i *miners* e il meccanismo del consenso distribuito.

2.5 La V Direttiva antiriciclaggio e il D.lgs. 25 maggio 2017, n. 90

Il fenomeno del riciclaggio e i suoi risvolti sul tessuto economico e finanziario sono stati oggetto nel corso degli anni di numerosi interventi legislativi volti a contrastarne gli effetti dannosi.

A proposito basti citare la Risoluzione del Comitato dei Ministri del Consiglio d'Europa del 1980, come anche nel 1988 la dichiarazione dei principi per la prevenzione dell'utilizzo del sistema bancario per il riciclaggio di fondi di origine illecita, promulgata dal Comitato di Basilea[320]. Successivamente, con la Convenzione di Vienna del 1988 gli stati aderenti si impegnarono a implementare nel proprio ordinamento una fattispecie penale che incriminasse le condotte di trasferimento, conversione, dissimulazione di proventi derivanti da reati connessi alle sostanze stupefacenti.

I primi atti legislativi di rango comunitario prendono forma nel 1991 con la direttiva 91/308/CEE, e via via si sviluppa una stretta correlazione tra il contrasto al finanziamento del terrorismo e la prevenzione del riciclaggio come abuso del sistema finanziario.

[320] RISPOLI FARINA., in RUGGIERO C., *La nuova disciplina dell'antiriciclaggio*, Torino, 2009

Nel corso del tempo sono entrate in vigore diverse Direttive, in particolare, nel 1991 venne introdotta la c.d. prima direttiva antiriciclaggio (Direttiva n. 91/308/CEE), che prevedeva obblighi di prevenzione solo in capo ad entri creditizi e finanziari.

Successivamente, la seconda direttiva antiriciclaggio (Direttiva 2001/97/CE) estende gli obblighi anche ai soggetti non finanziari. La Direttiva 2005/60/CE e la IV Direttiva (2015/849) hanno comportato innovazioni, obblighi più specifici ed una limitata estensione dei soggetti coinvolti.

Più recentemente nel maggio 2018 è stata emanata la V Direttiva[321] (2018/843 del parlamento europeo e del consiglio del 30 maggio 2018), la quale ha di fatto esteso l'ambito applicativo della normativa antiriciclaggio e ha interessato specialmente le criptovalute e i soggetti che operano professionalmente con esse. La proposta di suddetta direttiva è avvenuta nel 2016 a seguito del proliferarsi degli attentati terroristici[322] ed anche a causa del noto scandalo "*Panama papers*"[323], che hanno spronato l'Unione Europea a implementare misure più stringenti ed efficaci andando a modificare quella che è la IV direttiva antiriciclaggio[324]. Il legislatore italiano, invece, ha emanato nel 2017 il D.lgs. n. 90/2017[325] in attuazione della IV direttiva, e nel farlo ha in concreto anticipato alcune delle previsioni contenute nella V direttiva che verranno illustrate di seguito più avanti.

---

[321] Pubblicata nella Gazzetta Ufficiale UE del 19 giugno 2018, entrata in vigore il ventesimo giorno successivo alla data di pubblicazione. Ai sensi dell'art. 4 della Direttiva Ue 2018/843 gli Stati membri, entro il 10 gennaio 2020, dovranno conformarsi recependo le disposizioni legislative, regolamentari e amministrative a tal fine necessarie., DE VIVO A., - TRINCHESE G., *Le novità della V direttiva antiriciclaggio*, in *Documenti di ricerca della fondazione Nazionale dei commercialisti*, reperibile al seguente link http://www.dirittobancario.it/news/antiriciclaggio/le-novita-della-v-direttiva-antiriciclaggio-analizzate-dalla-fondazione-dei-commercialisti

[322] In particolare gli attacchi di Parigi del 13 novembre 2015, di Bruxelles del 22 marzo 2016 e la strage di Nizza del 14 luglio dello stesso anno

[323] https://www.lastampa.it/2016/04/03/esteri/panama-papers-miliardi-in-paradisi-fiscali-coinvolti-i-leader-del-mondo-e-oo-italiani-H8lq5CzzH72TzRIn9QA6ZO/pagina.html

[324] Direttiva (UE) 2015/849 del Parlamento Europeo e del Consiglio del 20 maggio 2015 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione.

[325] Decreto legislativo 25 maggio 2017, n. 90 Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006.

Generalmente, la normativa europea e italiana antiriciclaggio si configura come un insieme di disposizioni di *compliance* a cui gli operatori professionali devono adeguarsi predisponendo determinate misure volte a rendere più difficoltose le operazioni di ripulitura di capitali illeciti[326].

I punti fondamentali delle normative antiriciclaggio sono la conoscenza del cliente e della sua operatività, la comunicazione di attività sospette all'UIF[327] e la costituzione di adeguati presidi organizzativi[328]. Nel caso di operazioni poco "limpide" poiché incoerenti con le disponibilità economiche del cliente o incompatibili con la sua attività svolta, ci si potrebbe trovare a operazioni "sospette". Pertanto, i soggetti obbligati ad essere *compliant* con le disposizioni delle normative antiriciclaggio devono organizzarsi in modo tale da procedere adeguate verifiche sulla provenienza dei fondi, sulla relativa titolarità effettiva, cosi come l'attività professionale da esso svolta[329].

Nel caso delle criptovalute, l'unico modo per poter porre un freno o quantomeno un controllo all'inquinamento dell'ordine economico finanziario è porre degli obblighi di verifica e segnalazione in capo ai soggetti che permettono l'entrata e l'uscita dal mondo "virtuale"[330], andando a creare una sorta di "dogana" in modo tale da non inquinare la valuta reale con criptovalute di provenienza delittuosa[331]. Questo tipo di

---

[326] DANIELLI A., - GENDUSA M., - DI MAIO M., - RINALDI G, *bitcoin e criptovalute, cit*., 35

[327] Unità di informazione finanziaria, l'*«UIF riceve e acquisisce informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo, ne effettua l'analisi finanziaria e, su tali basi, ne valuta la rilevanza ai fini della trasmissione agli organi investigativi (Nucleo speciale di polizia valutaria della Guardia di finanza-NSPV e Direzione investigativa antimafia-DIA) e della collaborazione con l'Autorità Giudiziaria. L'Unità assicura altresì la trasmissione alla Direzione Nazionale antimafia e antiterrorismo dei dati ed effettua le analisi richieste. In particolare, l'Unità riceve e analizza le segnalazioni di operazioni sospette inviate dai soggetti obbligati; riceve, inoltre, comunicazioni oggettive concernenti operazioni a rischio di riciclaggio o di finanziamento del terrorismo individuate sulla base di criteri oggettivi in apposite istruzioni attuative, nonché il flusso mensile di segnalazioni aggregate da parte degli intermediari finanziari»* http://uif.bancaditalia.it/sistema-antiriciclaggio/uif-italia/index.html

[328] DANIELLI A., - GENDUSA M., - DI MAIO M., - RINALDI G, *op. cit*., 35

[329] LUCEV R., - BONCOMPAGNI F., *Criptovalute e profili di rischio penale nelle attività degli exchanger*, in *Giurisprudenza penale* n. 3/2018, 3

[330] DI VIZIO F., *Le cinte daziarie del diritto penale, cit*., 23*;* MAJORANA D., *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web,* in *Corriere Tributario*, n. 8/2018, 634

[331] *è stato introdotto l'obbligo di adeguata verifica della clientela a carico degli scambiatori (exchanger), che svolgono una funzione assimilabile alle porte poste lungo le antiche cinte daziarie: infatti gli exchanger, sono gli unici operatori che, cambiando le criptovalute in moneta reale e viceversa, sono in grado di identificare le persone che danno luogo a tali transazioni. In tal modo, la regolamentazione degli scambiatori di bitcoins (e criptovalute in generale) potrà avere il massimo*

soluzione quindi ha il pregio di rendere più difficoltose le operazioni di riciclaggio in quanto renderebbe rischiosa la conversione in valuta fiat. Però, non è estremamente efficace in quanto grazie alle tecniche di *mixing* è possibile rendere impervia la ricostruzione dello storico di una transazione e del relativo soggetto agente permettendogli di riutilizzare le criptovalute "mixate" per l'acquisto di beni o servizi.

Come anticipato poc'anzi, nell'implementare la IV Direttiva il legislatore italiano ha introdotto nell'ordinamento italiano disposizioni innovative rendendolo il capofila rispetto agli altri stati membri[332]. È stata fornita, come anticipato (v. *supra,* cap I, §1.9), una definizione di valuta virtuale[333] ed anche dei prestatori di servizi relativi all'utilizzo delle valute virtuali[334] i quali sono stati assoggettati agli obblighi di *compliance* antiriciclaggio. Infatti, modificando la disciplina dei cambiavalute (ad opera dell'art.8 del d.lgs. n. 90/2017 che modifica l'art. 17-*bis* del D.lgs. 13 agosto 2010, n. 141 introducendo i commi 8-*bis* e 8-*ter*) i suddetti prestatori di servizi sono obbligati ad iscriversi in una apposita sezione speciale del registro dei cambiavalute ai sensi dell'art. 128-*undecies* del T.U.B estendendo quindi ad essi la disciplina dei cambiavalute e quindi anche a quella antiriciclaggio. Cosi facendo, il legislatore ha imposto agli *exchange* di criptovalute di predisporre presidi per effettuare l'"adeguata verifica" e provvedere all'eventuale successiva segnalazione di operazioni sospette.

Sorprendentemente, però, ai suddetti obblighi sono sottratti i prestatori dei servizi di *wallet* digitale (i quali invece vengono esplicitamente ricompresi tra i soggetti obbligati dalla V Direttiva Antiriciclaggio), nonostante nella definizione dei prestatori di servizi relativi si faccia riferimento a servizi di «conservazione di valuta virtuale». Infatti, vengono imposti gli obblighi della normativa antiriciclaggio a prestatori di servizi relativi all'utilizzo di valuta virtuale «*limitatamente allo volgimento dell'attività*

---

effetto con il minimo investimento di risorse e massima concentrazione dei controlli», MAJORANA D., *op. cit.,* 634

[332] ACCINNI G., P., *Profili di rilevanza penale delle "criptovalute, cit.,* 17

[333] Articolo 1, comma 2 lettera qq) del D.lgs. 21 novembre 2007, n. 231, come modificato dal D.lgs. 25 maggio 2017, n. 90. «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»

[334] Articolo 1, comma 2 lettera ff) del D.lgs. 21 novembre 2007, n. 231, come modificato dal D.lgs.25 maggio 2017, n. "prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso"

di conversione di valute virtuali da ovvero in valute aventi corso forzoso», quindi lasciando fuori i *wallet provider*.[335]. L'incongruenza è palese, in quanto è risaputo che anche i *wallet provider* giocano un ruolo essenziale nell'attività dei criminali informatici e rischia di lasciare senza controllo le criptovalute che rimangono del circuito "virtuale" e che non vengono quindi convertite. Per l'utilizzo delle criptovalute e per la relativa "ripulitura" non è sempre necessaria la loro conversione[336], e di ciò il legislatore europeo ha tenuto conto nell'emendare le disposizioni della IV direttiva.

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

Nonostante questa pecca, la normativa italiana contiene previsioni particolarmente efficaci. In particolare, l'*exchanger* viene gravato di diversi obblighi. Uno di questi è espresso dall'articolo 17 e ss. d.lgs. 231/2007 come emendato dall'D.lgs. 90/2017, secondo cui i soggetti obbligati «*procedono all'adeguata verifica*» del cliente provvedendo ad identificarlo; ciò avviene tramite i dati identificativi forniti (documenti di identità) e la relativa verifica (confrontandoli con i dati in possesso da una fonte esterna ritenuta come affidabile). L'obbligo di adeguata verifica però sorge solo in occasione «*dell'instaurazione di un rapporto continuativo o del conferimento dell'incarico per l'esecuzione di una prestazione professionale*», oppure «*in occasione*

[335] NADDEO M., N*uove frontiere del risparmio, cit*., 103

[336] CARLISLE D., *Virtual Currencies and Financial Crime. Challenges and Opportunities*, Royal United Services Institute for Defence and Security Studies, *Occasional Paper*, marzo 2017, 14

dell'esecuzione di un'operazione occasionale, disposta dal cliente, che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che sia effettuata con una operazione unica o con più operazioni che appaiono collegate per realizzare un'operazione frazionata.».

Invece, si procederà alla adeguata verificata in ogni caso, a norma del comma 2 dell'art. 17, in caso di «*sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile*» e in caso di «*dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione*». In occasione di instaurazione di rapporti continuativi vi è l'obbligo di acquisire e valutare le «*informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale*»[337] ma in caso di «*elevato rischio di riciclaggio*» i suddetti controlli devono essere effettuati anche in caso di prestazioni occasionali (art. 18 lett. c)).

Sono poi previste due tipologie di obblighi di verifica: l'art. 23 del d.lgs. 231/2007 relativo agli obblighi semplificati (*simplified due diligence*)[338] mentre l'art. 25 tratta gli obblighi rafforzati di adeguata verifica (*enanched due diligence*)[339], le quali verranno adempiute in relazione al rischio rilevato (art.19 comma 2 d.lgs. 90/2017).

Agli obblighi di adeguata verifica e controllo seguono gli obblighi di segnalazione all'UIF dell'art. 35 del d.lgs. 231/2007 in caso di operazione sospetta quando gli exchange «*quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano*

---

[337] «*per tali intendendosi, quelle relative all'instaurazione del rapporto, alle relazioni intercorrenti tra il cliente e l'esecutore, tra il cliente e il titolare effettivo e quelle relative all'attività lavorativa, salva la possibilità di acquisire, in funzione del rischio, ulteriori informazioni, ivi comprese quelle relative alla situazione economico-patrimoniale del cliente, acquisite o possedute in ragione dell'esercizio dell'attività.*»

[338] «*in presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, i soggetti obbligati possono applicare misure di adeguata verifica della clientela semplificate sotto il profilo dell'estensione e della frequenza degli adempimenti previsti dall'art.*»

[339] «*soggetti obbligati, in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo, adottano misure rafforzate di adeguata verifica della clientela acquisendo in- formazioni 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*»

da attività criminosa»[340], corredati dal rispettivo obbligo *erga omnes* di riservatezza all'art. 39 nei riguardi del cliente o di terzi sull'avvenuta segnalazione, sull'esistenza di indagini o sull'invio di informazioni all'UIF[341].

Il decreto legislativo 90/2017 ha inoltre emendato anche l'apparato sanzionatorio della disciplina antiriciclaggio. A proposito la legge delega[342] aveva indirizzato il Governo ad un regime sanzionatorio caratterizzato da pene meno severe e limitate ai casi di particolare gravità, e questo risultato è stato raggiunto con l'art. 55 del d.lgs. 231/2007 (cosi come modificato dal d.lgs. 90/2017).

Ai primi commi sono stati introdotti tre nuove e distinte fattispecie di reato applicabili nel caso di gravi violazioni[343] degli obblighi di adeguata verifica, di conservazione delle informazioni raccolte e degli obblighi di fornire informazioni veritiere[344]. Nello specifico, il primo comma dell'art. 55 punisce condotte di falsificazione di «*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*» e di utilizzazione di dati e informazioni falsi della stessa tipologia durante le procedure di adeguata verifica (ovviamente andrà dimostrata la conoscenza della falsità dei dati e delle informazioni da parte del soggetto attivo, dovendo essere sufficiente anche il mero dolo eventuale[345]).

Il secondo comma dell'art. 55 invece punisce le condotte di acquisizione o conservazione di dati falsi o non veritieri («*sul cliente, sul titolare effettivo,*

---

[340] Inoltre, viene specificato che il sospetto è da evincersi «*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*»

[341] Art. 39 (Divieto di comunicazioni inerenti le segnalazioni di operazioni sospette). - «*1. Fuori dai casi previsti dal presente decreto, è fatto divieto ai soggetti tenuti alla segnalazione di un'operazione sospetta e a chiunque ne sia comunque a conoscenza, di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo.*»

[342] N.170/2016, articolo 15, lett. h, n.1

[343] «*Le fattispecie previste dall'art. 55, comma 1 e 2, d.lgs. 231/2007, dopo la riforma del 2017, risultano innervate attorno a condotte provviste di sviluppati caratteri fraudolenti e decettivi; condizione che pone seri problemi di delimitazione rispetto alle tradizionali fattispecie penali del riciclaggio*» DI VIZIO F., *op. cit.,* 56

[344] KROGH M., *Gli obblighi e le nuove sanzioni antiriciclaggio nel d.lgs. 25 maggio 2017, n. 90*, in *Notariato*, n. 5/2017, 166

[345] ACCINNI G., P., *Op. cit.*, 25

sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale e sull'operazione») e l'avvalersi di mezzi fraudolenti al fine di pregiudicare la corretta conservazione dei suddetti dati e informazioni (in questo caso sarà rilevante l'accertamento del dolo specifico).

Infine, al terzo comma è stato introdotto una fattispecie di reato che vede come soggetto agente il cliente, il quale, assoggettato all'obbligo di fornire di dati necessari per l'espletamento della adeguata verifica, fornisce dati o informazioni falsi o non veritieri.

È rimasta, infine, intoccata la fattispecie contravvenzionale (punibile quindi anche se di carattere colposo) del quarto comma dell'art. 55 che punisce la violazione del divieto di comunicazione dell'art. 39 comma 1 e art. 41 comma 3 cosi come anche i commi seguenti.

Spostando l'attenzione sulla V Direttiva Antiriciclaggio, è possibile senza dubbio affermare che abbia portato nel panorama europeo novità di non poco conto. Come già accennato poc'anzi, l'impulso della modifica della IV direttiva antiriciclaggio discende dai recenti eventi di terrorismo internazionale e dal conseguente obiettivo di contrastare detto fenomeno[346] colpendone il suo finanziamento[347]. Le proposte volte a perseguire questo obiettivo spaziavano dallo smorzare gli effetti criminogeni delle valute virtuali

---

[346] Espressamente enunciato nei Considerando 1, «*La direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio costituisce il principale strumento giuridico per la prevenzione dell'uso del sistema finanziario dell'Unione a fini di riciclaggio di denaro e finanziamento del terrorismo. Tale direttiva, il cui recepimento è stato previsto entro il 26 giugno 2017, definisce un quadro giuridico efficiente e completo per il contrasto della raccolta di beni o di denaro a scopi terroristici prescrivendo agli Stati membri di individuare, comprendere e mitigare i rischi collegati al riciclaggio di denaro e al finanziamento del terrorismo.*» e 2, «*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 o che beneficiano di deroghe all'applicazione di obblighi giuridici che potrebbero essere non più giustificate. Per stare al passo con queste nuove tendenze è opportuno adottare ulteriori misure volte a garantire la maggiore trasparenza delle operazioni finanziarie, delle società e degli altri soggetti giuridici, nonché dei trust e degli istituti giuridici aventi assetto o funzioni affini a quelli del trust («istituti giuridici affini»), allo scopo di migliorare l'attuale quadro di prevenzione e di contrastare più efficacemente il finanziamento del terrorismo. È importante rilevare che le misure adottate dovrebbero essere proporzionate ai rischi.*».

[347] La definizione di finanziamento del terrorismo direttiva UE 2015/849, art.1 comma 5 «*la fornitura o la raccolta di fondi, in qualunque modo realizzata, direttamente o indirettamente, con l'intenzione di utilizzarli, o sapendo che sono destinati ad essere utilizzati, in tutto o in parte, per compiere uno dei reati di cui agli articoli da 1 a 4 della decisione quadro 2002/475/GAI del Consiglio*»,

al neutralizzare i rischi relativi agli strumenti di pagamento anonimi[348], ed anche al rafforzamento dei poteri delle autorità di controllo e della loro cooperazione.

Intervenendo sull'ambito applicativo, sono state introdotte norme che ricomprendono ed estendono l'obbligo di *compliance* della normativa antiriciclaggio ai prestatori di servizi relativi alla conversione delle valute virtuali ed anche ai prestatori di servizi di portafoglio digitale (è stato già sottolineato come nella normativa italiana essi non siano stati ricompresi tra i soggetti obbligati).

Inoltre, sono state introdotte novità in tema di misure di obblighi di adeguata verifica. Le novità in questione riguardano l'art. 13 della precedente direttiva antiriciclaggio, dove è stata aggiunta la possibilità di provvedere all'identificazione del cliente anche attraverso «*i mezzi di identificazione elettronica o i pertinenti servizi fiduciari di cui al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio o altre procedure di identificazione a distanza o elettronica sicure, regolamentate, riconosciute, approvate o accettate dalle autorità nazionali competenti*». La normativa italiana a proposito non ricomprende espressamente questa possibilità e pertanto il legislatore nazionale dovrà modificare l'art. 18 comma 1 d.lgs. n. 231/2007 per renderlo compatibile con la più recente direttiva[349].

Concludendo, nonostante le accortezze espresse nel considerando IX della V direttiva[350], la normativa italiana ma soprattutto la V Direttiva hanno il pregio di porre delle «*cinte daziarie*»[351] con funzione di filtro all'ingresso del mondo "reale".

Così facendo, ossia assoggettando gli *exchange* e i *wallet provider* agli obblighi di adeguata verifica e segnalazione, è possibile rendere meno agevole il *cyberlaundering* attraverso l'uso delle criptovalute caratterizzato sia dal far confluire la valuta legale nel mondo virtuale "ripulendola", sia dal far perdere le tracce (ostacolandone la ricostruzione della provenienza delittuosa) delle criptovalute profitto di reati commessi *online* dal registro della *blockchain*.

Però, da più parti si auspica un intervento legislativo che abbia una portata globale (in virtù della più volta considerata transnazionalità del cyberspazio) in quanto

---

[348] DE VIVO A., - TRINCHESE G., *Le novità della V direttiva antiriciclaggio*, *cit*., 7

[349] DE VIVO A., - TRINCHESE G., *op. cit.,* 15

[350] V. *Supra,* pag. 40

[351] DI VIZIO F., *op. cit.,* 53, e MAJORANA D., *Disciplina giuridica e fiscale delle criptovalute, cit.,* 630

assoggettare solo alcuni degli stati crea necessariamente dei "paradisi" dove i criminali possono far proliferare le proprie attività illecite[352].

2.6 L'abusivismo bancario e finanziario

I reati relativi all'esercizio abusivo e finanziario sono anch'essi rilevanti nel caso di utilizzo delle valute virtuali.

Prestandosi a utilizzi e funzioni teoricamente simili a quelli delle valute avente corso legale[353], è chiaro che le attività di emissione o erogazioni di finanziamenti sotto forma di criptovaluta possano sconfinare dall'area del non punibile andando a ledere i beni giuridici la cui protezione è affidata alle norme del TUB e del TUF.

Nel 2015 la Banca d'Italia pubblicava un *dossier* in cui si faceva presente come l'offerta al pubblico di valori virtuali e l'erogazione di servizi di cambio potesse concretare il rischio di una violazione delle prerogative degli intermediari autorizzati, assumendo rilevanza penale[354]. In particolare, «*le attività di emissione di valuta virtuale, conversione di moneta legale in valute virtuali e viceversa e gestione dei relativi schemi operativi potrebbero invece concretizzare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati (artt. 130, 131 TUB per l'attività bancaria e l'attività di raccolta del risparmio; art. 131 ter TUB per la prestazione di servizi di pagamento; art. 166 TUF, per la prestazione di servizi di investimento)*» (nel caso in cui le suddette attività vengano poste in essere da soggetti che l'esercitino professionalmente e non da privati).

In verità, in seguito all'emanazione del d.lgs. 90/2017 non sembra così lampante la configurazione delle suddette fattispecie penali[355]. Seppur alcuni Autori propendono per la tesi opposta, ritenendo configurabili i reati delle disposizioni speciali del settore

[352] ACCINNI G., P., *Op. cit.*, 29

[353] BOCCHINI R., *Lo sviluppo della moneta virtuale*, *cit.*, 29

[354] Reperibile al seguente link *https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf*

[355] DI VIZIO F., *op. cit.,* 60

bancario e finanziario[356], molte invece sono le voci che predicano cautela nell'affermare l'integrazione dei suddetti reati in virtù di un "pericoloso" utilizzo dell'analogia e del rispetto del principio di tassatività[357].

In virtù dell'introduzione del comma 8-*bis* all'art. 17-*bis* del d.lgs. 141/2010 è stato sancito l'obbligo per i prestatori di servizi relativi all'utilizzo delle valute virtuali di iscriversi una sezione speciale registro dei cambiavalute. Questa disposizione permette alle Autorità di vigilanza di poter esercitare un controllo sugli *exchange*[358](ma anche sui *waller provider*e i prestatori di servizi di *mixing*) ma non viene specificato quali siano le sanzioni conseguenti alla sua violazione. È possibile però affermare che sarà applicabile il comma 5 dell'art. 17 del d.lgs. 141/2010 che sanziona con un illecito amministrativo l'esercizio abusivo dell'attività di cambiavalute (sanzione che verrà irrogata dal Ministero dell'economia e delle finanze)[359].

Riguardo la configurazione delle fattispecie penali invece è necessario procedere per gradi. L'art. 132 del T.U.B., rubricato "Abusiva attività finanziaria", non sembra configurabile in quanto gli operatori professionali di servizi relativi all'uso delle criptovalute non erogano alcun tipo di finanziamento. La fattispecie, infatti, rimanda all'art. 106 del d.lgs. 385/1993 e al D.M n.53/2015[360], dove è definita l'attività di erogazione di finanziamento che palesemente non è possibile inquadrare nell'attività degli *exchange* o dei *wallet provider* (invero l'art. 132 T.U.B non è neanche richiamato tra quelli possibilmente configurabili dalla Banca d'Italia nel dossier del 2015).

---

[356] «*Se all'epoca di tali considerazioni poteva apparire dubbia la sussumibilità dell'attività propria degli exchanger entro le definizioni legali di attività bancaria, di raccolta del risparmio e simili – e, con essa, la configurabilità dei predetti reati di abusivismo bancario e finanziario –, oggi ogni incertezza appare superata dall'espresso riconoscimento di tale categoria da parte del legislatore, e dal contestuale obbligo di registrazione degli exchanger in una apposita sezione del registro dei cambiavalute (art. 17-bis d.lgs. 141/2010*», LUCEV R., - BONCOMPAGNI F., *op. cit.*, 2

[357] D'AGOSTINO L., *Operazioni di emissione, cambio e trasferimento di criptovaluta*, *cit.*, 8, DI VIZIO F, *op. cit.* 60 ss.; NADDEO M., *op. cit.* 104 ss., STURZO L. *Bitcoin e riciclaggio, cit.*, 23

[358] D'AGOSTINO L., *op. cit.*, 17

[359] D'AGOSTINO L., *op. cit.*, 18.; d'accordo sul punto anche NADDEO M., *op. cit.* 104 ss., e DI VIZIO F, *op. cit.* 61 ss.,

[360] Decreto del MEF del 2 aprile 2015, n. 53 (*"Regolamento recante norme in materia di intermediari finanziari in attuazione degli articoli 106, comma 3, 112, comma 3, e 114 del TUB e 7-ter, comma 1-bis, della legge 30 aprile 1999, n. 130"*), pubblicato nella Gazzetta Ufficiale della Repubblica Italiana n. 105 dell'8 maggio 2015

L'art. 130[361] e l'art. 131[362] T.U.B (rubricati Abusiva attività di raccolta di risparmio e Abusiva attività bancaria) sembrano anch'essi non configurabili[363] in virtù degli elementi costitutivi della fattispecie, rispettivamente l'"attività di raccolta del risparmio tra il pubblico" e l'esercizio del credito. Infatti, non è possibile affermare che gli *exchange* effettuino attività di raccolta di risparmio o esercizio del credito[364] cosi come definito dall'art. 11 comma 1 T.U.B[365].

Discorso simile per l'art. 131-*bis* T.U.B[366], che incrimina l'abusiva emissione di moneta elettronica. Questo reato più che configurabile dagli *exchange* o dai *wallet* providers, sembrerebbe interessare l'attività dei *miners* i quali di fatto con la propria attività "stampano" nuova valuta virtuale. Però, anche per questo reato viene stroncata la sua applicazione a causa della tassatività degli elementi costitutivi[367]: infatti, è stato già discusso precedentemente come le criptovalute non possano essere qualificate alla stregua di valuta elettronica secondo la definizione dell'art. 1, comma 1 lett. *h-ter* T.U.B[368].

Si potrebbe pensare di sottoporre i *miners* a limiti di emissione similarmente a quelli previsti per le valute elettroniche o a autorizzazione e controllo da parte delle

---

[361] «*Chiunque svolge l'attività` di raccolta del risparmio tra il pubblico in violazione dell'articolo 11 è punito con l'arresto da sei mesi a tre anni e con l'ammenda da euro 12.911 a euro 51.645*»

[362] «*Chiunque svolge l'attività` di raccolta del risparmio tra il pubblico in violazione dell'articolo 11 ed esercita il credito è punito con la reclusione da sei mesi a quattro anni e con la multa da euro 2.065 a euro 10.329*»

[363] DI VIZIO F, *op. cit.*, 63; D'AGOSTINO L., *op. cit.*, 13

[364] è da escludere «*dall'ambito operativo della norma sia i professionisti del trading diretto di criptovaluta, i quali offrono servizi di cambio di moneta reale in virtuale, e viceversa, senza alcun obbligo di rimborso; sia i professionisti del trading indiretto, che operano come meri intermediari tra la domanda e l'offerta di criptomoneta*», D'AGOSTINO L., *op. cit.*, 13

[365] «*Ai fini del presente decreto legislativo è raccolta del risparmio l'acquisizione di fondi con obbligo di rimborso, sia sotto forma di depositi sia sotto altra forma.*»

[366] «*Chiunque emette moneta elettronica in violazione della riserva prevista dall'articolo 114-bis senza essere iscritto nell'albo previsto dall'articolo 13 o in quello previsto dall'articolo 114-bis, comma 2, è punito con la reclusione da sei mesi a quattro anni e con la multa da 2.066 euro a 10.329 euro*»

[367] E comunque, parrebbe assurdo incriminare i *miners* per la loro attività, in quanto il loro lavoro è fondamentale per il funzionamento della *blokchain* delle criptovalute e perciò assoggettare al suddetto reato significherebbe di fatto negare la possibilità di utilizzare le valute virtuali.

[368] *«moneta elettronica»: il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento come definite all'articolo 1, comma 1, lettera c), del decreto legislativo 27 gennaio 2010, n. 11, e che sia accettato da persone fisiche e giuridiche diverse dall'emittente*

autorità di vigilanza, ma questa soluzione sarebbe incoerente non solo con i principi alla base della creazione dei valori virtuali, ma anche con quelli che regolano il libero esercizio dell'impresa.

Identiche considerazioni sono da farsi per l'art. 131-ter T.U.B[369], l'elemento costitutivo della fattispecie dei "servizi di pagamento" non permette di ricomprendere l'attività degli *exchange* o dei *wallet provider* nella definizione riportata all'art. 1 comma 1, lett. b) del D.lgs. 11/2010[370]. Infatti, sarebbe quasi inconcepibile considerare gli exchange come degli intermediari a cui gli utenti si affidano per inviare e ricevere criptovalute come fanno gli istituti bancari con i bonifici. Le criptovalute nascono proprio per creare un sistema di trasferimento di "monete" in assenza di un ente centrale che ne gestisca il funzionamento, ed è proprio attraverso il principio del consenso che le transazioni vengono elaborate e confermate.

Una breve considerazione invece sull'art. 1 comma 1 lett. b) n. 2) che richiama «l'attività di servizi che permettono prelievi in contante da un conto di pagamento»; sono presenti sul territorio nazionale e in tutto il mondo numerosi "ATM"[371] che permettono di acquistare bitcoin[372] (o altre criptovalute) o di ritirare denaro contante vendendo i propri bitcoin. Quest'operazione seppur nella pratica sia simile a quella effettuata dai comuni sportelli automatici, non è sostanzialmente assimilabile e senza dubbio non può attribuire la qualifica di attività di prestazione di servizi di pagamento ai proprietari dei suddetti ATM.

Le avvertenze pubblicate dalla Banca d'Italia nel 2015 richiamano anche l'art. 166 del T.U.F[373]. In quest'ultimo caso il principio di tassatività osta all'applicazione del

---

[369] «*Chiunque presta servizi di pagamento in violazione della riserva prevista dall'articolo 114-sexies senza essere autorizzato ai sensi dell'articolo 114-novies è punito con la reclusione da sei mesi a quattro anni e con la multa da 2.066 euro a 10.329 euro*»

[370] «*"servizi di pagamento": le seguenti attività: 1) servizi che permettono di depositare il contante su un conto di pagamento nonché' tutte le operazioni richieste per la gestione di un conto di pagamento; 2) servizi che permettono prelievi in contante da un conto di pagamento nonché' tutte le operazioni richieste per la gestione di un conto di pagamento; 3) esecuzione di ordini di pagamento, incluso il trasferimento di fondi, su un conto di pagamento presso il prestatore di servizi di pagamento dell'utilizzatore o presso un altro prestatore di servizi di pagamento: 3.1.esecuzione di addebiti diretti, inclusi addebiti diretti una tantum; 3.2.esecuzione di operazioni di pagamento mediante carte di pagamento o dispositivi analoghi; 3.3. esecuzione di bonifici, inclusi ordini permanenti*»

[371] *http://www.treccani.it/vocabolario/bancomat*

[372] Sono presenti in 72 paesi, e sono circa 4717 attualmente funzionanti. Fonte: *https://coinatmradar.com*

[373] «*1. È punito con la reclusione da uno a otto anni e con la multa da euro quattromila a euro diecimila chiunque, senza esservi abilitato ai sensi del presente decreto: 1. a) svolge servizi o attività di*

suddetto articolo in virtù del fatto che nella definizione di strumenti finanziari dell'art. 1 comma 2 T.U.F non si faccia alcun riferimento alle criptovalute.

In conclusione, sono molte le opinioni dissonanti[374] con la Banca d'Italia e che ritengono non integrarsi le fattispecie di abusivismo presenti nel T.U.B e T.U.F.; pertanto, soltanto con una modifica di ciascuna fattispecie sarebbe possibile ricomprendere gli *exchange*, i *wallet provider* e i *miners* tra i soggetti attivi dei suddetti reati.

In verità, è stato evidenziato come in alcuni casi gli *exchange* potrebbero mettere in atto attività rientranti negli istituti via via richiamati dalle fattispecie penali[375], e quindi andrà fatta un'analisi caso per caso a seconda dell'effettiva attività dell'*exchange*.

2.7 I reati tributari

L'utilizzo sempre più diffuso delle criptovalute e i profitti derivanti dalla loro conversione (a causa delle ampie fluttuazioni del relativo prezzo di mercato) hanno suscitato attenzione anche riguardo la configurabilità dei reati tributari *ex* D.lgs. 74/2000.[376]

---

investimento o di gestione collettiva del risparmio; b) offre in Italia quote o azioni di OICR; c) offre fuori sede, ovvero promuove o colloca mediante tecniche di comunicazione a distanza, prodotti finanziari o strumenti finanziari o servizi o attività di investimento; c-bis) svolge servizi di comunicazione dati.; 2. Con la stessa pena è punito chiunque esercita l'attività di consulente finanziario abilitato all'offerta fuori sede senza essere iscritto nell'albo indicato dall'articolo 31; 2-bis. Con la stessa pena è punito chiunque esercita l'attività di controparte centrale di cui al regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio, del 4 luglio 2012, senza aver ottenuto la preventiva autorizzazione ivi prevista.»

[374] Ad eccezione di LUCEV R., - BONCOMPAGNI F., *op. cit.*, 2 ss.

[375] *«Nello specifico, le considerazioni che precedono non risolvono ogni possibile fenomenologia delle attività concretamente svolte dai prestatori di servizi relativi alla valuta virtuale. È presente nell'esperienza di alcuni prestatori di servizi concernenti le valute virtuali che offrono remunerate prestazioni di custodia, intermediazione nel trasferimento e gestione delle valute virtuali, al di fuori quindi di conti utilizzati esclusivamente per la prestazione di servizi di pagamento. I prestatori dei servizi, inoltre, potrebbero consentire la costituzione di depositi in moneta virtuale secondo precisi tassi di cambio, obbligandosi a riconvertirli a richiesta del depositante in moneta legale, all'esito di impieghi intermedi in valute virtuali convertibili ed in tempi diversi dal primo cambio. Attività che potrebbero integrare forme di raccolta del risparmio tra il pubblico con l'acquisizione di fondi in valuta avente corso legale, convertibili in moneta virtuale a sua volta riconvertibili nei primi»*, DI VIZIO F, *op. cit.*, 63

[376] LUCEV R., - BONCOMPAGNI F., *op. cit.*, 5

È bene però accertare quale sia il regime fiscale delle criptovalute per determinare la configurabilità dei suddetti reati. In particolare verrà analizzato i profili fiscali riguardanti gli *exchanger*, i privati e i *miners* sia riguardo le imposte sui redditi IRES, IRPEF sia l'imposta sul valore aggiunto (IVA).

Innanzitutto, bisogna considerare le pronunce della Corte di Giustizia dell'Unione Europea[377] ed anche il parere emesso dall'Agenzia delle Entrate[378] che nelle proprie considerazioni cita e prende spunto la sentenza della Corte europea.

La Corte Europea in questa importante pronuncia ha ammesso che le operazioni di conversione di valuta fiat in valuta virtuale (e viceversa) se «*effettuate a fronte del pagamento di una somma corrispondete al margine costituito dalla differenza tra il prezzo di acquisto delle valute e quello di vendita praticato dall'operatore ai propri clienti costituiscono prestazioni di servizi a titolo oneroso.*»[379] In specie, le suddette operazioni rientrano tra le operazioni "*relative a divise, banconote e monete con valore liberatorio di cui all'articolo 135, paragrafo 1, lettera e), della direttiva 2006/112/CE*". Tali operazioni, «*pur riguardando operazioni relative a valute non tradizionali (e cioè diverse dalle monete con valore liberatorio in uno o più Paesi), costituiscono operazioni finanziarie in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento*».

Pertanto, la Corte di Giustizia sancisce la qualificazione delle sovra indicate prestazioni come esenti ai fini IVA in quanto rientranti nell'ambito applicativo dell'art. 135, paragrafo 1, lett. e) della direttiva 2006/112/CE.

L'Agenzia delle Entrate, invece, adotta un approccio che discerne i profitti degli operatori professionali relativi alla conversione di criptovalute (gli *exchange*)[380], dai profitti delle persone fisiche che detengono criptovalute (e che compiano operazioni di

---

[377] Corte di Giustizia UE, Sez. V, 22 ottobre 2015, Causa C-264/14, Skatteverket c. David Hedqvist, con nota di CAPACCIOLI S., *Bitcoin: le operazioni di cambio con valuta a corso legale sono prestazioni di servizio esenti*, in *Il Fisco*, 2015

[378] Risoluzione N. 72/E., reperibile al seguente link https://www.agenziaentrate.gov.it/wps/file/nsilib/nsi/normativa+e+prassi/risoluzioni/archivio+risoluzioni/risoluzioni+2016/settembre+2016+risoluzioni/risoluzione+n.+72+del+02+settembre+2016/RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf

[379] Considerazioni dell'Agenzia delle Entrate sulla citata pronuncia della Corte Europea nella risoluzione N. 72/E

[380] DI VIZIO F., *op. cit.,* 65

acquisto e alienazione delle stesse).

I profitti degli operatori professionali, secondo la agenzia delle entrate sono rilevanti ai fini delle imposte IRES, IRAP e IVA.[381] Nel caso dell'IVA, però, l'ente riscossore italiano stabilisce l'esenzione dei proventi derivanti dall'attività di cessione e acquisto di criptovaluta in cambio di valuta avente corso legale con profitto («*pari al margine che scaturisce dalla differenza tra l'importo corrisposto dal cliente che intende acquistare/vendere bitcoins e la migliore quotazione reperita dal prestatore del servizio sul mercato*»[382]) in quanto è applicabile l'art 10, comma 1, n. 3) D.P.R 633/1972, riguardante le operazioni aventi ad oggetto valute estere aventi corso legale e i crediti in valute estere (eccettuati i biglietti e le monete da collezione e comprese le operazioni di copertura dei rischi di cambio)[383]

Detto ciò, non essendo redditi soggetti a imposizione, vengono meno i requisiti necessari per considerare l'applicazione dei reati enunciati nel d.lgs. 74/2000 agli art. 4, 5 e 10-ter. (rubricati rispettivamente Dichiarazione infedele, Omessa dichiarazione e *Omesso versamento di IVA*)[384].

Discorso diverso invece per l'IRES. L'Agenzia delle Entrate ha espressamente stabilito che i redditi degli *exchanger* derivanti dall'attività di intermediazione contribuiscono alla "*formazione della base imponibile soggetta ad ordinaria tassazione ai fini IRES*". Per tal motivo, è possibile ritenere configurabili i reati ascritti agli artt. 2 e 3 d.lgs. 74/2000 (*dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti e Dichiarazione fraudolenta mediante altri artifici*)[385] come anche (più verosimilmente[386]) i reati agli artt. 4 e 5 d.lgs. 74/2000[387] (sempre in caso di superamento delle soglie di punibilità).

---

[381] Risoluzione N.72/E

[382] V. Risoluzione N.72/E; sul punto, anche LUCEV R., - BONCOMPAGNI F., *op. cit.*, 5

[383] CAPACCIOLI S., *Introduzione al trattamento tributario delle valute virtuali: criptovalute e bitcoin* in *Diritto e pratica tributaria internazionale,* n.1/2014, 49; DI VIZIO F., *op. cit.,* 67. e LUCEV R., - BONCOMPAGNI F., *op. cit.*, 6

[384] DI VIZIO F., *op. cit.,* 67; LUCEV R., - BONCOMPAGNI F., *op. cit.* 6; CAPACCIOLI S. *op. cit.,* 49

[385] LUCEV R., - BONCOMPAGNI F., *op. cit.*, 5

[386] LUCEV R., - BONCOMPAGNI F., *op. cit.*, 6

[387] «*alla prima contestazione andrà incontro l'exchanger che presenti una dichiarazione annuale contenente elementi attivi per un ammontare inferiore a quello effettivo, mentre alla seconda contestazione andrà incontro l'exchanger che ometta del tutto la presentazione della dichiarazione annuale*» LUCEV R., - BONCOMPAGNI F., *op. cit.*, 6

Spostando invece il *focus* dell'attenzione sui *miners,* è bene tenere a mente che essi ricevono per ogni blocco aggiunto alla *blockchain* (v. *supra*, *proof of work*) un numero determinato di *bitcoin*[388] (attualmente 12.5 *bitcoin*, che al tasso di cambio attuale[389] corrispondono a circa 63779,28 Euro).

A proposito, è necessario inquadrare il regime fiscale dei *bitcoin* ottenuti come ricompensa per poter determinare la configurazione di eventuali reati tributari. È stato rilevato che se i *miners* abbiano organizzato le risorse necessarie alla loro "produzione", i relativi profitti rientrerebbero nel reddito di impresa abituale (art. 55 TUIR). In caso invece attività di impresa occasionale, i relativi profitti rientrerebbero nei redditi diversi (art. 67 TUIR). Dai primi è possibile dedurre i costi di produzione, i secondi invece vengono sottoposti a tassazione al lordo dei costi sostenuti[390].

Riguardo le persone fisiche che detengono criptovalute al di fuori del contesto dell'attività d'impresa, l'Agenzia delle Entrate si è espressa in favore della tesi che afferma che l'acquisto e vendita di criptovalute non vadano a generare redditi imponibili (in particolare, per l'assenza della finalità speculativa).

Per questo motivo, l'*exchanger* non sarà sanzionabile ex. art. 5, comma 1-bis d.lgs. 74/2000 (Omessa dichiarazione del sostituto d'imposta), in quanto esso non è tenuto ad alcun adempimento quale sostituto d'imposta[391]. Inoltre, sarà da escludere la rilevanza dei reati di omesso versamento, ossia l'art 10-bis e 10-ter, d.lgs. 74/2000, in quanto vi è assenza di un rapporto di sostituzione di imposta tra *exchanger* e persona fisica; relativamente al secondo, perché le operazioni con moneta virtuale sono esenti dall'imposta IVA.

Riassumendo, a seguito dell'inclusione dei redditi derivanti dall'attività degli *exchager* nell'alveo di applicazione dell'IRES, ed anche dei *miners* nell'ambito dei redditi di impresa, è possibile dunque ipotizzare un concreto rischio di configurabilità di reati tributari.

Pertanto, non solo le criptovalute possono essere dirette protagoniste dei reati di riciclaggio, ma l'effettuazione di attività professionale può comportare a configurare

---

[388] Il numero dei *bitcoin* ricevuti come ricompensa per l'energia computazionale offerta al sistema si riduce periodicamente

[389] Maggio 2019, fonte: *https://www.coingecko.com/it/monete/bitcoin*

[390] DI VIZIO F., *op. cit.,* 66

[391] LUCEV R., - BONCOMPAGNI F., *op. cit.*, 5; DI VIZIO F., *op. cit.,* 67

anche diverse tipologie di reati, non solo quelli relativi all'abusivismo, ma anche tributari. Tutto ciò a conferma del fatto che le criptovalute comportino rischi penali attivi su più fronti.

2.8 Conclusioni

Nel presente capitolo sono state evidenziate ed analizzate le possibili applicazioni pratiche delittuose delle criptovalute, con una specifica attenzione ai reati contro il patrimonio e di carattere finanziario.

È stato esposto come le caratteristiche intrinseche delle criptovalute e del cyberspazio dove esse "circolano" le rendano particolarmente appetibili per essere utilizzate per commettere reati di qualsiasi tipologia. I reati commessi *online* presentano peculiarità che ne rendono più agevole l'esecuzione e più ardua la repressione.

In particolare, il reato di riciclaggio, autoriciclaggio ed impiego di denaro, beni o altra utilità di provenienza illecita vedono come ideali l'utilizzo delle criptovalute proprio per la loro anonimità (pseudo-anonimità) e per l'esistenza di tecniche di *mixing* che permettono di ostacolare la ricostruzione delle transazioni nello storico della *blockchain*. È inoltre utile tener a mente che vi è la possibilità di dar vita a *software* la cui esecuzione automatica tramite *smart contracts* possono integrare le fattispecie delittuose di reati anche estremamente gravi.

Inoltre, è stata condotta un'analisi sulla possibilità di configurare i reati relativi all'abusivismo bancario o finanziario cosi come attualmente in vigore, constatando un impervio ostacolo nei principi di tassatività e nel divieto di estensione analogica in *malam partem*.

Infine, è stata accertata la possibilità di configurare i reati tributari del d.lgs. 74/2000 in seguito all'inclusione dei redditi derivanti dall'attività dei prestatori di servizi relativi alle criptovalute nei redditi rilevanti per le imposte IRES e IRAP (e non dell'IVA).

Le conclusioni che quindi si possono trarre sono le seguenti. Le criptovalute, purtroppo, così come sono state ideate e progettate, si prestano ad essere strumentalizzate per la configurazione di diversi reati, come anche per essere utilizzata

come “moneta” richiesta dai criminali o dalle loro vittime o come compenso per l’esecuzione di un’operazione illecita.

Il loro utilizzo non va però scoraggiato di sana pianta ma è necessaria una particolare attenzione a come vengono utilizzate. Ciò è possibile predisponendo degli efficaci presidi preventivi (come le norme antiriciclaggio) affinando le tecniche di investigazione e migliorando la cooperazione internazionale tra le autorità inquirenti.

CAPITOLO III

I PROFILI PROCESSUALI: *DIGITAL FORENSICS* E PROVE ELETTRONICHE

SOMMARIO: 3. I *cybercrimes* e le problematiche processuali. – 3.1. La prova digitale. – 3.1.1 (*Segue*) La prova digitale e la prova documentale. – 3.2 Le indagini digitali. – 3.2.1 (*Segue*) Le indagini sulla *blockchain*: cenni di ordine generale alla c.d. "*bitcoin forensics*". – 3.3. Le indagini informatiche e mezzi di ricerca della prova "tradizionali": la perquisizione, l'ispezione e sequestro di dati digitali. – 3.3.1 (*Segue*) Il sequestro della prova digitale. – 3.3.2 (*Segue*) Una panoramica delle questioni sul sequestro di *bitcoin*. – 3.3.3 (*Segue*) Il caso *Silk Road* e *Bitgrail*. – 3.3.4. I soggetti processuali nelle indagini informatiche. – 3.3.5. Conclusioni.

3. I *cybercrimes* e le problematiche processuali

Il diffondersi dei reati realizzati con l'utilizzo dei *computer* e della rete *internet* solleva problematiche non solo rilevanti per il diritto penale sostanziale, ma anche di tipo prettamente processuale.

Se prima dell'avvento delle recenti rivoluzioni tecnologiche le condotte materiali degli individui si realizzavano nel mondo "*offline*", ora le azioni e i "fatti" rilevanti per il diritto penale sono caratterizzati dalla loro appartenenza al mondo "virtuale"[392], privi di una materialità naturalistica[393]. Il diritto ha da sempre preso in considerazione «*beni corporali*» ed «*oggetti tangibili*»[394] che caratterizzavano in via esclusiva l'ambiente in

[392] «*Il concetto di condotta, teorizzato per una realtà fisica nella quale le conseguenze sono percepibili ed empiricamente verificabili nel luogo dove si trova l'agente, sfuma della dimensione virtuale*»: così CUOMO L., - RAZZANTE R., *La disciplina dei reati informatici*, Torino, 2007, 14 ss.

[393] «*il concetto di azione penalmente rilevante subisce nella realtà virtuale una accentuata modificazione fino a sfumare in impulsi elettronici; l'input rivolto al computer da un atto umano consapevole e volontario si traduce in un trasferimento sotto forma di energie o bit della volontà dall'operatore all'elaboratore elettronico, il quale procede automaticamente alle operazioni di codificazione, di decodificazione, di trattamento, di trasmissione o di memorizzazione di informazioni*». Cass., Sez. Un., 26 marzo 2015, ROCCO, in *Diritto penale e processo*, 2015, 1291 ss., con nota di FLOR R.

[394] CUOMO L., - RAZZANTE R., *La disciplina dei reati informatici*, Torino, 2007, 15 ss.

cui operava l'individuo, ma così attualmente non è, in quanto il progresso tecnologico ha portato ad una continua dematerializzazione della vita dei consociati[395].

Cambia il modo di interagire, di comunicare e di percepire il "reale". Ciò che è da sempre stato dotato di una propria entità materiale percepibile dai sensi, ora viene "digitalizzato" sotto forma di "dati", ossia di semplici *bit*. I bisogni dell'individuo che in altri tempi necessitavano di tempo e ingenti risorse per essere soddisfatti, ora possono essere espletati con il minimo sforzo attraverso pochi e semplici "*click*"[396].

Tutto ciò comporta che anche il modo con cui vengono commessi i reati è stato rivoluzionato dall'avvento degli strumenti elettronici e dalla rete internet (basti pensare alle truffe online, le diffamazioni e il riciclaggio solo per citarne alcuni).

È stato già evidenziato nel corso del precedente capitolo come le tecniche di *cyberlaundering* configurano il reato di riciclaggio attraverso condotte materiali e azioni che differenziano nettamente dal riciclaggio "tradizionale" (attraverso l'uso del contante).

Fatte queste considerazioni, anche il processo penale deve adeguarsi ed adattarsi alle nuove modalità di commissione dei reati[397]. Infatti, le prove perderanno la loro connotazione materiale, e saranno costituite da "dati" informatici; si assisterà sempre di più alla scomparsa di prove documentali in senso stretto, a favore di elementi probatori dematerializzati[398].

In particolare, nel caso della *blockchain* gli unici elementi oggetto di indagine possono essere le transazioni iscritte nel registro, come anche gli *address* degli attori delle transazioni. Pertanto, nei processi riguardanti i reati commessi tramite *computer* e rete *internet* si assisterà ad un uso sempre più frequente di "prove elettroniche". Non esistendo un registro cartaceo dell'elenco delle transazioni della *blockchain* consultabile o sequestrabile ai fini probatori, necessariamente si utilizzeranno nei procedimenti penali prove del suddetto tipo.

---

[395] CUOMO L., - RAZZANTE R., 14

[396] LUPARIA L., *Sistema penale e criminalità informatica*, Milano, 2009, 60 ss.

[397] In particolare, «*I* computer *possono essere gli strumenti necessari per la commissione di reati (soggetto attivo di delitti), possono contenere le prove dei crimini di tipo tradizionale (testimoni di delitti) oppure possono essere l'obiettivo di atti criminali (soggetto passivo di delitti*)» CUOMO L., - RAZZANTE R., 59.

[398] LUPARIA L., Computer crimes *e procedimento penale*, in GARUTI G. (a cura di), *Modelli differenziati di accertamento*, t. I, Torino, 2011., 4 ss.

Infine, la più volte sottolineata transnazionalità della suddetta tipologia di reato comporta notevoli questioni sotto i profili della competenza e della giurisdizione, ed anche fondamentali questioni in tema di cooperazione internazionale tra autorità giudiziarie e investigative[399].

3.1 La prova digitale

In seguito all'incremento dell'uso dei sistemi informatici e telematici è sempre più frequente assistere nei procedimenti penali all'esperimento di tecniche di indagine caratterizzate dall'elevato contenuto tecnologico ed anche dall'uso di prove c.d. "informatiche" o "digitali" (*electronic evidence*)[400]. Ciò ha portato i protagonisti dei procedimenti a misurarsi con prove contenute in *computer*, nella rete *internet* o su una *blockchain*, assistendo così al tramonto delle prove "tradizionali" come, ad esempio, la testimonianza.

È bene sottolineare che le prove digitali e le indagini informatiche non riguardano solo ed esclusivamente i c.d. *computer crimes* (in senso stretto)[401], ma hanno rilevanza

---

[399] SIGNORATO S., *Types and features of cyber investigations in a globalized world* (*Tipologie e caratteristiche delle "cyber investigations" in un mondo globalizzato)*. Relazione alla Conferenza biennale internazionale "Quinta sezione, scienze criminali, evoluzioni e tendenze nel diritto penale contemporaneo", Timisoara (Romania), 28 ottobre 2016, in *Diritto penale contemporaneo*, 2016, 3, 11.

[400] Seppur frequentemente utilizzati come sinonimi, i termini «*electronic evidence*» e «*digital evidence*» non sono totalmente sovrapponibili. Infatti tra le electronic evidence sono ricompresi non solo i dati digitali ma anche quelli analogici che possono essere rappresentati digitalmente. DI PAOLO G., *Prova informatica (diritto processuale penale)*, in *Enc. dir., annali*, VI, Milano, 2016, 736 ss.; sul punto, MARAFIOTI L., Digital evidence *e processo penale*, in Cass. pen., 2011, p. 4509., secondo cui la *digital evidence* è «*informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su di una determinata periferica, oppure dal fatto di essere stata trasmessa secondo modalità informatiche o telematiche*»; per un'ulteriore definizione di prova digitale, *«sono il complesso delle informazioni digitali che sono in grado di stabilire se un crimine è stato commesso o che possono rappresentare un collegamento tra un crimine e i suoi esecutori*» CASEY, Digital evidence and computer crime, in *Academic Press*, 2000, p. 196 ss.; altri autori, come MOLINARI F., M., *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013, p. 1261., propendono per una definizione che tenesse in considerazione in particolare la natura immateriale della prova, qualificandola come «*prova di natura digitale*»., PITTIRUTI M., Digital evidence *e procedimento penale* in *Processo penale e politica criminale*, a cura di PAOLOZZI G., - MOCCIA S., - MARAFIOTI L., - LUPARIA L., - MARCHETTI P., Torino, 2017, 7

[401] «*Questa categoria di reati informatici si connota per un nuovo oggetto passivo su cui la condotta va a cadere (quali i dati, le informazioni, i programmi od altri "prodotti" informatici o digitali, compresi i "sistemi informatici" in genere) oppure dal fatto che il computer ed i prodotti informatici in genere*

anche per i reati comuni[402], molti dei quali possono essere commessi mediante sistemi informatici o telematici[403].

Essendo i sistemi informatici protagonisti della vita sociale, lavorativa e privata degli individui, è del tutto fisiologico che i "dati" trasmessi, ricevuti e memorizzati avranno sempre più rilevanza a livello probatorio riguardo ai "fatti" del procedimento.

In particolare, le prove digitali presentano caratteristiche peculiari che le differenziano nettamente dalle prove che si è abituati a considerare[404].

Innanzitutto, ciò che *in primis* caratterizza le prove digitali è l'immaterialità[405]. Esse non sono altro che dati informatici, sotto forma di codice binario (stringhe di *bit*[406]), memorizzati in supporti fisici (come i *computer*) o fluttuanti nella rete *internet*. In virtù di quest'aspetto le prove digitali non sono tangibili[407], e per la loro esistenza non è imprescindibile un determinato supporto informatico poiché esse sono autonome ed indipendenti dalla *res* che li contiene[408], potendo essere duplicata e riprodotta infinite volte[409].

---

costituiscono lo strumento tipico di realizzazione del 'fatto' criminoso.», FLOR R., *Lotta alla "criminalità informatica"e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Diritto penale contemporaneo, 2012,* reperibile al seguente link: https://www.penalecontemporaneo.it/d/1676-lotta-alla-criminalita-informatica-e-tutela-di-tradizionali-e-nuovi-diritti-fondamentali-nell-era-d, 4 ss.

[402] DANIELE M., *La prova digitale nel processo penale* (Relazione, con integrazioni e note, svolta al Convegno "Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali", Como,21-22 maggio 2010), in *Rivista di diritto processuale*, 2011, 2, 283-298., 5 ss.

[403] Ad esempio, diffamazione, molestie e *stalking*. DI PAOLO G., *op. cit.,* 736

[404] «*Di fronte alle prove digitali i processualisti si trovano a disagio, in quanto sono abituati a pensare alle prove come a degli oggetti fisici, dotati di un'evidente corporeità`. Le prove digitali si presentano, invece, come entità immateriali*», DANIELE M., *op. cit.*, 284 ss.

[405] DI PAOLO G., *op. cit.*, 738 ss.; DANIELE M., *op. cit.*, 284 ss.

[406] «*zeroes and ones of electricity*» KERR O., Digital Evidence and the New Criminal Procedure, in 105 Colum. L. Rev., 2005, 291

[407] «*Ciò non significa che esse non abbiano una loro fisicità`: concettualmente si tratta di impulsi elettrici che rispondono ad una sequenza numerica prestabilita e che, convogliati in un supporto informatico dotato di una memoria, originano informazioni intellegibili. È però, una fisicità che, in assenza del supporto, non può essere percepita come tale*». DANIELE M., *op. cit.*, 284 ss.

[408] «*oggi nessuno dubita più del fatto che le prove digitali esistano indipendentemente dai supporti in cui si trovano, i quali sono solo involucri esterni di per sé processualmente irrilevanti. spesso vi è, anzi, un'assoluta sproporzione tra le prove digitali ed i loro recipienti: un supporto di piccole dimensioni è in grado di contenere una massa enorme di informazioni digitali*». DANIELE M., *op. cit.*, 285 ss.

[409] DI PAOLO G., *op. cit.*, 738 ss.

Le prove digitali sono anche "fragili"[410], poiché esse possono essere alterate, modificate e definitivamente eliminate sia ad opera del soggetto che ha dato vita ai dati oggetto della prova digitale, sia da investigatori poco attenti ed inesperti.[411]

Infatti, è fondamentale che il procedimento di acquisizione della prova sia condotto con l'utilizzo di tecniche altamente specialistiche in modo tale da non inquinare in alcun modo la prova rilevata ma anche da provvedere alla sua conservazione in modo sicuro ed efficace, a riparo da qualsiasi tentativo di manomissione[412].

Una delle tematiche fondamentali a cui gli investigatori debbono far più attenzione è conferire alla prova elettronica la c.d. «*resistenza informatica alle contestazioni*»[413], ossia la garanzia di integrità[414] e autenticità del dato informatico nell'ambito della sua «*continuità probatoria*»[415] (la c.d. "*chain of custody*", letteralmente "catena di custodia"[416]).

Data la specialità delle competenze necessarie all'acquisizione e conservazione delle prove digitali, vi è il rischio che una «*deriva tecnicista*»[417] porti ad una sostanziale

---

[410] DI PAOLO G., *op. cit.*, 740 ss.

[411] DANIELE M., *op. cit.*, 288 ss.; DI PAOLO G., *op. cit.*, 740 ss.

[412] A proposito, «*A titolo d'esempio, un file comune, quale una immagine in formato* jpg*, comprende circa un milione di* bit *42; la modifica di uno solo di essi può comportare un mutamento irreversibile, tanto che il file potrà apparire illeggibile o corrotto. Perché il dato sia alterato, è sufficiente che venga aperto una sola volta: quantomeno, infatti, sarà stato modificato il metadato relativo alla data di ultimo accesso, con il rischio che ne venga annullata la rilevanza probatoria*». PITTIRUTI M., *op. cit.*, 11

[413] ZICCARDI, *Scienze forensi e tecnologie informatiche*, in LUPÁRIA e ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007, 11

[414] «*la garanzia di aver mantenuto inalterati tutti i dati e lo stato del supporto fisico che li contiene durante le varie fasi del repertamento e dell'analisi*» ZICCARDI, *La procedura di analisi della fonte di prova digitale*, in LUPÁRIA e ZICCARDI, *op. cit.*, 65

[415] DI PAOLO G., *op. cit.*, 738; «la *possibilità di tenere traccia del procedimento di repertamento e analisi in ogni suo punto mediante la produzione di report a vari livelli di dettaglio*» ZICCARDI, *La procedura di analisi della fonte di prova digitale*, in LUPÁRIA e ZICCARDI, *op. cit.*, 65

[416] «*Chain of custody (CoC) refers to the process of documenting and maintaining the chronological history of handling digital evidence. Extreme care is required to protect CoC from being altered or destroyed unauthorizedly. The ultimate aim of CoC is to demonstrate that alleged evidence is, in fact, relevant to the alleged crimes instead of being falsely planted. Weak CoC leads to inadmissibility of digital evidence in the court of law*» AUQIB H., L., - ROOHIE N., M., *Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer in Digital Investigation* n. 28, 2019, 44 e ss.; «*Deve essere dedicata massima cura alla catena di custodia* (chain of custody) *ovvero alla metodologia di custodia e di trasporto, sia fisico sia virtuale delle* digital evidences*»,* Cass. 16 dicembre 2009 (dep.19 gennaio 2010), n. 2388, ATERNO S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito,* fasc.4, 2013, 0955B

[417] LUPÁRIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in LUPÁRIA e ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007, 134 ss.; DI PAOLO

delega, da parte del pubblico ministero, ai soggetti incaricati di esperire le indagini informatiche sulla ricostruzione fattuale oggetto del procedimento penale[418].

Inoltre, vi è da considerare che non sempre la prova digitale può assurgere a rango di prova che conferisca certezza assoluta su determinate questioni, come l'effettivo utilizzo da parte di un determinato soggetto di un *computer*[419]. È stato più volte rimarcato in precedenza come le tecniche di localizzazione dell'indirizzo IP esistono, ma non consentono di provare con assoluta certezza che un soggetto si sia effettivamente collegato alla rete (senza considerare i già trattati strumenti di navigazione *internet* anonima). A mero titolo di esempio, anche riuscendo a determinare grazie anche alla collaborazione degli *internet service provider* la linea telefonica utilizzata per la commissione di un illecito, se il *router* è connesso a più *device* o da più persone sarà arduo provare (al di la di ogni ragionevole dubbio) che un determinato soggetto (e non altri che utilizzano quella connessione) abbia posto in essere la condotta incriminata[420]. Pertanto, anche riguardo la prova elettronica sono state mosse critiche analoghe a quelle proposte nei confronti delle prove scientifiche[421], specialmente riferendosi al rischio di una «*sopravvalutazione giudiziale dei dati raccolti*»[422] e di fondare i processi su materiale probatorio facilmente manipolabile ed alterabile.[423]

Data l'intrinseca immaterialità, le prove digitali si prestano a destare problematiche in ordine alla loro reperibilità. Infatti, nella maggior parte dei casi le prove digitali sono disperse in più "luoghi informatici", come ad esempio *server* o *computer* localizzati in

---

G., *op. cit.*, 740 ss.

[418] DI PAOLO G., *op. cit.*, 738 ss..; «*segnatamente, il baricentro di un processo fondato sulla prova scientifica si colloca sempre più nelle indagini preliminari, fase nella quale il dato digitale viene di regola acquisito dalla polizia giudiziaria e successivamente analizzato da tecnici. Risultano quanto mai attuali, quindi, le perplessità di quanti si domandano se nel processo penale odierno l'esperto non stia scalzando poco a poco il giudice, diventando una sorta di "segreto padrone" del processo.*» L. MARAFIOTI, *Digital evidence e processo penale*, in Cassazione. penale, 2011, 4510

[419] Sul punto, «*Non per questo, in caso di prova informatica, è sostenibile il raggiungimento di una perfetta coincidenza tra le risultanze informatiche e la verità fattuale. Anzi, la stessa facilità estrema di modificazione della prova digitale rivela, in realtà, la presenza di un notevole margine di errore.*» L. MARAFIOTI, *Digital evidence e processo penal*e, in *Cass. pen.*, 2011, 4510

[420] L. MARAFIOTI, *op. cit.,* 4510

[421] CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, 3520

[422] LUPÁRIA, *op. ult. cit.*, 134

[423] DI PAOLO G., *op. cit.*, 739

differenti parti di uno Stato o in più Stati.[424] Ovviamente questa caratteristica genera problematiche riguardo la competenza e la giurisdizione dei titolari delle indagini, sia di rango nazionale che internazionale[425].

Sempre dall'immaterialità deriva la «*promiscuità*»[426], ossia la capacità delle prove elettroniche di contenere non soltanto i dati connessi alla commissione dei reati per cui si procede, ma anche potenzialmente un numero illimitato di dati irrilevanti per le indagini che possono anche riguardare aspetti della vita privata di determinati individui[427]. È senza dubbio condivisibile l'opinione di chi considera i computer (ma anche *smartphone, tablet* ecc.) come una «*proiezione tecnologica della persona*»[428], pertanto la relativa analisi permette agli investigatori di entrare in contatto con dati sensibili di un certo rilevo. [429] Paragonata alla capacità lesiva delle intercettazioni, le prove digitali si presentano come notevolmente più lesive del diritto alla riservatezza in quanto contengono non soltanto i dati e informazioni che il soggetto esterna con terzi, ma anche dati personali che l'individuo non ha deciso di condividere con altri, conservandoli nel proprio computer[430].

La ricerca della prova elettronica, quindi, è capace di incidere fortemente sui diritti garantiti dalla Costituzione proprio in virtù del fatto che i dispositivi informatici sono diventati "contenitori" di una mole sterminata e variegata di dati personali; basti pensare alle *e-mail*, *chat*, siti *internet* visitati fino a ricomprendere anche la posizione GPS e gli spostamenti fisici da un luogo ad un altro. È necessario quindi trovare un equilibrio tra la tutela dei diritti e delle libertà fondamentali[431], e le esigenze di tipo

---

[424] DANIELE M., *op. cit.*, 285

[425] CHIAVARIO M., *Le nuove tecnologie e processo penale in giustizia e scienza: saperi diversi a confronto*, Torino, 2006, 78

[426] DANIELE M., *op. cit.*, 287

[427] DANIELE M., *op. cit.*, 288

[428] DI PAOLO G., *op. cit.*, 739

[429] DI PAOLO G., *op. cit.*, 739

[430] RUGGIERI F., *Profili processuali nelle investigazioni informatiche*, in PICOTTI L. (a cura di) *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 158 s.; DANIELE M., *op. cit.*, 288

[431] In particolare, le investigazioni digitali potenzialmente vanno ad incidere sulla libertà di corrispondenza e comunicazione (art. 15 Cost.), come anche il diritto al rispetto della vita privata (e familiare) tutelato dall'art. 8 CEDU e dall'art. 7 della Carta dei diritti fondamentali dell'Unione Europea. Inoltre, è interessato anche il diritto alla protezione dei dati personali (art. 8 della citata Carta dei diritti fondamentali dell'Unione Europea), DI PAOLO G., *op. cit.*, 739

processuale attraverso la costituzione di ottimali garanzie per evitare una lesione profonda del diritto alla riservatezza[432].

Le problematiche non si esauriscono sulle caratteristiche delle prove digitali, ma si estendono anche relativamente alla loro classificazione da parte della dottrina e la relativa riconducibilità alle norme del codice di procedura penale.

Innanzitutto, era dubbia l'appartenenza della prova digitale, in termini di risultato ottenuto dalla prova, alla categoria delle prove rappresentative dirette[433] o delle prove critiche indirette[434]. Come è stato rilevato da più autori[435], esse possono appartenere ad entrambe le categorie, ma se si volesse trovare un unico fattore in comune tra tutte le prove digitali, questo è identificabile nella già citata intrinseca immaterialità[436].

Inoltre, una parte della dottrina si è espressa a favore della tesi che qualifica le prove digitali tra le prove scientifiche[437], in quanto esse comportano l'utilizzo della scienza informatica. A differenza, però, della prova scientifica strettamente intesa (che comporta «*l'utilizzo di determinati strumenti conoscitivi nei momenti di ammissione, assunzione e valutazione della prova*»[438]), la prova digitale necessita di elevate competenze tecniche già nel momento di individuazione e apprensione del dato che costituirà la prova[439].

---

[432] DI PAOLO G., *op. cit.*, 739

[433] «*l'equivalente sensibile sulla cui base occorre rievocare il fatto da provare è costituito da un secondo fatto che rappresenta il primo, consistendo in una narrazione di questo in quanto realmente accaduto.*» MOSCARINI P., *Principi delle prove penali*, 2014, Torino, 8.

[434] Sono prove con cui si rievoca «*l'accadimento, anche nelle sue modalità, attraverso un procedimento logico basato sulle regole dell'esperienza*», MOSCARINI P., *op. cit.*, 9; esempi sono c.d. *file* di *log* che testimoniano l'accesso ad un determinato sito in un determinato momento, PITTIURUTI M., *op. cit.,* 8.; della prova digitale nel procedimento penale e le garanzie dell'indagato, Torino, 2012, 7

[435] FERRUA P., *La prova nel processo penale: profili generali*, in FERRUA P., - MARZADURI E., - SPANGHER G., (a cura di), *La prova penale*, Torino, 2013, 11

[436] PITTIURUTI M., *op. cit.,* 9

[437] «*Un sottotipo* [della prova scientifica] *di recente emersione, a causa dell'alto grado di tecnicismo richiesto per trasformare le informazioni originariamente contenute in macchinari alquanto complessi in dati intellegibili da un giudice*» MARAFIOTI L., *Digital evidence e processo penale*, in *Cass. pen.,* 2011, 4510; le prove digitali appartengono «*alla categoria delle prove tecniche o scientifiche, quali prove derivate dall'impiego di tecnologie informatiche*». NOVARIO F., *Le prove informatiche*, in FERRUA P., - MARZADURI E., - SPANGHER G., (a cura di), *La prova penale*, Torino, 2013, 123; per una definizione di prova scientifica, essa è una prova che, «*partendo da un fatto dimostrato, utilizza una legge scientifica per accertare l'esistenza di un ulteriore fatto da provare*». Così TONINI P., *La prova scientifica: considerazioni introduttive*, in *Dir. pen. proc.*, 2008, Dossier prova scientifica, 8

[438] DOMINIONI O., *La prova penale scientifica*, Milano, 2005, 12

[439] PITTIURUTI M., *op. cit.,* 15

Come già chiarito, è pericoloso equiparare le prove digitali al rango di prova conferente assoluta certezza riguardo al fatto da provare. Seppur sia certo che un determinato sito *internet* è stato visitato da un determinato computer ad un determinata ora, non potrà assurgere a certezza assoluta l'identità della persona che effettivamente ha compiuto tali azioni[440].

Riguardo la riconducibilità alle norme processuali, inizialmente in dottrina si era propensi a sposare la tesi che riteneva le prove digitali alla stregua delle prove atipiche *ex*. art. 189 c.p.p.[441]; questo perché già nella relazione al progetto preliminare del codice di procedura penale si faceva riferimento alla necessità di prevedere le future innovazioni tecnologiche che avrebbero preso piede nell'ambito delle investigazioni. Ma, alla luce delle modifiche che hanno interessato gli istituti dei mezzi di prova e di ricerca della prova ad opera della legge n. 48/2008[442], è possibile far rientrare le prove digitali all'interno dei suddetti istituti, riformulati proprio per ricomprendere questa nuova tipologia di prova[443].

Inoltre, vi è da considerare che molto spesso le prove digitali non sono direttamente inquadrabili tra le prove prive di disciplina (prove atipiche), ma si caratterizzano per essere «*una diversa forma di manifestazione di istituti codicistici già a lungo sperimentati*»[444]. Infatti, è possibile utilizzare nel procedimento tecniche scientifiche peculiari attraverso gli istituti della perizia o della consulenza tecnica.

A riguardo, la giurisprudenza di legittimità[445] si è espressa nel senso che se le leggi scientifiche utilizzate si basino su leggi collaudate di altre scienze universalmente conosciute, non sono riconducibili all'art 189 c.p.p. e quindi non necessitano della

---

[440] BARILI A., *Accertamenti informatici*, in VALLI R., (a cura di), *Le indagini scientifiche nel procedimento penale*, Milano, 2013, 598

[441] GUALTIERI P., *Prova informatica e diritto di difesa*, in *Dir. pen. proc.*, 2008, Dossier prova scientifica, 70. Il testo dell'articolo «*Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.*»

[442] Legge di "*Ratifica ed esecuzione della Convenzione del Consiglio d´Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell´ordinamento interno*"

[443] PITTIURUTI M., *op. cit.,* 19

[444] PITTIURUTI M., *op. cit.,* 19 e MARAFIOTI L., *Digital evidence e processo penale*, in *Cass. pen., 2011*, 4511

[445] Cass., Sez. I, 21 maggio 2008, Franzoni, in Cass. pen., 2009, p. 1840 ss., con nota di CAPRIOLI F.

previa audizione delle parti[446]. Le indagini informatiche, utilizzando leggi matematiche (ed anche appartenenti alla scienza informatica) possono entrare nei procedimenti penali senza particolari difficoltà tramite la perizia e la consulenza tecnica.[447]

Però, l'art. 189 c.p.p. non perde del tutto rilevanza nell'ambito delle prove digitali. La spiccata varietà fenomenologica delle tecniche di indagine e della stessa prova digitale può dar vita a questioni sulla corretta tipizzazione in un determinato schema giuridico, pertanto sarà necessario un approccio caso per caso per determinare se la tecnica investigativa rientrerà tra gli istituti codicistici o meno.

Un aspetto da non tralasciare è la sopracitata capacità lesiva delle tecniche di indagine informatiche dei diritti fondamentali della persona. L'art. 189 c.p.p. richiama proprio la libertà morale della persona, pertanto il giudice dovrà attentamente valutare se ammettere l'esperimento della prova; ma, la giurisprudenza si è mostrata poco incline a tutelare il diritto alla riservatezza degli indagati, prediligendo il principio di non dispersione della prova[448].

3.1.1 (*Segue)* La prova digitale e la prova documentale

È necessario trattare la questione della riconducibilità delle prove digitali nell'ambito operativo delle prove documentali così come disciplinate all'art. 234 c.p.p., che così recita: «1. *È consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo. 2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia.*».

Seppur concepita appositamente per «*strumenti analogici la cui peculiarità è data da grandezze fisiche che assumono valori continui*»[449], vi sono state pronunce giurisprudenziali in favore della tesi che annovera le prove digitali tra le prove

[446] PITTIURUTI M., *op. cit.*, 20

[447] NOVARIO F., *Le prove informatiche*, *cit.*, 122; PITTIURUTI M., *op. cit.*, 20

[448] DOMINIONI O., *Un nuovo idolum theatri: il principio di non dispersione probatoria*, in *Cass. pen.,* 1997, 768.; PITTIURUTI M., *op. cit.*, 22; Cass., Sez. V, 14 ottobre 2009, Virruso, in *C.E.D.* Cass., rv. 246954

[449] ZACCHÉ F., *La prova documentale*, Milano, 2012, 26.; PITTIURUTI M., *op. cit.*, 23

documentali dell'art 234 c.p.p.[450]. Infatti, nella norma si fa espressamente riferimento a rappresentazioni di fatti «*mediante* […] *qualsiasi altro mezzo*» e ciò dovrebbe bastare per poter ricondurre i dati informatici nell'alveo dell'art. 234 c.p.p.[451]

Perplessità sulla tesi di cui sopra si sono avute in riferimento alla necessità del dato informatico dell'intermediazione di un *computer* o di altro dispositivo per poter assolvere la sua funzione rappresentativa, ma la norma è abbastanza chiara sulla questione del mezzo attraverso cui si rappresentano fatti, persone o cose.

In precedenza veniva concettualmente confuso il dato digitale con il supporto informatico attraverso cui esso veniva conservato o rappresentato sotto forma di immagine, filmato o registrazione audio[452]. Quest'errata concezione era anche normata nell'art. 491-*bis* c.p. nella parte in cui specificava cosa si dovesse intendere per "documento informatico"[453], definendo quest'ultimo come «*qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*». È lampante come l'attenzione era erroneamente posta sul supporto informatico in quanto contenente dati digitali e non sui dati digitali stessi. È innegabile che il dato digitale abbia una valenza probatoria a prescindere dal suo supporto[454] e nella maggior parte dei casi vi è una sproporzione tra

---

[450] Cass., Sez. III, 5 luglio 2012, Lafuenti, in *C.E.D.* Cass., rv. 253573

[451] NAPPI A., *La prova documentale e i limiti del contradditorio*, in *CP*, 2002, 1185

[452] DANIELE M., *op. cit.*, 284. Viene puntualizzato da parte della dottrina che le «*necessità di un "traduttore" artificiale è presente anche in altri tipi di documenti che non hanno natura digitale, bensì analogica, e che tradizionalmente sono riconosciuti tali dall'unanime dottrina. Si pensi ai microfilm, alle pellicole cinematografiche, ai nastri magnetici, ai dischi in vinile etc»:* così CARDINO A., - GUIDA R., - RANALDI A., *Processo penale e prove documentali* in *Enciclopedia del diritto*, a cura di CENDON P., Padova, 2004, 24

[453] La suddetta parte è stata abrogata dall'art. 3, comma 1, lett. b), della l. 18 marzo 2008, n. 48; in RAPETTO U., - MANCINI D., *Crimine informatico,* Roma, 2008, 16, viene sottolineato però che rimane valido quanto stabilito dall'art. 621 c.p., ossia che «*agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi*», dimostrando come urgerebbe, quindi, una modifica legislativa anche in relazione al suddetto reato.

[454] CARDINO A., - GUIDA R., - RANALDI A., *Processo penale e prove documentali* in *Enciclopedia del diritto*, a cura di CENDON P., Padova, 2004, 24, secondo cui l'intangibilità dei dati informatici non vale ad escludere la materialità. Inoltre, viene considerato il dato digitale elaborato tramite computer (stampato o visualizzato sul monitor ecc.) come una copia del dato digitale originario. Viene anche esplicitato, contrariamente alla dottrina precedente, che il dato digitale «*non può prescindere in alcun modo dall'esistenza di un supporto materiale sul quale gli elettroni*; «*Anche nel caso del documento informatico, l'intangibilità del contenuto non implica infatti, l'incorporabilità del contenente […] (pertanto) l'elemento della corporalità, anche se non immediatamente evidente, è da considerarsi*

la valenza probatoria del supporto e quella dei dati al suo interno in quanto anche una esigua unità fisica di memorizzazione (hard disk) può contenere innumerevoli dati utili per un processo.[455]

L'art. 1 della Convenzione di Budapest sulla criminalità informatica del 23 novembre 2001[456], del Consiglio d'Europa, fornisce una definizione di documento informatico molto più dettagliata e precisa rispetto alla sopracitata norma del codice penale italiano. Si legge infatti che un documento informatico è «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione».

A livello nazionale, il Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005 n. 82) all'art.1 lett. *p* stabilisce che che un documento informatico è «*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*». Quest'ultima definizione è di più ampio respiro rispetto a quella contenuta nella Convenzione di Budapest, ma si presta ed essere rilevante specificatamente nei processi civili e amministrativi.

In proposito, in dottrina è stato puntualizzato che è necessario discernere quelle che sono le prove "contenute" su di un supporto analogico da quelle che sono invece dati informatici digitali a sé stanti, a prescindere dal supporto informatico[457]. Le prime non sono idonee a rappresentare fatti o persone senza il supporto, i secondi invece si[458].

In virtù di quest'ultima caratteristica, l'attenzione è da porsi sulla effettiva e sicura conservazione dei dati ed anche sulla loro tutela contro manomissioni o distruzioni. Ciò comporta serie problematiche ogniqualvolta venga rappresentato un dato informatico in forma cartacea (come la stampa di una *screenshot* o di una fotografia in

---

presente» FINOCCHIARO G., *La firma digitale*, in *Commentario del codice civile*, a cura di SCIALONA-BRANCA, Roma, 2000, 56.

[455] DANIELE M., *op. cit.*, 285

[456] L'art. 2 della legge 48/2008 di ratifica della convenzione ne dà piena esecuzione. L'art. 1 della convenzione pur se non espressamente richiamato deve ritenersi come operante nel nostro ordinamento.

[457] PITTIRUTI M., *op. cit.*, 24; KALB L., *Il documento nel sistema probatorio*, Torino 2000, 72; TONINI P., *Documento informatico e giusto processo*, *cit.*, 403 ss.

[458] Viene però puntualizzato che «*l'originale del documento informatico è quello formato dal computer che lo ha generato, e non anche il diverso supporto, informatico o meno, usato per la sua riproduzione o per la sua trasmissione all'esterno*» CARDINO A., - GUIDA R., - RANALDI A., *op. cit.*, 25. Mentre nel caso della memorizzazione informatica, ad esempio, di un documento cartaceo, non sarà considerato come un documento informatico in senso stretto, ma «*una semplice memorizzazione in forma digitale del testo di un documento cartaceo tradizionale*» CARDINO A., - GUIDA R., - RANALDI A., *op. cit.*, 26

formato digitale). Infatti, vi è il rischio che cosi facendo si aggirino tutte le accortezze rivolte all'accertamento dell'autenticità e genuinità della prova prodotta in giudizio. Più precisamente, non è problematica in sé e per sé la stampa cartacea del dato informatico ma è opportuno provvedere a raccogliere la prova in modo tale da garantire che quanto trasferito sul supporto cartaceo non sia stato frutto di fraudolente alterazioni.

È necessario quindi dare la possibilità di dimostrare l'attendibilità del dato informatico, e questa occasione può venir meno in caso di modificazione (definitiva, attraverso la sovrascrittura di altri dati) o smarrimento da parte dell'utente, come anche in caso di infruttuoso esperimento di rogatoria internazionale (nel caso in cui i dati siano custoditi in server locati in stati esteri, come avviene nella maggior parte dei casi)[459].

Le soluzioni che vengono prospettate sono due[460]: o viene negato categoricamente l'utilizzo nei processi di prove digitali contenute in supporti informatici, o viene accettato il loro impiego a fini probatori dopo il vaglio di ammissibilità del giudice.

Sarebbe preferibile la seconda, in quanto precludere l'ingresso di dati digitali nel processo significherebbe, al giorno d'oggi, privarsi di un notevole quantitativo di materiale probatorio estremamente rilevante nei *cybercrimes* e non. Ovviamente, il controllo da parte del giudice circa l'attendibilità della prova è fondamentale[461], in quando un superficiale accertamento della genuinità della prova prodotta può comportare l'utilizzo di prove contraffatte o completamente create *ad hoc*[462].

In conclusione, è possibile comunque affermare la riconducibilità delle *digital evidence* nell'ambito della prova documentale; il relativo utilizzo in chiave probatoria richiede tuttavia una adeguata ed attenta verifica da parte del giudice sulla genuinità ed autenticità del dato informatico.

3.2 Le indagini digitali

[459] PITTIRUTI M., *op. cit.*, 26

[460] In particolare da PITTIRUTI M., *op. cit.*, 26 e CUOMO L., - RAZZANTE R., *op. cit.*, 46

[461] DENTI V., *Prova documentale* (*diritto processuale civile*) in *Enciclopedia del diritto* XXXVII, Milano, 1998, 713

[462] PITTIRUTI M., *op. cit.*, 27

Attualmente, in seguito all'incremento degli attacchi informatici perpetrati non solo contro imprese ma anche nei confronti di singoli individui, è necessario senza dubbio sviluppare metodi di indagine specifici per l'accertamento dei reati commessi tramite *pc* e la rete *internet*. Si stimano perdite economiche per circa 400 milioni di dollari, dovute a 700 milioni di violazioni o perdite di dati informatici[463], ma si ritiene che queste cifre siano nettamente maggiori in quanto nella maggior parte dei casi non vengono effettuate le denunce da parte delle vittime dei crimini informatici, sia perché vi è scarsa fiducia nell'utilità della denuncia, sia perché molto spesso la vittima non sa di aver subito un attacco informatico[464].

Focalizzandoci sugli aspetti critici delle indagini digitali, esse si caratterizzano per avere ad oggetto prove «*raccolte in un luogo virtuale*»[465]. La scena del crimine nei *cybercrimes* è nella maggior parte dei casi costituita da sistemi informatici o software, «*tra i polpastrelli dell'autore e la tastiera, tra i suoi occhi e le emissioni elettromagnetiche del* monitor»[466].

Innanzitutto, le procedure volte alla ricerca delle prove digitali avranno come obiettivo quello di acquisire le prove senza alterare o "inquinare" il supporto informatico dove sono memorizzate[467]. Inoltre, è necessario garantire anche la genuinità della prova raccolta e che la copia di essa trasportata eventualmente su un diverso supporto informatico sia perfettamente fedele all'originale.

Quindi, le attività di indagine saranno finalizzare alla preservazione, analisi e documentazione delle attività portate a termine con l'ausilio di un sistema informatico o telematico al fine di ricavare elementi probatori per dimostrare la colpevolezza[468].

È opportuno procedere a qualche distinzione per fare chiarezza sull'oggetto e le tipologie di indagini informatiche. In dottrina si afferma che le indagini informatiche in senso stretto «*insistono su un oggetto, il dato digitale, che interessa agli organi*

---

[463] SIGNORATO S., *op. cit.*; Ead., *European Union Agency For Network and Information Security* (ENISA), *Cyber Insurance: Recent Advances, Good Practices and Challenges*, 7 November 2016

[464] SIGNORATO S., *ult. op. cit.*, 28

[465] CUOMO L., GIORDANO L., *Informatica e processo penale*, in *Processo penale e Giustizia*, 2017, 4

[466] STRANO M., *Nuove tecnologie e nuove forme criminali. Relazione alla Conferenza sul Cybercrime, Palermo*, 3-5 ottobre 2002, reperibile *on-line* al seguente link: *http://www.dvara.net/ HK/Cybercrime-STRANO.pdf*

[467] CUOMO L., – RAZZANTE R., *op. cit.,* 34

[468] CUOMO L., GIORDANO L., *op. cit.*, 4

inquirenti poiché può rappresentare (nel senso di "rendere di nuovo presente") una variegata realtà»[469]. Il suddetto dato digitale, preesiste al processo o sotto forma di dato già memorizzato su di un dispositivo informatico – con la conseguente operatività dei mezzi di ricerca della prova della perquisizione e del sequestro informatici (artt. 247, comma 1-*bis,* e 254 c.p.p. - o sotto forma di dato che viene captato durante la sua trasmissione, mediante intercettazione telematica[470] Fatte queste considerazioni, è possibile distinguere le indagini informatiche in indagini relative alle «*computer-derivated evidence*» e le indagini che hanno ad oggetto le «*electronic evidence a genesi procedimentale*». Nel primo caso, il computer o la rete internet sono l'oggetto dell'attività investigativa, mentre nel secondo caso il computer è il mezzo di conservazione o formazione della prova. Quest'ultima categoria non può però ricondursi alle indagini aventi ad oggetto documenti informatici o tracce digitali in senso stretto, in quanto i relativi dati raccolti non sono stati ricavati da un sistema informatico o telematico o intercettati durante la loro circolazione nella rete.[471]

È possibile distinguere tre tipologie di investigazioni digitali: le investigazioni preventive, preliminari e proattive[472].

Le prime (*pretrial investigations),* sono condotte con la finalità di prevenire la commissione di reati. Si collocano in una finestra temporale antecedente alla ricezione della *notitia criminis*, in quanto vi è ormai la tendenza, specialmente nel diritto penale, a prevedere presidi preventivi. Anzi, proprio per i reati informatici dove la repressione dei reati è compito arduo per gli investigatori e i giudici, gli strumenti di contrasto ideali sono rappresentati proprio da disposizioni preventive, alla stregua di quanto è accaduto per la responsabilità penale degli enti ed il contrasto dei fenomeni corruttivi nella pubblica amministrazione.

Essendo la *cybersecurity* un aspetto ormai fondamentale della sicurezza non solo dei singoli ma anche dello stato, le indagini a scopo preventivo sono effettuate soprattutto dalle diverse *intelligence*, sia nazionali che internazionali. Non sono rari i

---

[469] v. LUPÁRIA, *La ricerca della prova digitale*, cit., 144.; MOLINARI M., *op. cit.,* 699; «*si va da un'immagine, un suono, un testo, al contenuto di una comunicazione riservata o elementi ad essa esterni, alle operazioni eseguite da un sistema informatico durante una sessione (file di log), all'agganciamento del telefono cellulare ad una data cella e così via*», DI PAOLO G., *op. cit.*, 740

[470] DI PAOLO G., *op. cit.*, 740

[471] DI PAOLO G., *op. cit.*, 741

[472] SIGNORATO S., *ult. op. cit.*, 30

casi di utilizzo da parte dei governi di *software* di spionaggio i quali sono mezzi indubbiamente eccessivamente invasivi della *privacy*[473] dei consociati. Infatti, essi possono non solo acquisire i dati memorizzati su di un *device,* ma anche attivare a distanza le *webcam* e i microfoni installati sugli apparecchi informatici[474]. I rischi delle derive autoritarie da parte di alcuni governi totalitari sono lampanti, e possono mettere a serio repentaglio le libertà fondamentali dei cittadini ad essi sottoposti.

Le investigazioni preliminari (*reactive investigations*), invece, sono messe in moto dopo che la *notitia criminis* sia giunta alle autorità competenti. In questo caso le modalità di indagine sono influenzate dai codici di rito dei diversi stati, dove è necessario contemperare gli strumenti investigativi con i principi di adeguatezza e proporzionalità[475].

Nel caso degli stati sottoposti alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), l'art. 8[476] (Diritto al rispetto della vita privata e familiare) della suddetta convenzione stabilisce che è possibile comprimere il diritto sancito nel primo comma solo se vi è un'espressa previsione di legge.

Le investigazioni proattive (*Proactive investigations*) invece sono una sintesi delle prime due categorie, in quanto presentano aspetti di prevenzione e aspetti di repressione[477]. Attualmente sono una tipologia di indagine poco conosciuta e praticata, in quanto viene utilizzata specialmente per la prevenzione e repressione dei reati di terrorismo e di criminalità organizzata. Le investigazioni digitali stanno sempre più assumendo questa tipologia di investigazione, in quanto si assiste ad una fusione tra indagini a fine repressivo/rieducativo e indagini con finalità preventive. Ciò può

---

[473] ANDOLINA E., *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della "privacy" e onde eversive*, in *Archivio penale*, 2015, 3, 916-938

[474] SIGNORATO S., *Types and features of cyber investigations*., *cit*. 194

[475] MOSCARINI P., *op. cit*., 10.; SIGNORATO S., *ult. op. cit*., 195

[476] «*1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può` esservi ingerenza di una autorità` pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società` democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.*»

[477] KOSTORIS E., *Processo penale, delitto politico e "diritto penale del nemico",* in *Rivista di diritto processuale,* 2007, 4; SIGNORATO P., *ult. op. cit*., 195

portare alla creazione di un nuovo sistema penale "intermedio"[478], dove però è possibile dar vita a fenomeni di aggiramento delle tutele giurisdizionali dovute dal fatto che le investigazioni del primo tipo non devono seguire le discipline codicistiche.

Passando all'analisi delle caratteristiche delle investigazioni digitali, la prima che merita di essere presa in considerazione è l'estrema tecnicità. Se condotte da soggetti poco esperti, vi è il rischio (come è stato già diffusamente esplicitato in precedenza) di alterare o inquinare la prova da assumere rendendola addirittura inutilizzabile in quanto definitivamente compromessa la sua capacità probatoria[479].

Un'ulteriore caratteristica è il raggio operativo che spesso non si estende ad un solo Stato ma può arrivare a ricomprendere l'intero globo. Per questo motivo, è utile stabilire norme applicabili in più giurisdizioni possibili (auspicabilmente di portata globale) in modo tale da evitare conflitti di competenza tra autorità inquirenti ma anche conflitti in ordine alla circolazione del materiale probatorio.[480]

Un efficiente sistema di cooperazione internazionale tra Stati nei mezzi di circolazione di prova e di indagine è estremamente necessaria se si vuole contrastare i *cybercrimes* in maniera proficua. In verità, sta acquisendo sempre più importanza la cooperazione tra le autorità inquirenti e i privati, specialmente le imprese più che le singole persone fisiche.

Di fatto, sono le società commerciali a subire la maggior parte degli attacchi[481], in quanto i relativi profitti sono potenzialmente maggiori rispetto ad attacchi contro singoli individui (considerando anche gli ingenti costi che la preparazione di un sofisticato attacco informatico comporta)[482]. Una collaborazione attiva da parte dei

---

[478] SIGNORATO P., *ult. op. cit.*, 195

[479] Sono stati proposti da parte della *International organization for standardization* (ISO), degli standard minimi per la raccolta di prove digitale riguardo la identificazione, conservazione, raccolta analisi ecc. Non sono ovviamente raccomandazioni legalmente vincolanti, ma la loro adozione è utile anche per un efficace circolazione delle prove tra i vari stati. V. SIGNORATO P., *ult. op. cit.*, 195

[480] In molti stati il principio di doppia incriminazione «stabilisce che il fatto deve costituire reato per la legge penale sia dello Stato richiedente, che di quello concedente, indipendentemente dalla diversità dei regimi sanzionatori», Estradizione in Enciclopedia online Treccani *http://www.treccani.it/enciclopedia/estradizione/*

[481] *https://www.ilsole24ore.com/art/tecnologie/2017-09-26/i-cyber-attacchi-costano-aziende-117-milioni-dollari-all-anno-in-media--105136.shtml?uuid=AEaZjqZC*; *http://www.ania.it/export/sites/default/it/pubblicazioni/Dossier-e-position-paper/Il-rischio-cyber-conoscerlo-di-piu-per-proteggersi-meglio-Position-paper.pdf*

[482] BRAGHO' G., *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in *Diritto e informatica* n.3, 2015, 518

privati può coadiuvare gli investigatori sia ad analizzare gli attacchi subiti, sia nella prevenzione di attacchi simili a danno di altre imprese[483].

Inoltre, un'ulteriore modalità di cooperazione riguarda anche il modo in cui vengono progettati i *devices* dal punto di vista *hardware* e *software*. Le imprese operanti in questo settore, ovviamente, nel realizzare i propri prodotti seguono logiche di mercato, ma si potrebbe ipotizzare che nel progettare (specialmente i *software*) si prevedano caratteristiche orientate a rendere non proibitivo l'analisi dei dati memorizzati da parte delle autorità inquirenti[484]. Una soluzione del genere, però, potrebbe presentare profili di criticità riguardo l'invadenza dello stato nella *privacy* degli individui[485] ma anche la sicurezza stessa dei dispostivi informatici[486].

Un caso del genere ha visto coinvolti la nota produttrice di *computer* e *smartphone* Apple, e l'FBI.

In seguito ad un attacco terroristico da parte di due soggetti afflittati all'ISIS[487], l'FBI riuscì ad entrare in possesso dello *smartphone* appartenente ad uno dei terroristi, ma per accedervi ed analizzare i dati in chiave preventiva di ulteriori reati era necessario un codice d'accesso noto solo al proprietario del *device*. In quell'occasione, Apple si rifiutò di fornire all'FBI un *software* capace di accedere ai dati dello *smartphone* aggirando il codice di sblocco, per motivi di *privacy* ma anche di sicurezza dei dispositivi Apple.

---

[483] La cooperazione dei privati è fondamentale anche fondamentale riguardo la conservazione e la fornitura dei dati da parte degli *internet service providers*. Il Codice della privacy all'art. 132 comma 4-ter contempla l'obbligo di conservazione e protezione dei dati del traffico telematico.

[484] In realtà degli accordi di tale tipologia sono stati già messi in pratica. Infatti, sono stati sviluppati dei software (tra i quali vi sono *EnCase Forensics Toolkit (FTK) P2 Commander Autopsy* o *Free Hex Editor Neo*) che con l'obiettivo di far risparmiare risorse e tempo agli investigatori, sono dotati di un c.d. "*push button forensics tool*" che permette di facilitare l'estrazione, conservazione e copia dei dati presenti in un sistema informatico. AL FAHDI M., - CLARKE N., L., - LI F., - FURNELL S., M., *Suspect-oriented intelligent and automated computer forensic analysis*,Vol. 18, Settembre 2016, 65-76; è possibile anche coinvolgere, oltre a *computer* e *smarphone*, anche i *device* appartenenti al c.d. *Internet of things*, ossia i *device* interconnessi tra di loro appartenenti allo stesso individuo. Per un'analisi approfondita, SERVIDA F., E., - CASEY E., *IoT forensic challenges and opportunities for digital traces*, in *digital investigation*, Volume 28, Supplement, aprile 2019, S22-S29

[485] COLE D., FABBRINI F., SCHULHOFER S., *Surveillance, Privacy and Trans-Atlantic Relations* Oxford, 2017, 155

[486] SIGNORATO S., *op. cit.*, 198

[487] Per ulteriori informazioni, *https://en.wikipedia.org/wiki/2015_San_Bernardino_attack; https://www.bbc.com/news/world-us-canada-35004024*

Nel comunicato diffuso dal CEO di Apple[488] viene spiegato che se un *software* con tali caratteristiche finisse nelle mani sbagliate potrebbe comportare una seria minaccia alla sicurezza di tutti i dispositivi Apple in circolazione. In aggiunta, l'FBI aveva anche richiesto che Apple progettasse i futuri *software* prevedendo la possibilità di aggirare il codice di sblocco, proprio per favorire l'attività delle indagini investigative, ricevendo una risposta negativa per gli stessi motivi di cui sopra[489] .

Infine, un accenno è doveroso in tema di indagini digitali "automatizzate": in seguito allo sviluppo della scienza in ambito di intelligenza artificiale e del c.d. *machine learning*[490], sono state sviluppate forme di indagini condotte autonomamente da software informatici.

È possibile distinguere due tipologie di *software* utilizzabili nelle indagini digitali[491]. La prima riguarda *software* capaci di localizzare un determinato dispositivo e di tener traccia degli spostamenti effettuati. La seconda tipologia include *software* capaci di espletare attività simili a quelle umane; tramite questi programmi informatici, infatti, è possibile determinare il grado di aggressività di un individuo nel digitare un messaggio calcolando il tempo trascorso tra una parola digitata ed un'altra. Oppure, è possibile, con l'uso di complessi algoritmi, riconoscere il sesso, religione, età ed abitudini quotidiane di soggetti monitorati, come anche determinare le caratteristiche di un sospettato o suggerire l'identità del probabile soggetto colpevole di un reato.[492]

Ipotizzando l'utilizzo di questi innovativi *software* da parte delle procure, ci si potrebbe imbattere nel rischio di fondare le motivazioni di sentenze di condanna o proscioglimento su prove ottenute senza la supervisione dell'uomo. Secondo Signorato

---

[488] «*The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.*» ed ancora «*While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect*»: così COOK T., *A Message to Our Customers*, 16 febbraio 2016

[489] SIGNORATO S., *op. cit.*, 198

[490] Per approfondimenti, https://it.wikipedia.org/wiki/Apprendimento_automatico; https://www.ilsole24ore.com/art/tecnologie/2019-01-08/machine-learning-deep-learning-e-reti-neurali-ecco-cosa-parliamo--095050.shtml?uuid=AEaToEBH

[491] Bipartizione proposta da SIGNORATO S., *op. cit.*, 199

[492] AL FAHDI M., - CLARKE N., L., - LI F., - FURNELL S., M., *op. cit.*, 65-76; SIGNORATO S., *op. cit.*, 199

A., un risultato del genere sarebbe da vietare, negando espressamente (implementando nuove norme nelle convenzioni internazionali e nelle leggi di diversi stati) la possibilità di fondare le sentenze esclusivamente su materiale probatorio acquisito tramite indagini automatizzate. A motivazione di questa opinione, vi è la considerazione che non è possibile affermare che *software* del genere siano infallibili, garantendo la massima certezza di ciò che viene predetto[493]. Si dovrebbe, pertanto, garantire il diritto alla difesa riguardo la contestazione della attendibilità del software. Però, si potrebbe pensare che le risultanze probatorie dei suddetti software possono essere utilizzate nei processi se e solo se siano confermate ed attentamente valutate da un essere umano.[494]

Concludendo, si è discusso di come le indagini digitali presentino caratteristiche peculiari in virtù della tipologia di prova che mirano recuperare. Inoltre, delicati sono i problemi legati al rispetto della *privacy* e all'adeguata verifica in sede processuale degli elementi di prova acquisiti, anche al fine si evitare l'ingresso in giudizio di elementi di conoscenza non attendibili, e pertanto da sottoporre al vaglio riferibile alla "nuova prova scientifica" ai sensi dell'art. 189 c.p.p.

3.2.1 (*Segue)* Le indagini sulla *blockchain*: cenni di ordine generale alla c.d. "*bitcoin forensics*"

Il diffondersi dell'utilizzo delle criptovalute tra gli utenti sta portando sempre di più all'attenzione delle autorità giudiziarie la necessità di condurre indagini efficienti e che permettano di poter utilizzare nei procedimenti penali prove significative per supportare le tesi proposte dai pubblici ministeri.

Si è già discusso nel corso della trattazione del seguente capitolo e in maniera più analitica nel capitolo precedente come le valute virtuali si prestino perfettamente ad essere utilizzate come "valuta" nella commissione dei *cybercrimes*, ossia come forma

[493] A proposito, ARSHAD H., - GAN A., - ANILA K., - BUTT A., *A multilayered semantic framework for integrated forensic acquisitionon social media* in *Digital investigations*, Volume 29, giugno 2019, 29, 147-158, secondo cui sono state poste molte critiche riguardo la validità e la correttezza delle informazioni pubblicate sui social network. È obbligatorio dunque determinare la correttezza e l'affidabilità di un contenuto pubblicato online prima di utilizzarlo in un processo alla stregua di qualsiasi altra prova»; ARSHAD H., JANTAN, A., OMOLARA, E., *Evidence collection and forensics on socialnetworks: research challenges and directions* in *Digital Investigations,* 2019, 28, 126-138

[494] SIGNORATO S., *op. cit.*, 199

di profitto a cui tendono i *cyber*-criminali. Non solo vengono utilizzate per il riciclaggio di denaro, ma vengono, ad esempio, richieste come "prezzo" da pagare nel caso delle estorsioni *on-line* (*phishing, sextortion*[495]*, ransomware et similia*); le criptovalute sono anche la "moneta" utilizzata nel *dark web* per l'acquisito di beni la cui compravendita è proibito dalla legge.

La loro crescente rilevanza nei *cybercrimes* comporta che anche le tecniche investigative e l'attività degli organi inquirenti siano necessariamente influenzate dalle loro caratteristiche strutturali e di funzionamento[496].

Come è stato più volte ribadito in occasione della trattazione del funzionamento della *blockchain*, il registro delle transazioni è pubblico ed è detenuto da tutti i nodi della rete; ognuno può accedervi, consultare le transazioni iscritte ed estrarne una copia.

Da un lato, questa caratteristica è estremamente utile ai fini investigativi in quanto è possibile analizzare tutti le "movimentazioni" delle valute virtuali a ritroso fino alla prima mai avvenuta. Infatti, come è stato ampiamente esplicato, obiettivo della creazione del *Bitcoin* non era la ottenere una totale anonimità (con la finalità di occultare operazioni poco limpide), ma raggiungere una sicura *privacy* nell'ambito delle proprie movimentazioni di denaro (*privacy* intesa come diritto alla riservatezza con la possibilità, a discrezionalità del soggetto, di rivelare i propri dati), dando vita ad un sistema "pseudo-anonimo". Pertanto, la sostanziale "ubiquità" della *blockchain* è un elemento a favore degli investigatori in quanto non sarà necessario, per poter accedere ai dati dei *server* locati in altre giurisdizioni, ricorrere a complesse operazioni coinvolgendo anche le autorità giudiziarie di altri paesi (che possono anche essere riluttanti a collaborare per scarso interesse o incapaci di collaborare per le insufficienti competenze tecniche)[497].

È da ricordare, però, che alcune criptovalute (*Monero* e *ZChash*) con il dichiarato motivo di rafforzare ancor di più la *privacy* degli utenti (come se non fosse già abbastanza) non prevedono una *blockchain* completamente trasparente, omettendo di

[495]https://www.repubblica.it/tecnologia/sicurezza/2018/03/24/news/estorsioni_a_sfondo_sessuale_dopo_videchat_500_denunce_in_3_anni-192153399/?ref=search

[496] NEILSON D., - HARA S., - MITCHELL I., *Bitcoin Forensics: A Tutorial*, 2016, in JAHANKHANI H., in *Global Security, Safety and Sustainability - The Security Challenges of the Connected World*, in *Communications in Computer and Information Science*, 2017, 630, 1

[497] NEILSON D., - HARA S., - MITCHELL I., *op. cit.*, 2

indicare l'importo della transazione e/o gli indirizzi dei *wallet*. In particolare, *Zchash* permette di scegliere se rivelare per ogni transazione l'importo e gli indirizzi (come avviene con il protocollo *Bitcoin*, *Ethereum* e le restanti criptovalute esistenti), oppure solo l'importo o uno dei due indirizzi; tutto ciò per facilitare gli utenti ad adempiere agli obblighi di *compliance* (in specie, gli obblighi antiriciclaggio) o di *audit*[498].

L'utilizzo di tali criptovalute renderebbe quasi impossibile riuscire ad effettuare qualsiasi operazione di indagine in quanto non si disporrebbe, a fini investigativi, neanche degli estremi degli *address* e dell'importo trasferito.

Il protocollo Bitcoin, invece, permette quantomeno di analizzare lo storico delle transazioni, offrendo agli investigatori elementi da analizzare per ricostruire la provenienza dei *bitcoin* o addirittura a risalire ai titolati degli *address*.

La crittografia, utilizzata nelle *blockchain* per garantirne la sicurezza e la riservatezza, è strumentalizzata dai *cyber-criminali* al fine di impedire le attività delle autorità inquirenti o comunque rallentarne notevolmente le indagini[499].

I sistemi di crittografia avanzati non sono impossibili da decifrare, ma comportano l'impiego di ingenti risorse e di tempo, il che renderebbe poco efficienti le indagini e darebbe occasione ai criminali di far perdere le proprie tracce[500].

È stato quindi sottolineato come una cooperazione dei produttori di beni e servizi[501] nell'ambito informatico o delle telecomunicazioni che utilizzano la crittografia sia estremamente necessario in modo tale che le unità investigative possano condurre le

---

[498] «*Shielded Zcash transactions are completely private. Like Bitcoin, Zcash transaction data is posted to a public blockchain; but unlike Bitcoin, Zcash ensures your personal and transaction data remain completely confidential. Zero-knowledge proofs allow transactions to be verified without revealing the sender, receiver or transaction amount. Selective disclosure features within Zcash allow a user to share some transaction details, for purposes of compliance or audit*», fonte: *https://z.cash*; per ulteriori informazioni, *https://z.cash/technology/*

[499] NAQVI S., *Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals* in *ARES, Proceedings of the 13th International Conference on Availability, Reliability and Securit, Hamburg, Germany* — August 27 - 30, 2018, New York, NY, USA, 2018, 2

[500] NAQVI S., *op. cit.*, 2

[501] V. Il caso di *Blackberry*, che ha contrattato la cessione delle proprie chiave di decrittazione in cambio dell'opportunità di operare nel territorio dei governi dei paesi contraenti, NAQVI S., *op. cit.*, 2; PHILIP J., T., - PARBAT K., *BlackBerry to open code for security check,* https://economictimes.indiatimes.com/tech/hardware/blackberry-to-open-code-for-security-check/articleshow/6249666.cms

dovute indagini essendo in possesso della chiave di decrittazione[502].

Tuttavia, nel caso del protocollo *Bitcoin* e delle altre criptovalute (ad eccezione di *Ripple*, la cui *governance* è centralizzata), non vi è un ente centrale con cui interfacciarsi o con cui confrontarsi nel caso in cui sia necessario condurre un'indagine che comporti la decrittazione di determinate informazioni.

Si potrebbe pensare di instaurare rapporti con i *wallet providers* e gli *exchange* di criptovalute in modo tale da poter chiedere loro di fornire le informazioni (nel caso le abbiano) sui propri clienti. Questa soluzione però è poco plausibile, in quanto i prestatori di servizi in ambito di criptovalute sarebbero riluttanti ad una collaborazione di tal tipo, esponendosi al rischio di perdita di una parte consistente della propria clientela: chi decide di operare con valute virtuali ha particolare apprensione per la propria *privacy* e quindi difficilmente sceglierebbe di affidarsi ad un *wallet provider* che collabori con le forze di *intelligence*. Nondimeno, gli obblighi derivanti dalla V Direttiva antiriciclaggio di fatto impongono ai *wallet provider* di adottare misure di adeguata verifica e di segnalazione di operazioni sospette; pertanto, almeno nell'ambito dell'operatività delle norme dell'Unione europea la suddetta cooperazione tra privati e autorità investigative è stata adeguatamente regolata.

Sebbene la c.d. *bitcoin forensics* sia ancora alle prime armi, notevoli sono i risultati che si sono ottenuti attraverso lo svolgimento di indagini sulla *blockchain*. Essa è definita come «l'impiego di strumenti statistici per aggregare transazioni e identificare utenti»[503].

La letteratura in materia propone diverse metodologie di indagine[504], una delle quali consiste nella "*deanomization*" ("de-anonimizzazione"). Questa tecnica consiste nel associare ad un *address* bitcoin l'identità di un soggetto, un indirizzo *e-mail*, un numero di telefono o qualsiasi altra identità digitale (*username*, *account Google* ecc.).

Possono essere distinte due categorie di metodi di *deanomization,* attivi e passivi. I metodi attivi consistono nell'utilizzo di tecniche di *social engineering*[505] o nodi della

---

[502] V. *supra,* par 3., sulla riluttanza di Apple a fornire un software capace di bypassare il codice di sblocco impostato dall'utente.;

[503] DANIELLI A., - DI MAIO D., - GENDUSA M., - RINALDI G., *op. cit.*, 42

[504] AVDOSHIN S., M., - LAZARENKO A., V., *Bitcoin Users Deanonimization Methods*, in *Trudy*, tom. 30, vol. 1, 2018, 30, 89-102., reperibile all'indirizzo https://bitcoinwhoswho.com/blog/scholarly-works/

[505] «*Nel campo della sicurezza informatica, l'ingegneria sociale (dall'inglese social engineering) è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili.Questa tecnica*

rete *bitcoin* "malevoli". I metodi passivi invece, si limitano ad analizzare le transazioni pubbliche della *blockchain*.

In particolare, i metodi di *social engineering* consistono nel cercare un diretto contatto con il soggetto in modo tale da scoprirne l'indirizzo *bitcoin* ad esso collegato. È attuabile, ad esempio, attraverso l'acquisto di un bene dal soggetto messo in vendita nei *dark markets*; questo è il metodo più efficace perché il venditore non fornirà informazioni false in quanto interessato a ricevere il pagamento. Un altro esempio, più squisitamente tecnico, è costituto dalla creazione di nodi della rete bitcoin con la finalità di intercettare le connessioni in entrata e quindi di rilevare l'indirizzo IP degli utenti che trasmettono le transazioni[506].

I metodi passivi, in particolare, sono costituiti da tecniche di analisi e indagine dello storico delle transazioni della *blockchain* che possono essere piuttosto sofisticate.

Una delle tecniche consiste nell'accorpare (il c.d. "*clustering*"[507]) più indirizzi bitcoin appartenenti allo stesso soggetto analizzando l'*input* e l'*output* della transazione, notando che il primo comprende più *address*, ed il secondo è costituito da un solo indirizzo[508]. Le tecniche più complesse invece studiano le movimentazioni dei *bitcoin* cercando di individuare e di accorpare gli indirizzi che ricevono più "moneta" senza spenderla; in tal modo, si cerca di individuare gli *address* dei *dark markets* di siti di scommesse illegali[509].

Oltre queste tecniche complesse, si è già discussa l'opportunità di ricorrere al c.d.

è anche un metodo (improprio) di crittanalisi quando è usata su una persona che conosce la chiave crittografica di un sistema e viene usata anche dalla polizia. Similmente al cosiddetto metodo del tubo di gomma (il quale è però una forma di tortura) può essere, secondo gli esperti, un modo sorprendentemente efficiente per ottenere la chiave, soprattutto se comparato ai metodi crittanalitici», *https://it.wikipedia.org/wiki/Ingegneria_sociale*

[506] Esistono, infatti, due tipologie di nodi nella infrastruttura della rete *peer to peer* del *bitcoin*: i *client* e i *server*. I *client* non accettano connessioni in entrata, mentre i *server* si. I nodi "malevoli", quindi, si andrebbero a configurare come nodi *server*, che quindi ricevono le connessioni in entrata costituite dalle transazioni: v. AVDOSHIN S. M., LAZARENKO A., *op. cit.*, 97

[507] *Online* è disponibile un sito web che permette di ricercare i *wallet* accorpati appartenenti allo stesso soggetto: v. *https://www.walletexplorer.com*

[508] I portafogli bitcoin non cumulano su un unico conto la totalità dei bitcoin. Se si è in possesso di un portafoglio contenente 5 *bitcoin*, e si ricevono 4 *bitcoin*, si avrà un *wallet* costituito da due "sotto portafogli" rispettivamente di 5 e 4 *bitcoin*; non quindi un unico portafoglio contenente 9 *bitcoin*. La criptovaluta *Ethereum*, invece, accorpa tutti gli *ether* posseduti in un unico conto. Cfr. ANTONOPOULOS M. A., *op. cit.*, 9

[509] AVDOSHIN S. M., LAZARENKO A., *op, cit.*, 97

blacklisting[510], ossia alla "marchiatura" dei *bitcoin* provenienti da soggetti noti per le loro attività illecite come ad esempio, tentativi di *phishing*, estorsioni *online* ecc.

Addirittura, esistono piattaforme online (il più noto è "*bitcoinwhoswho*"[511]) finalizzati a raccogliere le segnalazioni di indirizzi *bitcoin* fraudolenti; cosi facendo, gli utenti possono verificare se un determinato indirizzo bitcoin è stato segnalato per aver commesso tentativi di frodi o *phishing*, contribuendo alla sicurezza della rete *bitcoin*. È possibile anche di propria iniziativa fornire i propri dati alla suddetta piattaforma in modo tale da poter garantire agli altri utenti di non essere implicati in operazioni illecite, e ciò può essere utile nel caso di venditori che accettino e utilizzino i *bitcoin* come corrispettivo.

Un'ultima considerazione merita la circostanza che l'utilizzo dei già trattati servizi di *mixing* rende estremamente più complesso, ma non impossibile, l'analisi delle transazioni della *blockchain*. Inoltre, utilizzo del *browser* TOR e dei VPN può rendere vane le ricerche finalizzate all'individuazione dell'indirizzo IP che con i suddetti accorgimenti viene mascherato o sotto posto a stratificazione crittografica.

Quindi, le indagini informatiche in generale presentano peculiarità di non poco conto in ordine all'oggetto delle indagini, ma, le investigazioni relative alla criptovalute pongono nuove ardue sfide agli inquirenti. L'utilizzo della crittografia, dei servizi di *mixing* e di *tumbling* rendono più complicato l'esperimento di indagini proficue, ma comunque sono in via di sviluppo tecniche di analisi che possano aggirare questi ostacoli.

3.3 Le indagini informatiche e mezzi di ricerca della prova "tradizionali": la perquisizione, l'ispezione e il sequestro di dati digitali

Dopo le considerazioni trattate nei paragrafi precedenti, è necessario porre l'attenzione su quelli che sono gli istituti disciplinati al titolo III del libro III del codice di procedura penale, ossia i mezzi di ricerca della prova; in particolare, la perquisizione (artt. 247 – 251 c.p.p.), le ispezioni (artt. 244 – 246 c.p.p.) e i sequestri a scopo probatorio (artt. 253 – 263 c.p.p.).

---

[510] DANIELLI A., - DI MAIO D., - GENDUSA M., - RINALDI G., *op. cit.,* 42

[511] *https://bitcoinwhoswho.com*

Le perquisizioni e ispezioni, in quanto «tipici atti "a sorpresa"»[512], sono attribuite alla potestà dell'"autorità giudiziaria", rendendo esplicito come esse possono essere disposte non solo dal giudice, ma anche (e soprattutto, data la loro forte rilevanza nelle indagini preliminari) dal Pubblico Ministero[513].

Le prime, consistono nell'attività del «*perquirere*», finalizzata alla ricerca del corpo del reato o cose pertinenti a quest'ultimo[514], le seconde nell'attività dell'«*inspicere*», allo scopo di accertare sulle persone, nei luoghi o nelle cose le tracce e gli altri effetti materiali del reato[515], e sono entrambe attività che indiscutibilmente incidono sui diritti tutelati agli artt. 13 e 14 della Carta fondamentale. Per quest'ultimo motivo è prescritta la necessità di un decreto motivato ed è anche prevista la riserva di legge per quanto riguarda i casi in cui è possibile disporle e le relative modalità.

In riferimento alle prove digitali e al sempre più crescente fenomeno dei *cybercrimes*, parte della dottrina statunitense aveva già espresso le proprie preoccupazioni in ordine alla sfida lanciate al diritto processuale penale[516]. Venivano, in particolare, espresse perplessità sulla sufficienza di uno sforzo ermeneutico tale da ricomprendere le prove digitali e le tecniche di indagini informatiche nelle norme attualmente in vigore e per questo motivo è stato proposto di introdurre delle norme *ad hoc* in modo tale da evitare tentativi interpretativi estremi.

Queste problematiche, a dire il vero, riguardano in particolar modo le indagini informatiche, proprio perché (anche nel caso del nostro codice di procedura penale) le norme attualmente in vigore sono state concepite per dettare metodi di indagine che avessero luogo esclusivamente nel mondo materiale e "tangibile". Le particolarità delle indagini ed anche della prova a cui tendono impongono un ripensamento delle norme attualmente in vigore. Inoltre, vi è da considerare che cosi come le norme dei mezzi di ricerca della prova sono formulate con l'intento di rispettare i diritti costituzionalmente garantiti, le eventuali nuove norme devono tener presente l'idoneità delle prove

[512] CONSO G., - GREVI V., - BARGIS M., *Compendio di proceduta penale*, VIII, Milano, 2016, 334
[513] CONSO G., - GREVI V., - BARGIS M., *op. cit.*, 335
[514] CONSO G., - GREVI V., - BARGIS M., *op. cit.*, 335
[515] CONSO G., - GREVI V., - BARGIS M., *op. cit.*, 335
[516] KERR O., *Digital Evidence and the New Criminal Procedure*, in *105 Colum. Law Review*, 2005, 290.

elettroniche a ledere in misura molto maggiore la *privacy*[517].

In questo senso, l'adozione della Convenzione di Budapest del 2001 ha interessato in particolare le norme processuali con la finalità di contrastare i *cybercrimes*. Nel preambolo, secondo cui «*convinti della necessità di perseguire, come questione prioritaria, una politica comune in campo penale finalizzata alla protezione della società contro la criminalità informatica, adottando una legislazione appropriata e sviluppando la cooperazione internazionale*», si evince infatti che obiettivo ed oggetto della Convenzione è quello di introdurre modifiche normative o nuove leggi insieme ad una efficiente cooperazione internazionale, estremamente necessaria in quanto il cyberspazio non conosce confini, e nella maggior parte delle ipotesi le unità di *intelligence* dei vari Stati saranno costrette necessariamente a collaborare.

Inoltre, sempre nel preambolo, le affermazioni secondo cui *«[…] le reti informatiche e le informazioni in formato elettronico possano anche essere utilizzate per commettere reati che le prove connesse a tali reati possano essere conservate e trasferite tramite queste reti*», esplicitano l'intenzione del Consiglio d'Europa di focalizzarsi sulle prove digitali e la relativa analisi ai fini di repressione e contrasto dei crimini informatici.

L'Italia ha provveduto a dare esecuzione alla Convenzione nel 2008 (dopo sette anni la sua firma) con la legge n.48/2008[518], non con una sbrigativa ripetizione delle relative disposizioni, ma apportando numerose modifiche di ricamo delle norme del codice di rito[519].

In particolare, sono state diverse le modifiche che hanno interessato il contenuto lessicale delle norme in tema di mezzi di ricerca della prova, in modo tale da ricomprendervi anche le indagini e le prove digitali. Nonostante prima dell'introduzione della legge di recepimento della Convenzione di Budapest si fosse già provveduto ad estensioni analogiche e a nuove interpretazioni, una modifica legislativa era necessaria anche per conferire chiarezza sulle possibilità di utilizzo di particolari tecniche investigative nel pieno rispetto dei diritti costituzionalmente

---

[517] MOLINARI M., F., *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, fac. 2, 2012, 696B

[518] CAJANI F., *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono …*, in *Cib. dir.*, 2010, 186

[519] PITTIRUTI M., *op. cit.*, 33

granititi (la *privacy in primis*)[520].

Tuttavia, non sono state apportate modifiche che descrivessero in maniera dettagliata le modalità operative, ma è stato più volte introdotto (in diversi articoli, in particolare artt. artt. 244, comma 2, 247, comma 1-bis, nonché artt. 352, comma 1-bis, 354, comma 2, c.p.p.), l'indicazione di provvedere ad adottare «*misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*»[521]. In più, le prove digitali cosi raccolte devono essere "maneggiate" in modo tale da garantire «*la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*» (artt.254-bis e, ancora, 354, comma 2, c.p.p.; e similarmente art. 260, comma 2, c.p.p.).

Sono state quindi cristallizzate nelle norme attualmente in vigore i principi della tutela della genuinità ed integrità che devono ispirare gli investigatori[522] nel procedere alle indagini. Viene quindi data libertà d'azione riguardo gli strumenti, le tecniche e le concrete modalità di indagine, anche in virtù della continua evoluzione tecnologica che renderebbe sempre obsolete le disposizioni[523].

In dottrina diverse sono state le critiche[524] rivolte al legislatore italiano in virtù della mancata introduzione di una nuova disciplina organica delle indagini informatiche, che sarebbe stata da preferire alla scelta di modificare le diverse norme attualmente in vigore[525].

Riguardo le ispezioni, vi sono diversi elementi critici da tener in considerazione. Il suddetto mezzo di ricerca della prova, si caratterizza per limitarsi ad una verifica e la

---

[520] PITTIRUTI M., *op. cit.*, 34

[521] PITTIRUTI M., *op. cit.*, 35, secondo cui ciò costituisce il *letimotiv* della nuova disciplina cosi delineata dal legislatore italiano in seguito all'adozione della Convenzione di Budapest del 2001

[522] RICCI A., E., *Digital evidence, sapere tecnico-scientifico e verità giudiziale*, in CONTI C., (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Milano, 2011, 348

[523] PITTIRUTI M., *op. cit.*, 37.

[524] LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, in *Diritto Penale e Processo,* 6, 2008, 718; LUPARIA L., *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul Cybercrime*, in LORUSSO S., (a cura di), *Le nuove norme sulla sicurezza pubblica*, Padova, 2008, 64-65

[525] «*non mancano profili critici in merito a questa impostazione sistematica. Sotto un primo angolo di visuale, appare indubbio come nel caso di specie [ispezioni e perquisizioni], non si possa parlare di rilievi in senso tradizionale […], giacché si è in presenza di azioni ad alto contenuto tecnologico che già implicano scelte metodologiche e delicate valutazioni su base scientifica*» LUPARIA L., *Computer crimes e procedimento penale*, in GARUTI G. (a cura di), *Modelli differenziati di accertamento*, t. I, Torino, 2011., 384

rilevazione dello stato fattuale di una cosa (o persona)[526], senza effettivamente provvedere ad una analisi di ciò che è contenuto su di un supporto informatico[527]. A differenza della perquisizione, quindi, vi è l'assenza di una attività di ricerca, limitandosi gli inquirenti ad una osservazione del "reale"[528], scevra da ogni elemento valutativo[529]. Sembra difficile, secondo parte della dottrina, configurare una ipotesi di ispezione di dati informatici che non ricada nella disciplina delle perquisizioni o del sequestro probatorio. Infatti, l'adozione di «*misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione*» non può che comportare una analisi in concreto dei dati memorizzati su di un dispositivo, quindi accedendo ad esso[530].

La dottrina che abbraccia una diversa opinione[531] ricostruisce la fenomenologia dell'ispezione spiegando che si può effettuare una copia del dato informatico ritenuto rilevante tramite la tecnica del *bit stream image*[532], e soltanto dopo procedere alla analisi e verifica della "copia" del dato.

Secondo la prima opinione[533], è da accogliere con favore la pratica di operare su una copia del dato rilevante per non rischiare alterazioni o compromissioni del dato originale, ma è errato considerare tale attività come una semplice ispezione basandosi sull'assunto che il dato informatico "originale" non venga acquisito. Infatti, l'attività

---

[526] MOSCARINI P., *Ispezione (diritto processuale penale)*, in *Enc. dir., Agg.*, vol. II, Milano, 1998, 464

[527] V. BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici* in LUPARIA L., (a cura di) *Sistema penale e criminalità informatica*, Milano, 2009, 196: «L'ispezione informatica può risultare molto utile quando per la complessità del sistema informatico o l'interazione fra i vari sistemi da acquisire rende pressoché impossibile o assai sconsigliabile procedere alla perquisizione e al sequestro dell'intero network. »

[528] CUOMO L., - GIORDANO L., *op. cit.*, 2

[529] PITTIRUTI M., *op. cit.*, 37; «*L'ispezione si caratterizza per la sua limitazione all'esame obiettivo ed al rilevamento di una situazione di fatto attuale, nel modo in cui essa cade sotto la percezione sensiorilae dell'organo procedente*», CUOMO L., - RAZZANTE R., *op. cit.*, 63

[530] Invero, l'ispezione è tradizionalmente ricostruita quale analisi esterna, PITTIRUTI M., *op. cit.*, 47

[531] LUPARIA L., (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali*, BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* Milano, 2009, 196

[532] «*La bitstream image (clonazione) costituisce una "copia immagine" del supporto originale, ossia una replica esatta e identica, bit per bit, che riproduce anche le informazioni precedentemente cancellate e non soprascritte contenute all'interno dello spazio non allocato di un file system (dati che non verrebbero copiati tali quali nel corso di un semplice processo di copiatura dei files). La copia bitstream è unanimemente ritenuta uno strumento fondamentale e imprescindibile per le procedure di acquisizione e analisi di dati informatici*» MOLINARI F., M., *op. cit.*, 23

[533] PITTIRUTI M., *op. cit.*, 119

di duplicazione rientrerebbe, in realtà, nell'ambito del sequestro. Ciò è supportato da evidenze normative, ossia dal contenuto degli artt. 254-bis e 260, comma 2, c.p.p., che prescrivono la possibilità che l'autorità giudiziaria (quindi anche il pubblico ministero) disponga l'acquisizione del dato informatico tramite la sua duplicazione (con procedure che assicurino la integrità dello stesso).

Pertanto, nell'ambito delle indagini informatiche, una ispezione si dovrebbe considerare solo l'attività di osservazione "esterna" di un sistema informatico, con particolare attenzione alla connessione a periferiche (collegate e scollegate), ai *software* installati o al tipo di connessione a *Internet* utilizzata, ecc.[534] Andando oltre i limiti predetti, si rientrerebbe nell'ambito della perquisizione[535].

Le perquisizioni sono dirette all'individuazione e alla acquisizione del corpo del reato o altre cose pertinenti[536]. È disposta con decreto motivato, poiché essendo mezzo della ricerca della prova lesivo della libertà personale e del domicilio è necessario un controllo sulla legittimità del provvedimento.

Una delle differenze della formulazione della disciplina riguarda l'oggetto dell'attività che nel mezzo di ricerca della prova appena trattato consistono nei «*sistemi informatici o telematici*», mentre nel caso delle perquisizioni vi è un espresso riferimento ai «*dati, informazioni, programmi informatici*». Gli investigatori possono andare oltre la semplice osservazione esterna effettuando operazioni direttamente sui dati (ad esempio, aprire cartelle, *file*, eseguire programmi ecc.), sempre attuando misure idonee a non modificare o compromettere i dati[537](come l'utilizzo di *software* "*write-blocker*"[538]).

---

[534] CUOMO L., - GIORDANO L., *op. cit.*; ATERNO S., *Art. 8. Modifiche al titolo III del libro terzo del codice di procedura penale*, in CORASANITI G., - CORRIAS LUCENTE (a cura di), *Cybercrime, responsabilità degli enti e prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Padova, 2009, 206

[535] BELLORA C., *Ispezione giudiziale*, in *Dig. disc. pen.*, IV ed., VII, Torino, 1993, 275

[536] CUOMO L., - GIORDANO L., *op. cit.*, 2

[537] PITTIRUTI M., *op. cit.*, 39

[538] «*Un write blocker è un dispositivo usato dagli investigatori nel campo dell'informatica forense per prevenire eventuali scritture su hard disk o più genericamente dispositivi di memorie di massa (chiavi USB, schede di memoria, un tempo i floppy disk, etc...) oggetto di investigazioni. Generalmente il write blocker è posto tra il dispositivo esaminato e il computer utilizzato per esaminarlo. Ci sono due tipi di write blocker, native e tailgate: un write blocker native è usato per collegare il disco attraverso la sua interfaccia nativa (es.: disco IDE su interfaccia IDE o disco SCSI su interfaccia SCSI); un write blocker tailgate è usato invece per collegare il disco attraverso una interfaccia diversa (es.: disco IDE tramite USB o disco SATA tramite FireWire).*» v. definizione in *https://it.wikipedia.org/wiki/Write_blocker*.

In dottrina è stato evidenziato come, nella prassi, la perquisizione abbia mutato la sua funzione di atto prodromico al sequestro, essendo essa messa in atto solo a seguito dell'esperimento di questo secondo di ricerca della prova[539]; ma in realtà, la legge di recepimento della Convenzione di Budapest prescrive che la perquisizione *ex*. 247 comma 1-*bis* va effettuata prima di provvedere al sequestro unicamente del file rilevante ai fini investigativi[540].

Inoltre, è stata segnalata una ingiustificata asimmetria tra le discipline degli strumenti probatori appena trattati, in quanto nel caso delle perquisizioni si autorizzano esplicitamente le autorità investigative a procedere anche forzando le misure di sicurezza a tutela del sistema informatico o dei dati da perquisire[541]. Infatti, anche nelle attività ispettive è necessario in alcuni casi forzare le misure di protezione poste a tutela del dispositivo informatico.

Per concludere, le attività di ispezione e perquisizione nell'ambito delle indagini digitali sono caratterizzate da una sottile linea di demarcazione suscettibile di essere facilmente elusa, proprio in virtù della particolarità dell'oggetto materiale delle indagini, la prova elettronica[542].

3.3.1 (*Segue*) Il sequestro della prova digitale

Il sequestro per finalità probatorie, disciplinato negli artt. 253 e ss. del codice di rito, si differenzia dalle altre tipologie di sequestro in virtù del suo particolare oggetto, il «*corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti*»[543]; è previsto anche in questo caso con decreto motivato emesso dall'autorità

---

[539] MOLINARI F. M., *Questioni in tema di perquisizione e sequestro di materiale informatico,* in *Cass. pen.,* 2012, 12, «*Invero, rispetto alle attività di ricerca della prova tradizionali, la perquisizione di un computer è attività che per sua peculiare natura si presta a essere eseguita non prima ma dopo il sequestro dello stesso. La differenza non è di poco conto, in quanto il sequestro dell'elaboratore finalizzato alla sua perquisizione è attività che va a incidere non solo sul diritto al possesso della res (computer) ma altre*sì *sul diritto alla riservatezza nonché sulla privacy dei dati personali archiviati nella memoria elettronica*», Cfr. anche BONETTI M., *Riservatezza e processo penale*, Milano, 2003, 58; PITTIRUTI M., *op. cit.*, 41

[540] MOLINARI F., M., *op. cit.*, 708

[541] MONTI A., *La nuova disciplina del sequestro informatico* in LUPARIA L., *Sistema penale e criminalità informatica, cit.*, 195

[542] PITTIRUTI M., *op. cit.*, 42

[543] CONSO G., - GREVI V., - BARGIS M., *op. cit.*, 339

giudiziaria.

È nel secondo comma che viene poi specificato cosa si intende per corpo del reato: «*le cose sulle quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto, o il prezzo*.».

Il sequestro di materiale informatico è disciplinato nell'articolo 254-*bis* c.p.p., introdotto dalla più volte richiamata L. 48/2008, che viene configurato come un sequestro presso i fornitori di servizi informatici, telematici e di telecomunicazioni.

Le problematiche relative alla suddetta tipologia di sequestro riguardano sia l'oggetto sia «*l'estensione del vincolo reale*»[544]. Ed è già nella Convenzione di Budapest che si evince la difficoltà di determinare quali siano le *res* oggetto di sequestro; l'art 19 prescrive la possibilità per le autorità inquirenti di sequestrare «*un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici*», non circoscrivendo con precisione l'oggetto del sequestro. È necessario determinare se ogni volta che si procede ad un sequestro di dati informatici si necessario procedere all'apprensione del solo *hard disk* (che contiene i dati memorizzati e i programmi software installati) oppure l'intero apparato del computer (*monitor*, *mouse*, stampanti ecc.). In più, si potrebbe pensare di estendere il sequestro solo ed esclusivamente al dato rilevante per le indagini, e non all'interno dell'*hard disk*, che può contenere una mole ingente di dati non necessari e di contenuto "sensibile"[545], violando il principio di proporzionalità[546].

---

[544] MONTI A., *La nuova disciplina del sequestro informatico*, in LUPARIA L., (a cura di) *Sistema penale e criminalità informatica,* Milano, 2009, 198

[545] V. MONTI A., in LUPARIA L., *op. cit.,* 198, secondo il quale «la dottrina e la giurisprudenza più tecnologicamente avvertite avevano da subito evidenziato l'importanza di limitare l'estensione del sequestro ai soli dati digitali» MONTI A., in LUPARIA L., *op. cit.,* 198; BUONOMO G., *Profili penali dell'informatica*, Milano, 1994, 166; «*un sequestro indiscriminato di tutta la postazione di lavoro, in carenza di presupposti, potrebbe rivelarsi eccessivamente invasivo ed eccedente rispetto allo scopo di tutela della genuinità della prova, ledendo i diritti fondamentali della persona protetti a livello costituzionale dalle disposizioni relative alla riservatezza, alla segretezza, al diritto di proprietà e al diritto di difesa*», CUOMO L., - RAZZANTE R., *op. cit.*, 55

[546] MONTI A., in LUPARIA L., *op. cit.,* 198.; «*Il sequestro indiscriminato dell'intero sistema informatico, in carenza di presupposti, in taluni casi può rivelarsi eccessivamente invasivo ed eccedente rispetto allo scopo di tutela della genuinità della prova, ledendo in tal modo i diritti fondamentali della persona protetti a livello costituzionale dalle disposizioni relative alla riservatezza, alla segretezza, al diritto di proprietà e al diritto di difesa*», CUOMO L., - GIORDANO L., *op. cit.*, 3

Nonostante le chiare sollecitazioni della dottrina[547], sono state poche le pronunce giurisprudenziali che hanno ritenuto di circoscrivere l'oggetto del sequestro quanto meno al solo *hard disk*[548]. Numerose, invece, le pronunce in favore dell'apprensione della totalità degli apparecchi utilizzati per il funzionamento del *computer*, estendendo oltre il necessario l'ambito oggettivo del sequestro[549], il tutto giustificato dal "rapporto di pertinenzialità" che lega tali dispositivi al corpo del reato[550].

Un'ulteriore problematica è costituita dall'applicazione simultanea dell'art. 253 e dell'art. 254-*bis* c.p.p. Il primo, considera oggetto del sequestro le "cose", intese in senso materiale; siccome i dati digitali "cose" non sono (anche essendo beni immateriali comunque non è possibili accomunarli alle "cose"), si potrebbe giungere alla conclusione di escludere che la suddetta norma possa trovare applicazione nel caso di dati digitali[551]. Quindi, il sequestro informatico avrebbe una applicazione parallela e non gerarchicamente subordinata a quella dell'art 253, sancendo cosi la non sequestrabilità delle componenti *hardware* del *computer*[552].

Questa ricostruzione è criticata da altra parte della dottrina che sottolinea come l'art. 260 c.p.p. ricomprende tra i beni oggetto di sequestro anche i dati, informazioni e programmi informatici[553]. Per questo motivo, nell'ambito delle indagini sui *cybercrimes* i supporti informatici adibiti alla memorizzazione dei dati potranno essere oggetto di sequestro in quanto contengano i dati o i *software* utilizzati per compiere l'attività criminosa[554] (in virtù della loro pertinenza al reato piuttosto che dalla loro qualificazione come corpo del reato[555]).

---

[547] V. PITTIRUTI M., *op. cit.*, 44: «*Può, innanzitutto, escludersi che l'intero computer, comprensivo di tutta l'attrezzatura ad esso collegata (monitor, mouse, stampante, videocamera, microfono ecc.) costituisca corpo del reato o cosa pertinente al reato*».

[548] Trib.Torino in funzione di giudice del riesame, 7 febbraio 2000; Trib. Venezia in funzione di giudice del riesame, 6 ottobre 2000.

[549] Trib. Potenza, in funzione di giudice del riesame, 2 maggio 2002,; Trib. Salerno in funzione di giudice del riesame, 5 ottobre 2002.; Cfr. MONTI A., in LUPARIA L., *op. cit.,* 199; MONTI A., *No ai sequestri indiscrimanti di computer*, nota a trib. Brecia sez II, 9 ottobre 2006 in *dir. Internet*, 2007, 269

[550] Cass., Sez. III, 6 novembre 2002, Maggiore, in Guida dir., n. 3, 2003, 79

[551] MONTI A., in LUPARIA L., *op. cit.,* 201-202.

[552] MONTI A., in LUPARIA L., *op. cit.,* 201-202; PITTIRUTI M., *op. cit.*, 45

[553] PITTIRUTI M., *op. cit.* 45

[554] PITTIRUTI M., *op. cit.* 45

[555] «*per "cosa pertinente al reato" debbano intendersi, in senso lato, «le cose che servono, anche indirettamente, ad accertare la consumazione dell'illecito, il suo autore e le circostanze del reato, con riferimento a ogni possibile legame, individuabile caso per caso, tra le cose stesse e l'accertamento*

Inoltre, quando a norma del 260, comma 2, c.p.p., viene effettuata una copia dei dati digitali rilevanti, andrà considerata come oggetto del sequestro solo e soltanto la "copia forense", nella cui estrazione si concretizzerà l'esecuzione del sequestro stesso[556]. Non è pertanto sempre e in ogni caso necessaria un'attività costituita da due fasi, la prima diretta al sequestro "materiale" dell'*hardware*, la seconda finalizzata all'analisi dei dati in esso memorizzati.[557]

Passando oltre, non è da sottovalutare il fatto che il legislatore non ha predisposto un sequestro di dati informatici presso "chiunque", ma solo ed esclusivamente nei confronti di "fornitori di servizi informatici, telematici e di telecomunicazioni". Questi, possono essere: il locatore di spazio fisico in cui il soggetto indagato ha riposto il proprio *server*; il possessore dei dispositivi su cui l'indagato ha memorizzato dati, informazioni e programmi; il detentore dei dati rilevanti per l'indagine.[558]

Nel primo caso, si tratta di un soggetto che non viene interessato dal provvedimento di sequestro, ed avrà semplicemente un mero dovere di collaborazione con l'autorità giudiziaria. Nel secondo caso, invece, i soggetti considerati saranno destinatari diretti del provvedimento ablativo. Discorso analogo, infine, per i soggetti detentori dei dati rilevanti ai fini investigativi[559].

Infine, un'ulteriore problematica interpretativa scaturita dal "nuovo" art. 254-*bis* è dovuta al rischio di sovrapposizione della disciplina codicistica con quella, in materia di *data retention,* regolata dall'art. 132 d.lgs. n.196/2003 (Codice della *privacy*). Infatti, l'articolo del codice di rito in questione si riferisce anche ai «*dati di traffico o di ubicazione*», regolati anch'essi dal decreto legislativo appena citato, e determinare quale delle due discipline si applichi al caso concreto è fondamentale, in quanto sono ravvisabili differenze riguardo ai termini e ai controlli[560].

---

dell'illecito», Cass., Sez. VI, 7 aprile 1997, IANNINI, in *C.E.D. Cass., rv*. 207591.; PITTIRUTI M., *op. cit.,* 45

[556] PITTIRUTI M., *op. cit.* 47; «*inoltre in dottrina è stato sottolineato come la clonazione delle tracce informatiche non sia soltanto una semplice conservazione di dati digitali, quanto piuttosto un sequestro di informazioni, che deve essere soggetto alle norme sul sequestro e sul riesame*», ZAMPERINI V., *Impugnabilità del sequestro probatorio di dati informatici*, in *Dir. pen. proc*., 2016, 508; CUOMO L., - GIORDANO L., *op. cit*., 4

[557] PITTIRUTI M., *op. cit.,* 47

[558] MONTI A., in LUPARIA L., *op. cit.,* 211 ss.

[559] MONTI A., in LUPARIA L., *op. cit.,* 213 ss.

[560] PITTIRUTI M., *op. cit.,* 53

In dottrina, si è proposta la soluzione di considerare applicabile l'art. 254-*bis* c.p.p. solo con riferimento alle modalità operative con cui condurre il sequestro informatico. Per l'acquisizione dei dati di traffico, invece, è applicabile esclusivamente il Codice della *privacy*, in particolare l'art 132, che pone in capo ai prestatori di servizi di comunicazione elettronica obblighi di conservazione dei dati relativi al traffico telefonico e telematico per periodi di tempo determinati, consentendone quindi l'acquisizione con decreto del pubblico ministero[561].

Infine, resta da considerare la particolare ipotesi contemplata al comma 3 dell'art. 262 c.p.p., ossia la possibilità di convertire il sequestro probatorio in sequestro preventivo (artt. 321 e ss. c.p.p., collocato tra le misure cautelari reali) in riferimento ai casi di siti *web* il cui contenuto sia illecito (ad esempio, materiale pedopornografico ecc.)[562].

L'utilizzo dello strumento del sequestro preventivo, in tali ipotesi, presenta problematiche dello stesso ordine rispetto a quelle che sorgono nell'ambito dell'utilizzo dei mezzi di ricerca della prova, ossia l'immaterialità dei dati informatici.

Infatti, nel caso in questione il vincolo posto dalla misura cautelare non consiste nello spossessamento di una *res*, ma nell'imposizione al soggetto destinatario del provvedimento di una prestazione di *facere*[563]. Questo obbligo consiste nel porre in essere tutte le attività necessarie ad "oscurare" il sito *web*. Nello specifico, tale obbligo si andrà a configurare in capo ai c.d. "*access provider*"[564], che dovranno impedire la navigazione del sito *web* illecito da parte degli utenti della rete[565].

Inizialmente, la giurisprudenza[566] era tendenzialmente favorevole a ritenere

---

[561] PITTIRUTI M., *op. cit.*, 54

[562] Cfr. CUOMO L., RAZZANTE R., *op. cit.*, 58, secondo cui «*in realtà, viene specificato come non sia estremamente necessario provvedere al sequestro di un sito web su cui sia collegata una pagina web illecita in quanto sarebbe sufficiente la pubblicazione di un messaggio contenente gli estremi del provvedimento ablativo. Sarebbe necessario invece il sequestro della totalità del sito sostituendolo con gli estremi del provvedimento di sequestro se esso sia totalmente finalizzato a diffondere informazioni illecite o a divulgare ideologie ritenute* contra legem»

[563] CUOMO L., - GIORDANO L., *op. cit.*, 3

[564] Definito quale «*soggetto che consente all'utente l'allacciamento alla rete telematica*» da Trib. Bologna n. 3331 del 14 giugno 2004, in https://www.altalex.com/documents/dizionario-giuridico/2009/01/20/provider.

[565] Con un sistema di "filtraggio dei codici", DNS o IP: v. CUOMO L., - GIORDANO L., *op. cit.*, 3

[566] Cass., sez. I, 4 giugno 2014, n. 32846, in *CED Cass.*, n. 261195; Cass., sez. V, 5 novembre 2013, n. 10594, in *CED Cass.*, n. 259887; Cass., sez. V, 30 ottobre 2013, n. 11895, in *CED Cass.*, n. 258333; Cass., sez. V, 19 settembre 2011, n. 46504, in *www.dirittoegiustizia.it*; Cass., sez. V, 18 gennaio 2011,

l'oscuramento di pagine *web* o interi siti attraverso lo strumento del sequestro preventivo, ma diversi sono le criticità di un simile orientamento. L'imposizione di un "fare" è incompatibile con la suddetta misura cautelare proprio perché "reale". Essa consiste nell'apprensione fisica di una "cosa". Inoltre, bisogna considerare che l'art. 254-*bis* regola il sequestro (probatorio) presso i fornitori di servizi informatici, telematici e di telecomunicazioni, ma non vi è una simile disciplina nel capo relativo al sequestro preventivo[567].

La giurisprudenza successiva[568], invece, ha ritenuto che essendo la *ratio* dell'istituto in questione l'impedimento alla prosecuzione dell'attività illecita, nonché l'utilizzo della cosa per la commissione di ulteriori reati, è lecito imporre un'obbligazione inibitoria di "fare".

Particolare è anche la qualificazione del dato informatico come "cosa", in quanto il contenuto di ogni pagina *web* è dotato di una propria "fisicità" poiché memorizzato e conservato in un *computer*. Più nello specifico, ciò che è trasmesso tramite la rete internet sui siti web è memorizzato nei *server* degli *internet service providers* utilizzando «*un sia pure infinitesimale spazio fisico*»[569]. Pertanto, il sequestro preventivo avente ad oggetto l'obbligo di oscurare un sito *web* o una singola pagina *web* è perfettamente legittimo e secondo l'orientamento della Suprema Corte rispetta principi di legalità e proporzionalità[570].

Concludendo, la Convenzione di Budapest ha portato diverse modificazioni normative dettando le modalità e le finalità dei sequestri come anche degli altri mezzi di ricerca della prova trattati in precedenza. Parte della dottrina ha espresso opinioni negative in quanto una materia dominata da un così alto tasso tecnico meritava una dettagliata disciplina *ad hoc*. Probabilmente un intervento di questo tipo avrebbe impegnato il legislatore in un'opera che potenzialmente poteva restringere

---

n. 47081, in *CED Cass*., n. 251208; Cass., sez. V, 10 gennaio 2011, n. 7155, in *CED Cass*., n. 249510; Cass., sez. VI, 28 giugno 2007, n. 30968, in *CED Cass*., n. 237485; Cass., sez. III, 27 settembre 2007, n. 39354, in *CED Cass*., n. 237819; CUOMO L., - GIORDANO L., *op. cit*., 9

[567] CUOMO L., - GIORDANO L., *op. cit*., 3

[568] Cass., sez. un., 29 gennaio 2015, n. 31022, in *Foro it*., 2016, 1, 2, 52, CUOMO L., - GIORDANO L., *op. cit*., 9; PIATTOLI B., *Il sequestro preventivo di una pagina web: il funzionalismo della rete e le sue intersezioni nelle dinamiche processuali*, in *Dir. pen. proc*., 2016, 201

[569] Cass., sez. un., 29 gennaio 2015, n. 31022, in *Foro it*., 2016, 1, 2, 52; v. al riguardo CUOMO L., - GIORDANO L., *op. cit*., 4

[570] CUOMO L., - GIORDANO L., *op. cit*., 4

notevolmente l'iniziativa e la libertà d'azione degli organi inquirenti, anche considerando il continuo progresso tecnologico e l'evolversi delle tecniche di *digital forensics*.

3.3.2 (*Segue*) Una panoramica delle questioni sul sequestro di *bitcoin*.

Dopo aver trattato il sequestro preventivo e probatorio delle prove digitali in generale, è opportuno passare all'analisi delle problematiche che si possono presentare nel caso in cui le autorità inquirenti procedano al sequestro o alla confisca di criptovalute.

Le criptovalute sono, come le prove digitali, anch'esse caratterizzate dall'immaterialità e dall'essere essenzialmente dati informatici, ma la loro apprensione "fisica" è fortemente problematica in virtù della crittografia utilizzata per garantirne la sicurezza. Solo con la chiave privata è possibile "spendere" i *bitcoin*, ma il suo ritrovamento da parte delle forze dell'ordine non è sufficiente a imporre sul *bitcoin wallet* un vincolo di indisponibilità. In realtà dovrebbero essere proprio le chiavi private ad essere oggetto di sequestro (o confisca), in quanto i *bitcoin* sono solo, sintetizzando all'estremo, delle trascrizioni sulla *blockchain*.

Una delle questioni che si pongono in riferimento alle chiavi private riguarda la disponibilità del *wallet*. Se esso è di disponibilità non solo di un singolo soggetto ma anche degli *exchange* o dei *wallet providers,* probabilmente sorgeranno problematiche simili a quelle del sequestro presso terzi[571].

Inoltre, un'altra questione riguarda l'effettiva titolarità di un *wallet* in assenza di una previa procedura di adeguata verifica effettuata da un *exchange* (e con la V Direttiva anche da parte dei *wallet providers*). Infatti, nessuno può dire con certezza che un determinato soggetto è "titolare" di un *address bitcoin* alla stregua di un conto corrente bancario; se più soggetti conoscono la chiave privata possono "spendere" i *bitcoin* in esso contenuti.

---

[571] CAPACCIOLI S., *Il contesto dei cryptoassets e del cash out alla luce della nuova Direttiva Europea 2018/843 V Direttiva AML*, reperibile al seguente link: http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/antifrode_mezzi_pagamento/antifrode_mezzi_pagamento/GIPAF_Capaccioli.pdf

Procedendo per gradi, il sequestro probatorio è quello che probabilmente comporta meno problemi in riferimento ai *bitcoin*. Come sappiamo, la *blockchain* delle criptovalute (ad eccezione di *Monero* e *ZCash*) è pubblica e trasparente, rendendo superfluo procedere all'"apprensione" dello storico delle transazioni per poterlo utilizzare in un procedimento. Basterebbe semplicemente consultare la *blockchain*[572] e riprodurne il contenuto (ad esempio con una c.d. "*screen shot*" delle sole transazioni rilevanti e non dell'intera *blockchain*) acquisendo come prova documentale le transazioni in essa iscritta.

Riguardo il sequestro preventivo, Le uniche questioni sorgerebbero nel caso di sequestro delle chiavi private per poter assumere il controllo del *wallet*, effettuato presso i fornitori di servizi relativi alle criptovalute o sequestrando il computer di un soggetto privato. In tal modo, si mira a poter congelare i *bitcoin* per evitare che il "possessore" (*recitus*, l'individuo che ne conosce la chiave privata) possa servirsi di strumenti di *mixing* che possano far perdere le tracce sulla *blockchain* dei *bitcoin* posseduti.

Per un'analisi più completa, bisognerebbe distinguere la tipologia di *wallet* da sequestrare, sempre se l'oggetto del sequestro viene considerata la chiave privata e non i dati informatici iscritti nella *blockchain*. Pur non potendo normalmente la chiave di accesso essere considerata equivalente al bene che si intende sequestrare – si pensi all'ipotesi di un immobile - nel caso del sequestro di criptovalute (specialmente preventivo, a fini cautelari) la conoscenza della chiave privata è l'essenza del *wallet* stesso, sin quanto senza di essa i *bitcoin* rimarrebbero delle tracce sulla *blockchain* fini a sé stesse.

Nel caso dei *wallet* "*online*", l'oggetto del sequestro dovrebbero essere i dati informatici salvati presso i *server* del *wallet provider* (o dell'*exchange*).

Nel caso di portafogli "*desktop*", si potrebbe considerare oggetto del sequestro l'*hard disk* del *computer* dove è installato il *software* di gestione delle chiavi private.

I c.d. "*paper wallet*", sono portafogli dove la chiave pubblica e privata sono stampati su un foglio, pertanto in quel caso potrebbe bastare il sequestro del documento.

Gli "*hardware-wallet*" sono invece dei dispositivi, in molti casi simili alle *pen-drive*

---

[572] Ad esempio, sul sito *internet https://www.blockchain.com/it/explorer* è possibile consultare ogni blocco aggiunto ed i precedenti, insieme alle transazioni in esso iscritte

USB[573] che memorizzano e generano le chiavi private *offline*; in quest'ultima ipotesi dovrebbe eseguirsi il sequestro della *res* contenente le chiavi di decrittazione.

Infine, con il termine "*brain-wallet*", si suole far riferimento al fatto che venga memorizzata da parte di un individuo la chiave privata del proprio *wallet bitcoin*[574]. In questo caso non ci sarebbe nulla da sequestrare, pertanto questa forse sarebbe la situazione più complicata per riuscire a congelare dei *bitcoin* o altre criptovalute.

Proseguendo, diverse sono le accortezze da adottare da parte degli investigatori nel procedere al sequestro di *bitcoin*. Innanzitutto, nel caso di *wallet software* o *online*, il sequestro dell'*hard disk* o il modificare la *password* del *wallet* non è una misura sufficiente, in quanto l'utente può aver effettuato un *backup* dei dati o aver comunque la disponibilità della chiave privata.

Bisognerebbe, pertanto, creare un nuovo indirizzo *bitcoin*, possibilmente utilizzando i c.d. "*cold-wallet*", ossia i generatori di chiavi private *offline*, decisamente migliori dal punto di vista della sicurezza[575]. Successivamente, trasferire i *bitcoin* sequestrati presso il nuovo indirizzo. Di ciò è necessario redigerne verbale, anche se la *blockchain* già di per sé testimonia i trasferimenti di criptovaluta in maniera affidabile e definitiva.

In verità, sarebbe anche opportuno proteggere i *bitcoin* sequestrati da tentativi di sottrazione, ad esempio cifrando la chiave privata o adottando sistemi di *multisignature*[576]. Oppure, si potrebbe, per semplificare le operazioni, convertire i *bitcoin* in valuta avente corso legale, ma ciò può essere un'attività delicata in virtù delle forti oscillazioni dei prezzi delle criptovalute[577]. Tuttavia, l'attività di conversione di criptovaluta potrebbe essere considerata come un eccesso arbitrario di poteri da parte

---

[573] *https://en.wikipedia.org/wiki/USB_flash_drive*

[574] in realtà, più che memorizzare la chiave privata vengono memorizzate una serie di parole. Queste parole non vengono scelte a discrezionalità dell'utente, ma vengono individuate dopo aver trasformato la chiave privata in codice binario (applicando ad essa la funzione crittografica di *hash* SHA256), e associando ad ogni segmento di risultato ottenuto di codice una parola dal dizionario inglese in base alla sua posizione in ordine crescente. Per maggiori approfondimenti, https://medium.com/@barno/seed-phrase-mnemonic-phrase-come-ottenerlo-e-come-ripristinarlo-b8f157331111

[575] CAPACCIOLI S., *op. cit.*

[576] CAPACCIOLI S., *op. cit.*; *https://en.bitcoin.it/wiki/Multisignature*

[577] Problematiche del genere non si presenterebbero in caso in cui i *bitcoin* fossero oggetto di confisca, in quanto vengono appresi in via definitiva dallo stato che per una meno onerosa e più sicura gestione degli stessi può preferire la loro conversione in valuta fiat.

dell'autorità giudiziaria andando oltre la semplice apprensione del bene[578].

Concludendo, il tema del sequestro di *bitcoin* o di altre criptovalute può assumere aspetti polivalenti in base al caso concreto e alla tipologia di *wallet* utilizzato. In più, il relativo peculiare funzionamento richiede che gli investigatori adottino particolari misure

3.3.3 (*Segue*) Il caso *Silk Road* e *Bitgrail*

Uno dei casi più celebri e che più ha attirato l'attenzione dei media è senza dubbio il caso che ha visto coinvolti il sito presente sul *darkweb* "*The Silk Road*"[579] e l'ente investigativo di polizia federale degli Stati Uniti d'America, l'FBI.

Creato nel 2011, il sito *web* in questione era configurato come un portale di *e-commerce*, ma i beni offerti erano stupefacenti, carte e documenti falsi e ogni genere di merce illegale e la "valuta" utilizzata era esclusivamente il *bitcoin*. L'aspetto innovativo che ha decretato il successo del sito *web* è stato istituire un sistema si recensioni e di risoluzioni delle dispute, ponendo rimedio a quella che era una delle problematiche più critiche dell'acquisto *online* di merci illegali.[580] Il sito era noto all'FBI, ma era estremamente arduo capire chi fosse il gestore e proprietario del sito *web*. Sono state tentate tecniche di *social engineering*, attraverso la creazione di account falsi, attraverso i quali si riusciva ad entrare in confidenza con il gestore del sito, ma senza riuscire davvero a localizzare e identificare il soggetto responsabile dello stesso. La sua individuazione (nella persona di Ross Ulbricht) è stata possibile grazie ad alcuni errori di configurazione del *browser* d'accesso di Ulbricht e ad accessi effettuati al sito senza l'uso di TOR.

Come spesso accade, i *cyber*-criminali riescono ad essere individuati grazie ad alcune "tracce" sul *web* indicizzato che permettono dopo complesse analisi di forum, indirizzi *e-mail* ecc. di ricondurre un *nickname* ad un determinato soggetto.

Al termine del processo, sono stati definitivamente confiscati circa 144 *bitcoin*, i

---

[578] COSTABILE G., *Come funzionano le investigazioni e i sequestri su bitcoin,* reperibile al seguente link: https://www.agendadigitale.eu/sicurezza/come-funzionano-le-investigazioni-e-i-sequestri-su-bitcoin/

[579] silkroad6ownowfk.onion, indirizzo raggiungibile solo tramite il *browser* TOR.

[580] DORDAL P. L., *The dark web*, in *Cyber criminology*, *Advanced sciences and technologies for security applications*, a cura di JAHANKHANI H., Berlino, 2018, 110

quali sono ora in possesso dell'FBI[581].

Anche in Italia si è proceduto al sequestro – seppure nell'ambito di una procedura civilistica - di una ingente quantità di *bitcoin* nei confronti dell'*exchange* di criptovalute denominato "*BitGrail*"; società italiana fondata nel 2017, essa fu coinvolta nella fraudolenta sottrazione di una criptovaluta scambiata sulla piattaforma chiamata "Nano"[582]. Contrariamente a quanto affermato da *Bitgrail*, era stato un errore di programmazione del *software* dal cambiavalute virtuale italiano a permettere il furto della moneta virtuale. Nonostante l'offerta ai clienti da parte di *Bitgrail* di un piano di risanamento delle perdite, è stato chiesto il fallimento della società fiorentina, infine dichiarato dal Tribunale di Firenze con riguardo sia alla società, sia alla ditta individuale che aveva gestito per un certo periodo la medesima piattaforma [583]. In seguito alla sentenza di fallimento il Tribunale – che ha ritenuto configurabile una responsabilità civilistica della società da deposito irregolare - ha disposto il sequestro di circa 2.345 *bitcoin* e 4 milioni di Nano, e, nei confronti dell'amministratore Francesco Firano, di circa 170 *bitcoin* e oltre 500.000 euro.[584]

I *bitcoin* sequestrati sono stati trasferiti su un indirizzo *bitcoin* creato appositamente per il curatore della procedura fallimentare. Le chiavi private del suddetto *wallet* sono state poi depositate in un luogo terzo e sicuro, di cui il curatore e il coadiutore o chiunque abbia preso parte al sequestro non è in possesso di copie, restando inoltre ignoto il luogo di relativa custodia[585]. Ciò poiché era accaduto, durante la fase d'indagine del sito *web Silk Road*, che i due agenti dell'FBI che lavoravano al caso si fossero impossessati dei *bitcoin* sequestrati, essendo a conoscenza delle chiavi private dell'indirizzo su cui erano stati traferiti.

I due casi appena trattati sono solo quelli più celebri dell'esperienza statunitense e italiana, ma non si esclude che in futuro le procure e i tribunali dovranno sempre più interfacciarsi con indagini aventi ad oggetto le transazioni di criptovaluta e disporre sequestri o confische di *bitcoin*. Come si è appena discusso, le modalità per procedere

---

[581] Fonte: *http://fortune.com/2017/10/02/bitcoin-sale-silk-road*

[582] *https://coinmarketcap.com/it/currencies/nano/*

[583] Trib. Firenze, sez. fallimentare, sentenza 21/01/2019 n° 18.

[584]*https://www.ilsole24ore.com/art/finanza-e-mercati/2019-01-25/fallisce-bitgrail-piattaforma-italiana-le-criptovalute-190438.shtml?uuid=AE9Dg8LH*

[585] *https://www.agi.it/economia/furto_bitcoin_bitgrail-4010463/news/2018-06-09/v*

ai sequestri sono assai peculiari e delicate, pertanto si auspica che i soggetti coinvolti in tali operazioni siano mettano in pratica operazioni adeguate al fine di condurre provvedimenti cautelari efficaci.

3.4 I soggetti processuali nelle indagini informatiche

Dopo aver analizzato le peculiarità delle indagini informatiche e delle prove digitali, è necessario passare alla trattazione dei soggetti coinvolti nella fase investigativa.

Si è evidenziato come siano necessarie competenze tecniche in ambito informatico (e non solo) di un certo rilevo per poter condurre indagini efficaci ma anche per poter maneggiare le prove digitali in maniera corretto[586].

Proprio per raggiungere tale obiettivo, è stato introdotto introdotto dall'art. 11 della legge n.48/2008 il comma 3-*quinquies* all'art. 52 del codice di rito che estende la competenza del pubblico ministero distrettuale nelle indagini preliminari e nei procedimenti di primo grado[587] (art. 51, comma 1, lett. *a*, c.p.p.)[588]: «*Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414-bis, 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 609-undecies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente*».

Una simile asimmetria tra le norme di competenza territoriale del giudice e criteri di attribuzione delle funzioni del pubblico ministero[589] era già prevista agli artt. 51 comma 3-*bis* e 3- *quater* c.p.p. per i reati di criminalità organizzata (anche mafiosa), e

---

[586] PITTIRUTI M., *op. cit.*, 117

[587] CASSIBBA F., *L'ampliamento delle attribuzioni del pubblico ministero distrettuale*, in LUPARIA (a cura di), *Sistema penale e criminalità informatica*, 113

[588] L'articolo in questione partecipa agli elementi di atipicità dei procedimenti riguardanti i reati informatici, LUPARIA L., *Computer crimes e procedimento penale* in *Trattato di procedura penale*, diretto da SPANGHER G., *Modelli differenziati di accertamento*, a cura di GARUTI G., 376

[589] DI BITONTO M., L., *L'accentramento investigativo delle indagini sui reati informatici,* in *La ratifica della Convenzione del consiglio d'Europa sul* cybercrime*: profili processuali*, in *dir. Internet*, 2008, 503 e ss.; LUPARIA L., *ult. op. cit.*, 377

di terrorismo (sia interno che internazionale) per motivi che ubbidiscono alla *ratio* della unitarietà dei reati associativi e della loro stretta correlazione con il territorio; nel caso in questione, invece, la motivazione di una tal scelta legislativa è mossa dalla necessità di istituire organi di indagini specializzati[590], oltre che di favorire il coordinamento investigativo, sebbene quest'ultima finalità sia rimasta in buona parte disattesa.

Le previsioni in materia di "competenza" del p.m. introdotte ad opera della legge di attuazione della Convenzione di Budapest hanno come ambito operativo i reati tassativamente indicati[591], ossia i reati relativi allo sfruttamento sessuale dei minori[592] e i reati informatici[593] (in senso stretto)[594].

Diverse sono le critiche mosse nei confronti nella novella legislativa del 2008. Innanzitutto, è stato obiettato come sarebbe stato più opportuno estendere la competenza del pubblico ministero distrettuale non esclusivamente ai reati indicati ma anche alle attività investigative relative ad altre tipologie di illeciti[595].

Inoltre, viene fatto notare che anche l'ufficio del pubblico ministero distrettuale dovrà necessariamente acquisire conoscenze sulle nuove tecniche di indagine, con il

---

[590] LUPARIA L., *ult. op. cit.*, 377

[591] Senza possibilità di estensioni analogiche, in quanto le norme che regolano la competenza sono poste a tutela del principio del giudice naturale precostituito dalla legge (art. 25 Cost). CASIBBA F., *op. cit.*, 116

[592] Per completezza espositiva, i reati in questione sono: prostituzione minorile, art. 600-bis, c.p.; pornografia minorile, art. 600-ter, c.p.; detenzione di materiale pornografico, art. 600-quater, c.p.; iniziative turistiche volte allo sfruttamento della prostituzione minorile, art. 600-quinquies, c.p.: v. CASIBBA F., *op. cit.*, 114

[593] Sono I delitti di accesso abusivo ad un sistema informatico o telematico (615-ter c.p.); detenzione È diffusione abusiva I codici di accesso ai sistemi informatici o telematici (615-quater); diffusione apparecchiature, dispositivi ho programmi diretti a danneggiare o interromper un sistema informatico (art. 615-quinquies); installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche (617-bis c.p.); falsificazione, alternazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche (617-ter c.p.); di intercettazione, impedimento, o interruzione illecita di comunicazioni informatiche o telematiche (617-quater c.p.); installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche, di falsificazione alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (617-quinquies c.p.); danneggiamento di informazioni, dati e programmi informatici (617-sexies); danneggiamento di informazioni, dati, e programmi utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità (635-bis c.p.); danneggiamento di sistemi informatici o telematici (635-ter c.p.); frode informatica (art. 640 c.p.), CASIBBA F., *op. cit.*, 114

[594] Ossia aventi come oggetto materiale della condotta illecita un sistema informatico o telematico

[595] PITTIRUTI M., *op. cit.*, 118; LUPARIA L., *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul Cybercrime*, in LORUSSO S., (a cura di), *Le nuove norme sulla sicurezza pubblica*, Padova, 2008, 66

conseguente rischio di un sovraccarico di lavoro delle procure.[596]

Infine, si era criticata la lampante «*illogicità del sistema*»[597], determinata in quanto dalla mancata previsione da parte della legge n.48/2008 di un simmetrica "accentramento" della competenza sui reati informatici in capo ai giudici delle indagini preliminari e dell'udienza preliminare distrettuali, al pari della disciplina dedicata ai reati associativi[598]. Con il D.lg. 23 maggio 2008, n. 92 e la legge di conversione del 24 luglio 2008, n. 125 si è opportunatamente provveduto ad estendere anche ai reati ricompresi nell'art. 51 comma 3-*quinquies* la competenza del G.I.P e del G.U.P distrettuale, attraverso la modifica all'art 328, comma 1-quater. Inoltre, è stato stabilito che le funzioni del pubblico ministero vengano svolte da un sostituto, designato dal Procuratore della Repubblica, competente[599]nelle medesime materie appena citate.

In dottrina le critiche ad una simile scelta da parte del legislatore si incentrano anche sulle problematiche che scaturiscono dall'art. 25 Cost., e in particolare dal principio del giudice naturale precostituito per legge[600], in quanto il giudice competente non sarà quello prossimo al *locus commissi delicti*. Tale critica può essere smorzata dalle argomentazioni già proposte nel capitolo precedente riguardo la difficile individuazione del *tempus* e *locus commissi delicti,* con riguardo alle fattispecie di cui si tratta; pertanto, attribuire al P.M. distrettuale lo svolgimento delle indagini può semplificare l'individuazione del giudice competente quantomeno all'interno del distretto. Però viene sottolineato in dottrina come il chiaro obiettivo di dar vita ad indagini più efficienti non sia stato pienamente raggiunto in quanto non vi sono attualmente organismi di coordinamento di procure.

In realtà, è stato evidenziato da altra parte della dottrina che la previsione della "competenza" del pubblico ministero distrettuale era «*prevedibile*»[601], in quanto già precedentemente alla legge di attuazione della Convenzione di Budapest vi era la tendenza ad una simile estensione per contrastare più efficacemente i reati di

---

[596] Secondo LUPARIA L., in *Computer crimes e procedimento penale* «*è notoria l'enorme quantità di di notizie di reato che giungono alle procure in materia di frodi informatiche, detenzione di materiale pedopornografico e diffusione di virus*» 377

[597] PITTIRUTI M., *op. cit.*, 119

[598] LUPARIA L., *ult. op. cit.*, 379

[599] PITTIRUTI M., *op. cit.*, 119; LUPARIA L., *ult. op. cit.*, 378

[600] PITTIRUTI M., *op. cit.*, 120

[601] CASSIBBA F., in LUPARIA L., *op. cit.*, 122

criminalità organizzata e associativi. Ciò, in quanto, così facendo, si dava una più sicura attuazione all'art. 112 Cost., riducendo la possibilità di dispersione di elementi probatori e di informazioni rilevanti tra i diversi uffici delle procure[602].

Concludendo, la Convenzione di Budapest ha portato gli Stati firmatari ad adottare previsioni che avessero come finalità quella di migliorare e rendere più efficaci le indagini nell'ambito dei *computer crimes,* come anche di disciplinare i principi di esecuzione delle indagini, basati sulla integrità e tutela delle prove raccolte. Il legislatore italiano ha provveduto a modificare le norme sulla "competenza" dell'organo dell'accusa seguendo una "prassi" legislativa già utilizzata per la commissione di reati particolarmente gravi, dimostrando la volontà di centralizzare lo svolgimento delle indagini, così da sviluppare anche nuove competenze tecniche, al prezzo di un carico di lavoro maggiore per le procure distrettuali.

3.5 Conclusioni

Nella trattazione del capitolo è stata delineata una panoramica delle problematiche squisitamente processuali legate alle prove elettroniche, alle investigazioni e all'inquadramento delle criptovalute negli istituti del codice di procedura penale.

Sono state discusse le particolarità della prova digitale in quanto *res* intangibile e connotata dall'immaterialità. Si è altresì fatto cenno alle singolari questioni dibattute in dottrina riguardo la riconducibilità della prova elettronica nell'alveo operativo della prova documentale, anche in seguito alle modifiche apportate dalla Convenzione di Budapest e la relativa legge di attuazione (L. n. 48/2008)

Data la natura immateriale dei dati informatici, si è ritenuto opportuno analizzare le questioni attinenti all'adeguamento alle caratteristiche di questi ultimi dei mezzi di ricerca della prova tradizionali (ispezioni, perquisizioni e sequestro probatorio), nonché della misura cautelare del sequestro preventivo. È stato evidenziato come molto spesso, nello svolgimento delle investigazioni, le ispezioni tendano a sconfinare nell'alveo delle perquisizioni, poiché non ci si limita ad una osservazione esterna, ma nella maggior parte dei casi si entra in contatto col dato informatico rilevante per le

[602] CASSIBBA F., in LUPARIA L., *op. cit.*, 122

indagini.

Anche le investigazioni in ambito informatico hanno caratteristiche peculiari proprio in virtù dell'oggetto delle indagini e del "luogo" di commissione del reato, ossia non nella realtà fenomenica materiale ma nel mondo "virtuale". Diverse sono le accortezze da utilizzare nel momento dell'"apprensione" del dato informatico e della sua corretta conservazione. Infatti, le prove elettroniche sono decisamente più "fragili" rispetto ad una comune *res* materiale, in quanto anche una semplice disattenzione può compromettere l'integrità e la genuinità del dato informatico vanificando la sua valenza probatoria in giudizio.

La natura singolare dei *bitcoin*, poi, comporta che le indagini, ma soprattutto i sequestri, vengano eseguiti con modalità del tutto eccezionali. Considerato come oggetto del sequestro le chiavi private delle transazioni, dalla loro diversa configurazione dipenderà la concreta applicazione degli istituiti giuridici presenti nel codice di rito. Inoltre, è stata fornita una panoramica delle tecniche di indagine riconducibili alla c.d. *bitcoin forensics*, la scienza che si occupa di analizzare le transazioni sulla *blockchain* per poter riuscire a ricollegare determinate transazioni a dei soggetti, o perlomeno a localizzarli tramite l'indirizzo IP.

Sono stati quindi illustrati celebri casi giurisprudenziali statunitensi e italiani in tema di indagini aventi ad oggetto specificatamente i *bitcoin* (caso *Silk Road*), nonché di sequestro di criptovalute (caso *Bitgrail*). Il primo è stato quello che senza dubbio ha fatto più scalpore per la portata che il sito web illegale aveva raggiunto col passare degli anni. Il secondo, invece, è degno di nota poiché è stato il primo caso che ha visto le autorità giudiziarie italiane interfacciarsi con il sequestro di valute virtuali.

Infine, si è trattata la questione della competenza dei soggetti titolari delle indagini, in particolare dell'accentramento delle funzioni inquirenti nelle procure distrettuali ad opera della legge di attuazione della Convenzione di Budapest, con le conseguenze che ne derivano.

CONCLUSIONI

Le criptovalute e la *blockchain* hanno costituito una importante innovazione tecnologica, capace di rivoluzionare diversi aspetti della vita degli individui. È stato evidenziato come la tecnologia alla base del funzionamento ha applicazioni pratiche che spaziano dalla creazione degli *smart contracts* al miglioramento dei servizi gestiti dalla Pubblica Amministrazione.

A livello legislativo, non vi è ancora un'uniformità di vedute riguardo l'inquadramento giuridico della *blockchain* e la relativa disciplina applicabile, ma in alcuni ordinamenti vi sono stati dei tentativi di regolazione. In particolare, nell'ordinamento italiano è stata emanata una prima definizione di *blockchain* e *smart contracts*, ma è stata colta l'occasione in questo elaborato per sottolinearne le imprecisioni e contraddizioni che potrebbero comportare notevoli difficoltà applicative. È stata prestata attenzione anche al fenomeno delle ICO, e delle relative questioni di inquadramento e opportunità di regolamentazione; in qualità di esempio virtuoso, è stato preso come riferimento il corpo normativo svizzero e della Repubblica di Malta. Entrambi questi paesi hanno dato vita ad un sistema di norme che inquadra senza ambiguità la qualificazione giuridica dei *token* emessi in seguito ad una ICO; così facendo, hanno istituito dei poli di riferimento per le imprese, attraendo investimenti da capitali esteri. In assenza di norme prive di ambiguità applicative, si possono venire a creare situazioni in cui secondo una ricostruzione *ex post* venga stabilita l'applicazione di una disciplina che comporti sanzioni anche piuttosto afflittive. È il caso delle notevoli pronunce ad opera dell'autorità del mercato e della borsa statunitense, dove si è sussunta sotto la fattispecie delle *securities* diverse ICO. Inoltre, anche la Banca d'Italia e la CONSOB si sono trovate a pronunciarsi sulla classificazione di alcune ICO e la disciplina concretamente applicabile, dimostrando come ancora oggi sia incerta e soggetta ad una valutazione caso per caso la qualificazione di queste nuove tipologie di raccolta del risparmio.

Passando poi all'analisi dal punto di vista dei reati configurabili attraverso l'uso delle criptovalute, è stato poi tracciato quello che è possibile definire il profilo

criminologico del *cyber*-criminale, la cui indole criminosa è agevolata dall'utilizzo del *computer* e della rete *internet*. Nello specifico, è stata fornita una panoramica dei c.d. *criminal smart contracts*, con cui è possibile configurare reati eterogenei sfruttando il funzionamento dei contratti auto-eseguibili sulla *blockchain*.

Il reato di riciclaggio (art. 648-*bis* c.p.), e quelli ad esso affini come l'autoriciclaggio (art. 648-*ter*.1) ed anche il delitto di impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter*), sono quelli la cui commissione è più agevolata dall'utilizzo delle criptovalute. Non solo grazie alla loro anonimità, ma anche dall'utilizzo di particolari *escamotage* come il c.d. *mixing*, che permette di rendere ancora più difficile la ricostruzione dello storico delle transazioni e la relativa provenienza sulla *blockchain*; il tutto agevolato dall'utilizzo dei *browser* di navigazione anonima e le applicazioni di mascheramento dell'indirizzo IP.

Riguardo i diversi reati di abusivismo bancario e finanziario, è stato sottolineato come in dottrina sono quasi nella totalità concordi le opinioni che ritengono non integrati tali reati dall'utilizzo delle criptovalute in relazione alle condotte descritte nelle fattispecie. In virtù del principio di tassatività, non è possibile ricomprendere i *bitocoin* nell'alveo operativo delle norme; servirebbe una puntuale modifica legislativa che permettesse di far rientrare le criptovalute nello spettro applicativo dei suddetti reati.

L'inquadramento fiscale delle criptovalute e dei redditi ad esse correlate concorrono alla formazione della base imponibile delle imposte sui redditi, in particolare l'IRES, pertanto la relativa non dichiarazione può comportare, nel caso in cui vengano superate le soglie di rilevanza, la configurazione dei reati tributari. Discorso diverso per l'imposta sul valore aggiunto, dove i redditi relativi alla conversione o scambio di criptovalute rientra tra le operazioni esenti.

Infine, è stata condotta un'analisi dal punto di vista dell'impatto delle criptovalute nell'ambito del diritto processuale penale. Già con l'avvento dei documenti e dei dati informatici il diritto processuale ha subito adattamenti e integrazioni legislative con l'obiettivo di far rientrarli rientrare nell'ambito applicativo della legge. In particolare, la Convenzione di Budapest è stata determinante nell'introdurre novità legislative soprattutto riguardo le modalità di acquisizione delle prove elettroniche, ma anche alle procedure di corretta conservazione e protezione di quest'ultime una volta apprese.

È stata analizzata la particolare natura della prova digitale e le problematiche che essa comporta nel momento delle indagini e dell'utilizzo dei mezzi di ricerca della prova. Il caso più problematico è rappresentato dal sequestro dei *bitcoin* in quanto è ancora necessario sviluppare tecniche adeguate che permettano un efficace e sicuro sequestro delle chiavi private dei *wallet*. Infine, sono stati illustrati i casi di sequestro e confisca di *bitcoin* più celebri dell'esperienza statunitense e italiana.

Concludendo, al termine della stesura del presente elaborato è possibile affermare come le criptovalute si prestino a svariate attività illecite, e una loro regolamentazione è necessaria quanto meno per regolare il loro utilizzo come strumento finanziario a tutela del mercato e dei consumatori. Le misure di contrasto del riciclaggio e del finanziamento del terrorismo si possono, purtroppo, limitare soltanto ad una verifica e controllo dei soggetti e delle criptovalute "in ingresso" nel sistema finanziario e bancario.

A livello processuale, infine, è necessario che le procure e le autorità investigative si dotino di particolari competenze tecniche in modo tale da poter condurre indagini efficaci. Così facendo, si potrà contrastare l'utilizzo delle valute virtuali per scopi illeciti non solo a livello repressivo, ma si può anche agire sul piano di preventivo in quanto attualmente la consapevolezza della difficoltà nel condurre le indagini rendono appetibile l'uso degli strumenti informatici e delle criptovalute per commettere reati. Nonostante ciò, l'ideale sarebbe rafforzare ancor di più le unità investigative transnazionali, non solo a livello comunitario ma soprattutto nei paesi meno sviluppati, i quali nella maggior parte dei casi sono luogo d'azione preferito dai *cyber*-criminali proprio in virtù della scarsa competenza delle autorità locali.

BIBLIOGRAFIA

ACCINNI G., P., *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)* in *Archivio Penale* n. 1/2018

AL FAHDI M., - CLARKE N., L., - LI F., - FURNELL S., M., *Suspect-oriented intelligent and automated computer forensic analysis*, Vol. 18, settembre 2016, 65-76

AMETRANO, *Oltre l'oro digitale? Ben poco altro*, reperibile al link: http://nova.ilsole24ore.com

ANDOLINA E., *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della "privacy" e onde eversive*, in *Archivio penale*, 2015, 3, 916-938.

ANDONI M., - ROBU V., - FLYNN D., - ABRAM S., - GEACH D., - JENKINS D., MCCALLUM P., - PEACOCK A., *Blockchain technology in the energy sector: A systematic review of challenges and opportunities* in *Renewable and Sustainable Energy Reviews* n. 100, 2019

ANGELINI M., *Il reato di riciclaggio (art. 648-bis c.p.)*, Torino, 2008

ANNUNZIATA, *Distributed Ledger Technology e mercato finanziario: le prime posizioni dell'ESMA, in* Fintech, 2019

ANTOLISEI F., *Manuale di diritto penale. Parte speciale – I*. XVI ed., Milano 2016

ANTONOPOULOS M. A, *Mastering Bitcoin*, 2015

ARSHAD H., - GAN A., - ANILA K., - BUTT A., *A multilayered semantic framework for integrated forensic acquisitionon social media* in *Digital investigations*, Volume 29, giugno 2019, 147-158

ARVIND N., *What appened to the crypto dream, Part 1*, in *IEEE Security & privacy*, vol. 11, 2, marzo – aprile, 2013

ATERNO S., *Art. 8. Modifiche al titolo III del libro terzo del codice di procedura penale*, in CORASANITI G., - CORRIAS LUCENTE (a cura di), *Cybercrime, responsabilità degli enti e prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Padova, 2009

ATERNO S., *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito,* fasc.4, 2013, 0955B

AUQIB H., L., - ROOHIE N., M., *Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer in Digital Investigation*, n. 28, 2019,

AVDOSHIN S., M., - LAZARENKO A., V., *Bitcoin Users Deanonimization Methods*, in *Trudy*, tom. 30, vol. 1, 2018, 89-102.

BARILI A., *Accertamenti informatici*, in VALLI R., (a cura di), *Le indagini scientifiche nel procedimento penale*, Milano, 2013, 598

BASSETTI N., *Il repertamento e l'analisi della fonte di prova digitale in casi atipici: "best practices"*, in *Informatica e diritto*, 2015, 1-2, 361-371

BASSOLI, *La disciplina giuridica della seconda vita in Internet: l'esperienza Second Life,* in *Informatica e diritto*, 2009

BATIZ-BENET J., - SANTORI M., CLAYBURGH J., *The SAFT Project: Toward a Compliant Token Sale Framework*, 2017

BELLINI M., *Blockchain & Bitcoin: Come è nata, come funziona e come cambierà la vita e gli affari la tecnologia che è diventata il simbolo della rivoluzione digitale e valutaria*. Milano, 2018

BERLINGÒ V., *Il fenomeno della datification e la sua giuridicizzazione* in *Rivista trimestrale di diritto pubblico*, 3, 2017

BIASIOTTI M. A., *Presente e futuro dello scambio della prova elettronica in Europa*, in *Informatica e diritto*, 2015, 1-2, 35-63.

BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto e informatica*, 2017

BONETTI M., *Riservatezza e processo penale*, Milano, 2003

BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici* in LUPARIA L., (*a cura di*) *Sistema penale e criminalità informatica*, Milano, 2009

BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici* in LUPARIA L., (a cura di) *Sistema penale e criminalità informatica*, Milano, 2009

BRAGHÒ G., *Le indagini informatiche fra esigenze di accertamento e garanzie di difesa*, in *Diritto e informatica,* 3, 2005

BRYANS D., *Bitcoin and money laundering: mining for an effective solution*, *Indiana Law Journal,* Vol. 89, 441 e ss.

BUONOMO G., *Profili penali dell'informatica*, Milano, 1994

CAMPAGNA M., F., *Criptomonete e obbligazioni pecuniarie* in *Rivista di Diritto civile*, n. 1/2019

CAJANI F., - COSTABILE G., - MAZZARACO G., *Phising e furto d'identità digitale*, Milano, 2008

CAJANI F., *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono …*, in *Cib. dir.*, 2010

CALZONE O., *Servizi di mixing e monero* in *Il mondo dell'inteligence*, Gnosis, 28 luglio 2017, disponibile sul sito internet istituzionale del SISR al seguente link: www.sicurezzanazionale.gov.it

CAPACCIOLI S., *Bitcoin: le operazioni di cambio con valuta a corso legale sono prestazioni di servizio esenti*, in *Il Fisco*, 2015

CAPACCIOLI S., *Criptovalute e Bitcoin: un'analisi giuridica*, Milano, 2015

CAPACCIOLI S., *Il contesto dei cryptoassets e del cash out alla luce della nuova Direttiva Europea 2018/843 V Direttiva AML*, reperibile al seguente link: http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/antifrode_mezzi_pagamento/antifrode_mezzi_pagamento/GIPAF_Capaccioli.pdf

CAPACCIOLI S., *Introduzione al trattamento tributario delle valute virtuali: criptovalute e bitcoin* in *Diritto e pratica tributaria internazionale* N.1/2014

CAPONERA A., - GOLA C., *Aspetti economici e regolamentari delle «cripto-attività»* in *Occasional Papers*, Banca D'Italia, n.484

CAPRIOLI, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008

CARDINO A., - GUIDA R., - RANALDI A., *Processo penale e prove documentali* in Enciclopedia (a cura di) CENDON P., Padova, 2004, 24

CARLISLE D., *Virtual Currencies and Financial Crime. Challenges and Opportunities*, Royal United Services Institute for Defence and Security Studies, *Occasional Paper*, marzo 2017

CASEY, *Digital evidence and computer crime*, in *Academic Press*, 2000, 196

CASSIBBA F., *L'ampliamento delle attribuzioni del Pubblico Ministero distrettuale* in LUPARIA L., (*a cura di*) *Sistema penale e criminalità informatica*, Milano, 2009

CHIAVARIO M., *Le nuove tecnologie e processo penale in giustizia e scienza: saperi diversi a confronto*, Torino, 2006

CHIRIATTI M., *I nove (falsi) miti più comuni di bitcoin e delle valute virtuali*, in «Il Sole 24 Ore», https://www.ilsole24ore.com/art/tecnologie/2016-02-02/bitcoin-e-anonimo-171022.shtml?uuid=AC45ZDM C, 3 febbraio 2016

CLOUGH J., *Principles of cybercrime,* Cambridge, 2015

COLE D., - FABBRINI F., - SCHULHOFER S., *Surveillance, Privacy and Trans-Atlantic Relations* Oxford, 2017

CONSO G., - GREVI V., - BARGIS M., *Compendio di procedura penale*, VIII, Milano, 2016

CONSULICH F., *La norma penale doppia. Ne bis in idem sostanziale e politiche di prevenzione generale: il banco di prova dell'autoriciclaggio*, in *Rivista trimestrale diritto penale dell'economia*, n.3-4/2018

CONTI S., *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica e diritto*, 2015, 1-2, 153-164.

COSTABILE G., *Come funzionano le investigazioni e i sequestri su bitcoin,* reperibile al seguente link: https://www.agendadigitale.eu/sicurezza/come-funzionano-le-investigazioni-e-i-sequestri-su-bitcoin/

COSTABILE G., *Scena criminis, documento informatico e formazione della prova penale*, in *Diritto e informatica,* 3, 2005

CROSSER N., *Initial coin offerings as Investment Contracts: are a blockchain Utility tokens securities?*, in *The University of Kansas Law Review*, dicembre 2018

CUCCURU P., *Blockchain ed automazione contrattuale. Riflessioni sugli* smart contracts in *Nuova giurisprudenza civile commentata*, parte seconda n. 1/2017

CUOMO L., - GIORDANO L., *Informatica e processo penale*, in *Processo penale e Giustizia*, 2017

CUOMO L., - RAZZANTE R., *La disciplina dei reati informatici*, Torino, 2007

D'AGOSTINO L., *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del d.lgs. 90/2017*, in *Rivista di Diritto Bancario*, 1/2018

DANIELE M., *La prova digitale nel processo penale* (Relazione, con integrazioni e note, svolta al Convegno "Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali", Como,21-22 maggio 2010), in *Rivista di diritto processuale*, 2011, 2, 283-298.

DANIELE M., *La prova digitale nel processo penale* in *Rivista di diritto processuale*, 2011, 2, 283-298., 5 ss.

DANIELE M., *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Processo penale e Giustizia*, 2018, 5

DANIELLI A., - DI MAIO D., - GENDUSA M., - RINALDI G., *bitcoin e criptovalute, funzionalità e rischi delle monete virtuali, InDiritto*, 2018, Milano

DE GREGORIO E., *Riflessioni in tema di attualità e prospettive della raccolta e dello scambio della prova digitale* (Intervento al Seminario organizzato dall'ITTIG "Trattamento e scambio della prova digitale in Europa", Senato della Repubblica, Roma, 5 ottobre 2017), in *Informatica e diritto*, 2016, 2, 171-184.

DE VIVO A., - TRINCHESE G., *Le novità della V direttiva antiriciclaggio*, in *Documenti*

di ricerca della fondazione Nazionale dei commercialisti, reperibile al seguente link http://www.dirittobancario.it/news/antiriciclaggio/le-novita-della-v-direttiva-antiriciclaggio-analizzate-dalla-fondazione-dei-commercialisti

DENTI V., *Prova documentale* (*diritto processuale civile*) in *Enciclopedia del diritto* XXXVII, Milano, 1998, 713

DI BITONTO M., L., *L'accentramento investigativo delle indagini sui reati informatici,* in *La ratifica della Convenzione del consiglio d'Europa sul* cybercrime*: profili processuali*, in *dir. Internet*, 2008, 503

DI PAOLO G., *Prova informatica (diritto processuale penale)*, in *Enc. dir., annali*, VI, Milano, 2016,

DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti,* in Diritto penale contemporaneo, consultabile al seguente link: https://www.penalecontemporaneo.it/upload/6425-divizio2018a.pdf

DOMINIONI O., *La prova penale scientifica*, Milano, 2005

DOMINIONI O., *Un nuovo idolum theatri: il principio di non dispersione probatoria*, in *Cass. pen.,* 1997

DORDAL P., L., *The dark web*, in *Cyber criminology*, *Advanced sciences and technologies for security applications*, a cura di JAHANKHANI H., Berlino, 2018

DURRIEU R., *Rethinking money laundering & Financing of Terrorism in International Law: towards a new global order*, Leiden, 2003

EFANOV D., - ROSCHIN P., *The all-pervasiveness of the Blockchain technology* in *Procedia computer science* n. 123, 2018, Mosca

FELICIONI P., *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma* (nota a Cass. sez. un. pen. 1 luglio 2016, n. 26889), in *Processo penale e Giustizia*, 2016

FELICIONI P., *Le ispezioni e perquisizioni di dati e sistemi*, in CADOPPI A., - CANESTRARI S., - MANNA A., - PAPA M., *Cybercrime,* Torino, 2019

FERRUA P., *La prova nel processo penale: profili generali*, in FERRUA P., - MARZADURI E., - SPANGHER G., (a cura di), *La prova penale*, Torino, 2013

FIANDACA G., - MUSCO E., *Diritto penale. Parte speciale*, VII ed., Bologna, 2015

FINOCCHIARO G., *La firma digitale*, in *Commentario del codice civile scialona-branca*, Roma, 2000

FIORE S., *I reati contro il patrimonio*, Milano, 2010

FISCH C., *Initial coin offerings (ICOs) to finance new ventures* in *Journal of Business Venturing*, Vol. 34, n.1, 2019

FLOR R., *Lotta alla "criminalità informatica"e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Diritto penale contemporaneo,* 2012

FLOR R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Rivista italiana di diritto e procedura penale*, 2007

FRANCO, P. *Understanding Bitcoin: Cryptography, Engineering and Economics,* Hoboken, 2014

GALLI M., - GAROTTI L., Blockchain *e* smart contract*: le novità previste dal Decreto semplificazioni* in *Quotidiano Giuridico,* 26-2-2019

GAMMAROTA A., *Lo scambio transnazionale di notizie di reati informatici: questioni di legittimità e di effettività dei diritti di difesa dell'indagato-imputato,* in *Informatica e diritto*, 2015, 1-2, 391-406.

GAROFOLI R., *Manuale di diritto penale parte speciale*, Molfetta, 2017

GASPARRI G., *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?* in *Diritto dell'Informazione e dell'Informatica*., 2015, n. 3

GHILARDUCCI D., *Criminalizzazione globale*, in *www.terrelibere.it*, gennaio 2003.

GIUDICI P., *ICO e diritto dei mercati finanziari: la prima sentenza americana* in *Le società* n. 1/2019

GRAMOLI V., *From blockchain consensus back to Byzantine consensus*, in *Future Generation Computer* Systems, 2017

GRASSO - BELLAVIA, *Soldi sporchi. Come le mafie riciclano miliardi e inquinano l'economia mondiale*, Milano, 2011

GROSSO F., C., - PADOVANI T., - PAGLIARO A., *Trattato di diritto penale,* Milano, 2007

GUALTIERI P., *Prova informatica e diritto di difesa*, in *Dir. pen. proc.*, 2008, *Dossier prova scientifica*, 70

GULLO A., *Il delitto di autoriciclaggio al banco d prova della prassi: i primi (rassicuranti) chiarimenti della Cassazione* in *Diritto penale e processo*, n. 4/2017

HILEMAN G., – RAUCHS M., *Global Blockchain Benchmarking Study,* in *Cambridge Centre for Alternative Finance,* 2017.

IBBA S., - PINNA A., - LUNESU M. L., - MARCHESI M., - TONELLI R., *Initial coin offerings and agile practices* in *Future internet* n.10/2018

JUELS A., - KOSBA A., - SHI E., *The ring of gyges: investigating the future of criminal smart contracts, http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf*

KALB L., *Il documento nel sistema probatorio*, Torino 2000

KERR O., *Digital Evidence and the New Criminal Procedure*, in *105 Colum. Law Review*, 2005, 290

KIGER A., *Profiling of cybercriminals: topic model clustering of carding forum member comment histories* in *Social science computer review*, Vol. 36, n. 5, 2018, 591-609

KOSTORIS E., *Processo penale, delitto politico e "diritto penale del nemico"*, in *Rivista di diritto processuale,* 2007

KROGH M., *Gli obblighi e le nuove sanzioni antiriciclaggio nel d.lgs. 25 maggio 2017, n. 90*, in *Notariato.*, 2017, n. 5

KWONG Y., - KWOK R., *Peer-to-Peer Computing. Applications, Architecture, Protocols and Challenges,* Boca Raton-London-New York, 2012

LA ROCCA L., *La prevenzione del riciclaggio e del finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali*, in *Analisi Giuridica dell'economia*, n.1, 2015

LAGI L., *L'accertamento tecnico ripetibile. La gestione del reperto informatico,* in CADOPPI A., - CANESTRARI S., - MANNA A., - PAPA M., *Cybercrime,* Torino, 2019

LEMME G.- PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin* in *Rivista di diritto bancario* n. 11/2016

LAMPORT L., - SHOSTAK R., - PEASE SRI M., *International Byzantine Generals Problems*, in *ACM Transactions on Programming Languages and Systems*, Vol. 4, n.3, luglio1982

LI X., - JIANG P., - CHEN T., - LUO X., - WEN Q., *A survey on the security of blockchain systems* in, *Future Generation Computer Systems*, 2017

LUCCHETTI R., voce *Giochi (teoria dei)* in Enciclopedia della Scienza e della Tecnica. http://www.treccani.it/enciclopedia/teoria-dei-giochi_(Enciclopedia-della-Scienza-e-della-Tecnica)/

LUCEV R., - BONCOMPAGNI F., *Criptovalute e profili di rischio penale nelle attività degli exchanger*, in *Giurisprudenza penale* n. 3/2018

LUPARIA L., Computer crimes *e procedimento penale*, in GARUTI G. (a cura di), *Modelli differenziati di accertamento*, t. I, Torino, 2011

LUPARIA L., *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul Cybercrime*, in LORUSSO S., (a cura di), *Le nuove norme sulla sicurezza pubblica*, Padova, 2008

LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (L. 18 marzo 2008 n. 48). I profili processuali*, in *Diritto Penale e Processo,* 6, 2008

LUPARIA L.*, Sistema penale e criminalità informatica*, Milano, 2009

LUPARIA L., *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in LUPÁRIA e ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007

MAJORANA D., *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web,* in *Corriere Tributario* n. 8 del 2018

MANCINI N., Bitcoin*: rischi e difficoltà normative*, in *Banca impresa società*, 1, 2016

MANENTE M., Blockchain*: la pretesa di sostituire il notaio,* in Notariato n.3/2016

MARAFIOTI L., *Digital evidence e processo penale*, in *Cassazione penale*, 12, 2011

MARINUCCI G., - DOLCINI E., - GATTA G., L., *Manuale di diritto penale – Parte generale*, Milano, 2018

MAUGERI M., *Elementi di criticità nell'equiparazione, da parte dell'AEEGSI, dei* «prosumer» *ai «consumatori» e ai «clienti finali»* in *Nuova giurisprudenza civile commentata*, parte seconda, 2015

MAY T., C., *The Crypto Anarchist Manifesto*, 1988

MENDUNI E., *Enciclopedia della scienza e della tecnica*, 2010. Consultabile presso il seguente link: http://www.treccani.it/enciclopedia/prosumer_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/

MICHELLE GALLANT., *Money Laundering and the Proceeds of Crime,* Northampton, MA, USA, 2005

MILLS, J., "*Internet Casinos: A Sure Bet for Money Laundering*", JMLC, 8, 2018

MOLINARI M., F., *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cassazione penale,* 2, 2012

MOLINARI M., F., *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.*, 2013

MOLINARI M., F., *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2, 2012

MONTI A., *La nuova disciplina del sequestro informatico* in LUPARIA L., (*a cura di*) *Sistema penale e criminalità informatica*, Milano, 2009

MOSCARINI P., *Ispezione (diritto processuale penale)*, in *Enc. dir., Agg.*, vol. II, Milano, 1998

MOSCARINI P., *Principi delle prove penali*, Torino, 2014

MULINARI S., *Cyberlaudering: riciclaggio di capitali, finanziamento del terrorismo e crimine organizzato nell'era digitale*, Torino, 2003

NADDEO M., N*uove frontiere del risparimio, bitcoin exchnage e rischio penale* in *Diritto penale e processo*, n. 1/2019

NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*. Consultabile al link seguente: https://bitcoin.org/bitcoin.pdf

NAPPI A., *La prova documentale e i limiti del contradditorio*, in *CP*, 2002

NAQVI S., *Challenges of Cryptocurrencies Forensics – A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals* in *ARES,* 2018, Proceedings of the 13th International Conference on Availability, Reliability and Securit, Hamburg, Germany — agosto 27 - 30, 2018, New York, NY, USA, 2018

NASTRI M., *Nuove tecnologie: l'ultima domanda* in *Notariato* n. 5/2018

NEILSON D., - HARA S., - MITCHELL I., *Bitcoin Forensics: A Tutorial*, 2016, in JAHANKHANI H., *Global Security, Safety and Sustainability - The Security Challenges of the Connected World*, 2017, in *Communications in Computer and Information Science*, vol. 630., New York, 2017

NOVARIO F., *Le prove informatiche*, in FERRUA P. – MARZADURI E. – SPANGHER G. (a cura di), *La prova penale*, Torino, 2013

NOVETTA, *Survey of bitcoin mixing services: tracing anonymous bitcoins*, Mcleans (Virginia, USA), 2015, https://www.novetta.com/wp-content/uploads/2015/10/NovettaBiometrics_BitcoinCryptocurrency_WP-W_9182015.pdf.

KERR O., *Digital Evidence and the New Criminal Procedure,* in 105 *Colum. L. Rev.*, 2005

OECD, *Future Technology Trends,* in *OECD Science, Technology and Innovation Outlook,* Parigi, 2016

PETRINI D., *La responsabilità penale per i reati via internet*, Napoli, 2004

PHILIP J., T., - PARBAT K., *BlackBerry to open code for security check*, https://economictimes.indiatimes.com/tech/hardware/blackberry-to-open-code-for-security-check/articleshow/6249666.cms

PIATTOLI B., *Il sequestro preventivo di una pagina web: il funzionalismo della rete e le sue intersezioni nelle dinamiche processuali*, in *Dir. pen. proc.*, 2016

PICOTTI L., *Cybercrime* a cura di CADOPPI A., - CANESTRARI S., - MANNA A., Cybercrime, Milano, 2019

PICOTTI L., *Profili penali del* cyberlaundering*: le nuove tecniche di riciclaggio* in *Rivista trimestrale diritto penale economia,* n. 3-4/2018

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati* in *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004

PITTIRUTI M., Digital evidence *e procedimento penale* in *Processo penale e politica criminale*, a cura di PAOLOZZI G., - MOCCIA S., - MARAFIOTI L., - LUPARIA L., - MARCHETTI P., Torino, 2017

RAPETTO U., - MANCINI D., *Novità legislative in materia di crimine informatico, legge 18 marzo 2008 n.48 di ratifica della Convenzione di Budapest*, Roma, 2008

RAPUANO S., - CARDILLO M., *Le criptovalute: tra evasione fiscale e reati internazionali* in *Diritto e pratica tributaria*, n.1/2019

RAZZANTE R., *il riciclaggio come fenomeno transnazionale: normative a confronto,* Milano, 2014

RAZZANTE R., *La regolamentazione antiriciclaggio in Italia*, Torino, 2007

REUTER P., - TRUMAN E., M., *Chasing Dirty Money: The Fight against Money Laundering*, Oxford, 2004

RICCI A., E., *Digital evidence, sapere tecnico-scientifico e verità giudiziale*, in CONTI C., (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Milano, 2011

RICHARDS, *Transnational Criminal Organizations, Cybercrime and Money Laundering: a Handbook for Law Enforcement Officers, Auditors and Financial Investigations*, New York, 1998.

RINALDI G. *Approcci normativi e qualificazione giuridica delle criptomonete* in *Contratto e impresa* n. 1/2019

RISPOLI FARINA., in RUGGIERO C., *La nuova disciplina dell'antiriciclaggio*, Torino, 2009

RIVELLO P., *Tecniche scientifiche e processo penale*, in *Cassazione penale*, 4, 2012

ROSEMBUJ T., *Bitcoin*, Barcelona, 2016

ROSSI G., *Il cyberlaw tra metafore e regole* in *Rivista di diritto civile,* n. 6, 2002

RUGGIERO F., *Momento consumativo del reato e conflitti di giurisdizione nel* cyberspazio, in *Giurisprudenza di merito*, n.1/2002

RUGGIERI F., *Novità. Il protocollo 16 alla CEDU in vigore dal 1 agosto 2018. La proposta per l'ordine europeo di conservazione o di produzione della prova digitale*, in *Cassazione penale*, 2018, 7-8

RUGGIERI F., *Profili processuali nelle investigazioni informatiche*, in PICOTTI L (a cura di) *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004

SAGLIOCCA A., *"Open Source Intelligence" e "Deep Web": scenari moderni delle Investigazioni Digitali*, in *Ciberspazio e diritto*, 2017, 1, 171-202

SALMON J., - MYERS G., *Blockchian and associated legal isses for emerging markets* in *EMCompass*, Washington D.C., 2019

SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tuela penale l'incriminazione dei "dual-use software*" in *Rivista Italiana di Diritto e Procedura Penale*, fasc.2, 1 giugno 2017

SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*. Ed. III. Torino, 2016

SARZANA DI S.IPPOLITO F. – NICOTRA M., *Diritto della blockchain, intelligenza artificiale e IoT,* Milano, 2018

SAXENA R., *Cyberlaundering: the next step for money launderers?* in *St. Thomas Law Review Spring*, 1998

SEMINARA S., *Locus commissi delicti, giurisdizione e competenza del cyberspazio,* in http://informaticagiuridica.unipv.it/convegni/2012/SEMINARA%2023-11-2012.pdf

SERVIDA F., E., - CASEY E., *IoT forensic challenges and opportunities for digital traces*, in *digital investigation*, Volume 28, Supplement, aprile 2019, S22-S29

SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018.

SIGNORATO S., *Types and features of cyber investigations in a globalized world* (*Tipologie e caratteristiche delle "cyber investigations" in un mondo globalizzato)* in *Diritto penale contemporaneo*, 2016, 3

SIGNORATO S., *Types and features of cyber investigations in a globalized world* (*Tipologie e caratteristiche delle "cyber investigations" in un mondo globalizzato)*. Relazione alla Conferenza biennale internazionale "Quinta sezione, scienze criminali, evoluzioni e tendenze nel diritto penale contemporaneo", Timisoara (Romania), 28 ottobre 2016, in *Diritto penale contemporaneo*, 2016, 3

SIMONCINI E., *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, in *Rivista trimestrale di diritto penale dell'economia*, n. 4/2015

SOLMS S., - NACCACHE D., *On blind signatures and perfect crimes* in *Computer Security* n.11, 1992

STALANS L. J., - DONNER C., M., *Explaining why cybercrime occurs: criminological and psychological theories* in *Cyber Criminology*, Berlino, 2018

STOKES R., *Anti-Money Laundering Regulation and Emerging Payment Technologies, in Banking & Financial Services Policy Report*, volume 35, n. 5, maggio 2013

STRANO M., *Nuove tecnologie e nuove forme criminali. Relazione alla Conferenza sul Cybercrime, Palermo*, 3-5, ottobre 2002

STURZO L., *Bitcoin e riciclaggio 2.0* in *Diritto penale contemporaneo* n. 5/2018

SWAN M., *Blockchain: Blueprint for a New Economy*, Sebastopol, USA, 2015

SZABO, *Formalizing and Securing Relationships on Public Networks,* in *First Monday, Vol. 2, n. 9, 1997*, in http:// journals.uic.edu/ojs/index.php/fm/article/view/548/469.

TESTAGUZZA A., *Digital forensics. Indagini informatiche e procedimento penale,* Padova, 2014.

TESTAGUZZA A., *Il sequestro di dati e sistemi,* in CADOPPI A., - CANESTRARI S., - MANNA A., - PAPA M., *Cybercrime,* Torino, 2019

TONINI P., *La prova scientifica: considerazioni introduttive*, *in Dir. pen. proc.*, 2008, *Dossier prova scientifica*, 8.

TORRE M., *La raccolta della prova digitale in Italia: dagli accertamenti statici al captatore itinerante* (Intervento al Seminario organizzato dall'ITTIG "Trattamento e scambio della prova digitale in Europa", Senato della Repubblica, Roma, 5 ottobre 2017), in *Informatica e diritto*, 2016, 2, 157-170.

WERBACH, *Trust, But Verify: Why the Blockchain Needs the Law*, in *Berkeley Technology Law Journal*, 2018

ZACCHÉ F., *La prova documentale*, Milano, 2012

ZAGARIS B., - MACDONALD S., *Money Laundering, Financial Fraud, and Technology: The Perils of an Instantaneous Economy* in *George Washington Journal of Law & Economics*, 3/1992

ZAMPERINI V., *Impugnabilità del sequestro probatorio di dati informatici*, in *Dir. pen. proc.*, 2016

ZICCARDI G., *L'ingresso della computer forensics nel sistema processuale italiano: alcune considerazioni informatico-giuridiche* in LUPARIA L., (*a cura di*) *Sistema penale e criminalità informatica*, Milano, 2009

ZICCARDI, *Scienze forensi e tecnologie informatiche*, in LUPÁRIA e ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007

SITOGRAFIA

www.activism.net

www.agendadigitale.eu.

www.agenziaentrate.gov.it

www.agi.com

www.altalex.com

www.arijuels.com

www.bancaditalia.it.

www.bbc.com

bitblendervrfkzr.onion

https://bitcoinwhoswho.com

blockchatvqztbll.onion

www.blockchain4innovation.it

www.chiomenti.net

www.coingecko.com

www.coinschedule.com

www.corriere.it

www.dirittobancario.it

www.eba.europa.eu

www.ecb.europa.eu

www.finma.ch

www.ilsole24ore.com.

www.lastampa.it

www.novetta.com

www.penalecontemporaneo.it

www.repubblica.it.

www.sec.gov.

www.sicurezzanazionale.gov.it.

www.treccani.it.

www.tunnelbear.com

www.walletexplorer.com

www.weidai.com

https://z.cash

RIFERIMENTI GIURISPRUDENZIALI

Cass. Sez. un., 26.11.2009 (dep. 30.3.2010), n. 12433

Cass., Sez. 2, sent. n. 26229 del 09/05/2017 – dep. 25/05/2017, Rv. *contra* Cass., Sez. 6, sent. n. 1333 del 04/11/2015 – dep. 14/01/2016

Cass., sez. II, 15.4.2011, n. 17748

Cass., sez. II, 24.10.2013, n. 47147

Cass., Sez. III, 5 luglio 2012, Lafuenti, in *C.E.D.* Cass., rv. 253573

Cass., sez. un., 29 gennaio 2015, n. 31022, in *Foro it.*, 2016, 1, 2, 52

Cass., sez. V, 8.6.2018 (dep. 19.7.2018), n. 33862.

Cass., Sez. VI, 7 aprile 1997, IANNINI, in *C.E.D. Cass., rv.* 207591

Corte di Giustizia UE, Sez. V, 22 ottobre 2015, Causa C-264/14, Skatteverket c. David Hedqvist, con nota di CAPACCIOLI S., *Bitcoin: le operazioni di cambio con valuta a corso legale sono prestazioni di servizio esenti*, in *Il Fisco*, 2015

GUP Milano, 29.10.2008, in Riv. giur. ec. az., 2009, n. 5, 111 s., nota di FLOR R.

Sez. V, 14 ottobre 2009, Virruso, in *C.E.D.* Cass., rv. 246954
Tribunale, Firenze, sez. fallimentare, sentenza 21/01/2019 n° 18