LUISS

DOTTORATO DI RICERCA IN DIRITTO E IMPRESA

XXXII CICLO

LA CRIMINALITÀ ECONOMICA NELL'ERA DELLA *BLOCKCHAIN*

Modelli di responsabilità penale e nuove esigenze di tutela

TUTOR
Prof. Antonio Gullo

CANDIDATO
Luca D'Agostino

A.A. 2019/2020

LUCA D'AGOSTINO

LA CRIMINALITÀ ECONOMICA NELL'ERA DELLA *BLOCKCHAIN*
Modelli di responsabilità penale e nuove esigenze di tutela

A te Papà,

sempre nel mio cuore e nei miei pensieri

INDICE

pag.

INTRODUZIONE 1

CAPITOLO I

DALLA DISINTERMEDIAZIONE DEGLI SCAMBI ALLA NASCITA DEL MERCATO DELLA CRIPTOMONETA.

1. Le origini. Dal movimento crittoanarchico alla creazione di Bitcoin 9
   1.1. La forza centrifuga: *dominium* crittografico e disintermediazione degli scambi. 12
   1.2. L'opposta forza centripeta: capitalismo e concorrenzialità nel mercato dei *token*. 14
2. Il funzionamento tecnico della *blockchain.* 16
   2.1. Incentivi economici e validazione delle transazioni. 18
   2.2. Le diverse tipologie di infrastruttura. 19
   2.3. Mercato valutario virtuale ed economia della tokenizzazione. Alcune considerazioni preliminari. 21
3. Fondamenti giuridici della tecnologia a registro distribuito. Realtà e prospettive di regolazione del fenomeno. 23
   3.1. La definizione legislativa di DLT nella legge di conversione del decreto semplificazioni. 24
   3.2. *Smart contract,* efficacia probatoria e validazione temporale dei documenti registrati in *blockchain.* 25
4. La "poliforme" natura giuridica dei valori virtuali e le nuove frontiere della criminalità economica. 27

CAPITOLO II

AZIONE, OMISSIONE ED EVENTO IN *BLOCKCHAIN*.

1. Rilievi introduttivi. La potenzialità criminogene della tecnologia a registro distribuito. 29
   1.1. Le caratteristiche del cyberspazio e la commissione di reati *online*. 31

1.2. Transnazionalità degli illeciti e garanzia dell'anonimato. Le ragioni dell'utilizzo delle applicazioni economico-finanziarie della *blockchain* per propositi criminosi. 33
1.3. Cybercriminalità economica e desensibilizzazione soggettiva. 35
2. La tecnologia a registro distribuito e il diritto penale nel cyberspazio. 37
2.1. Azione ed evento nel diritto penale dell'informatica. 37
2.2. Azione ed evento in *blockchain*. 39
2.3. Omessa convalida, regole del consenso e caducazione del blocco. 40
3. *Smart contract* e agenti *software* autonomi. Considerazioni sul rapporto di autoria tra transazione illecita e operatore economico. 44
3.1. Esecuzione automatica del contratto e responsabilità penale. 47
3.2. Azione automatica del *software* e condotta penalmente rilevante. Un quadro di sintesi. 48
3.3. *Criminal smart contract* e *dual use software*. 50
4. L'evento in *blockchain* (rinvio) 54
5. Registri distribuiti e *locus commissi delicti*. 55
5.1. Principio di territorialità, reati informatici e luogo di commissione del reato 56
5.1.1. Il punto delle Sezioni Unite sul luogo di commissione dell'accesso abusivo a sistema informatico. 58
5.1.2. Rilievi critici. Le questioni irrisolte sul luogo di commissione del reato informatico. 61
5.2. L'ubiquità nell'infrastruttura. Problematiche relative all'individuazione del luogo di commissione del reato in *blockchain*. 63
5.3. Registri distribuiti e disciplina della continuazione *ex* art. 81 c.p. 65
5.4. Registri distribuiti e *tempus commissi delicti*. 67
5.5. *Locus commissi delicti* e natura ubiquitaria dell'infrastruttura. Alcune considerazioni conclusive. 70
6. Obblighi di controllo e omesso impedimento di reati. La posizione di garanzia in *blockchain*. 72
6.1. La causalità omissiva e la posizione di garanzia nel diritto penale. 73
6.1.1. Le fonti dell'obbligo giuridico impeditivo. Sintesi dello stato dell'arte. 74
6.1.2. Obbligo di garanzia e teoria del rischio. Brevi cenni. 78
6.2. *Internet Service Provider* e libertà nella rete 79
6.2.1. I modelli di responsabilità dell'ISP 83
6.2.2. In particolare: la responsabilità *per omissionem*. 86
6.3. *Blockchain* private e ibride. 87
6.3.1. *Blockchain permissioned* e titolarità del sistema. 89

6.3.2. *Blockchain permissioned* e posizione di garanzia. 92
6.4. Organizzazioni autonome decentralizzate, *governance* interna, e controlli societari. Alcuni spunti di riflessione. 96
6.5. *Blockchain* pubbliche. Alla ricerca di un garante? 100
6.6. La responsabilità dell'*exchange* e del *wallet provider* a titolo di concorso omissivo in riciclaggio. 101
7. Considerazioni finali e prospettive *de lege ferenda.* 102
7.1. Una proposta per l'introduzione di una fattispecie di reato propria del provider. 104
8. Azione, omissione ed evento in *blockchain*. Un quadro di sintesi. 108

CAPITOLO III

VALUTE VIRTUALI E NUOVE FRONTIERE DELLA CRIMINALITÀ ECONOMICA.

1. Le funzioni economiche dei valori virtuali. Una premessa di ordine metodologico. 112
1.1. Valute virtuali e moneta avente corso legale. 114
1.2. Bitcoin e funzioni tipiche della moneta. 117
1.3. Speculazione finanziaria e volatilità del prezzo della criptomoneta. 119
1.4. Mercato valutario virtuale e variabili macroeconomiche. Spunti di riflessione sulla condizione di equilibrio nel modello keynesiano della moneta. 120
1.5. Conclusioni in punto di natura giuridica delle valute virtuali dalla prospettiva del diritto penale. 123
1.5.1. Ricchezza virtuale e "profitto" in senso penalistico. 124
1.5.2. L'*asset* virtuale come documento informatico. Brevi cenni sulla punibilità del falso *ex* art. 491-*bis* c.p. 126
2. Alcuni aspetti definitori delle valute virtuali. 128
2.1. I primi tentativi di 'messa a fuoco' del fenomeno. La posizione delle autorità bancarie e finanziarie tra scetticismi e dubbi interpretativi. 129
2.2. La definizione di valuta virtuale nell'attuale quadro normativo. 132
2.3. Conclusioni sulla definizione di valuta virtuale. 135
3. Il riciclaggio dei proventi delittuosi nell'era della *distributed economy*. 136
3.1. Riciclaggio (art. 648-*bis* c.p.) e *cyberlaundering.* 138
3.1.1. In particolare: l'utilizzo delle valute virtuali per fini di riciclaggio. 141
3.2. Valori virtuali e *cyber-self-laundering* 144

3.3. Gli operatori professionali sul mercato valutario virtuale. 148
3.3.1. Piattaforme di *trading* e prestatori di servizi di cambio. 149
3.3.2. Servizi di *mixing*. 151
3.4. Valute virtuali e prevenzione del riciclaggio: dal D. Lgs. 90/2017 alla direttiva 2018/843/UE. 153
3.5. La responsabilità degli intermediari professionisti per concorso in riciclaggio. 156
3.5.1. La responsabilità dell'*exchange provider* per concorso omissivo in riciclaggio. Rinvio. 159
3.5.2. Intestazione fittizia di *asset* virtuali e trasferimento fraudolento di valori. Incertezze applicative e aporie sistematiche. 160
3.6. Cenni sulla tutela penale secondaria e sull'apparato sanzionatorio amministrativo per le violazioni della disciplina preventiva del riciclaggio. L'introduzione di una ipotesi speciale di confisca. 164
3.7. Valute virtuali e riciclaggio. Uno sguardo all'ordinamento svizzero. 165
3.8. Considerazioni finali. 169
4. Il contrasto al finanziamento del terrorismo tra prevenzione e repressione. Cenni all'evoluzione normativa. 172
4.1. *Virtual currencies and terrorist financing*. Note a margine del recente studio condotto dal Parlamento Europeo. 175
4.2. Valute virtuali e finanziamento di condotte con finalità di terrorismo (art. 270-*quinquies*.1 c.p.). 179
4.3. La criptomoneta come mezzo di scambio per l'acquisto di beni intrinsecamente illeciti sul *dark web*. Mercati neri virtuali e dintorni. 181
5. La valuta virtuale come oggetto (im)materiale del reato. Furto e indebita sottrazione di chiavi crittografiche. 184
5.1. Tra proprietà e possesso. *Dominium* crittografico, signoria di fatto e atti dispositivi in *blockchain*. 186
5.2. L'applicabilità della fattispecie comune di furto tra equilibrismi interpretativi ed esigenze di tassatività. 188
5.2.1. Portafogli elettronici e indebita sottrazione di valuta virtuale. Chiarimenti in ordine ai reati configurabili tra accesso abusivo a Sistema informatico e frode informatica aggravata. 192
5.2.2. L'appropriazione indebita di chiavi crittografiche da parte del fornitore di servizi di portafoglio digitale. 196
5.3. Una ipotesi residuale di applicazione dell'art. 624 c.p.? Il *mining* abusivo tra furto, frode informatica e truffa comune. 198
5.4. Frode informatica e sottrazione indebita di valuta virtuale: gli obblighi di criminalizzazione contenuti nella Direttiva 2019/713/UE 203

6. Valute virtuali e reati tributari nella nuova dimensione dell'economia. 205
6.1. L'assoggettamento al regime IVA delle operazioni di cambio di valuta virtuale. I principi affermati dalla Corte di Giustizia UE. 207
6.1.1. Oltre la sentenza della Corte di Giustizia. Cenni sul regime IVA applicabile alle cessioni di beni, alla prestazione di servizi e all'attività di *mining*. 209
6.2. La posizione dell'Agenzia delle Entrate sul regime fiscale applicabile alle cessioni e ai redditi derivanti da operazioni in valuta virtuale. 210
6.3. Profili di rilevanza penale dell'evasione delle imposte sui redditi e sul valore aggiunto relative ad operazioni in valuta virtuale 213
6.4. La sottrazione fraudolenta al pagamento delle imposte. 219
6.5. Le novità in materia di monitoraggio fiscale e i connessi profili sanzionatori. 223
7. Ablazione patrimoniale e confisca di valori virtuali. 227
7.1. La valuta virtuale come profitto del reato. Inafferrabilità della ricchezza digitale e limiti applicativi alla confisca. 229
7.2. Risparmio d'imposta e confisca diretta del denaro. *Quid iuris* nel caso della moneta virtuale? 231
7.3. Osservazioni conclusive. 233

CAPITOLO IV

VALORI VIRTUALI E TUTELA DEL MERCATO FINANZIARIO.

1. Dal mezzo di pagamento allo strumento d'investimento: l'informazione digitale come *asset* di natura finanziaria. 235
1.1. La "piazza" finanziaria virtuale tra mercato di scambio ed economia di prodotto. Considerazioni iniziali sulla necessità di tutela degli interessi collettivi. 237
1.2. L'*asset* virtuale come strumento finanziario. *Bene iudicat qui bene distinguit*? 239
1.2.1. I margini applicativi della definizione nazionale di prodotto finanziario. 243
1.2.2. *Trading* valutario e normativa antiriciclaggio. Rinvio. 245
1.3. Il *Fintech Action Plan* e le prime misure di attuazione. 245
1.4. Tipologia, natura e funzioni dei *token*. Incertezze ricostruttive ed equilibrismi classificatori. 247
2. Regolazione finanziaria, tutela dell'investitore e prerogative di controllo pubblico. Riflessioni sulla opportunità di un approccio flessibile alla tutela penale del risparmio. 252

2.1. *Blockchain* e *Fintech*. Spunti comparatistici sulle prime esperienze regolatorie. 255
2.1.1. L'esperienza statunitense e quella canadese. 256
2.1.2. La legislazione giapponese. 261
2.1.3. L'esperienza svizzera. Rinvio. 262
2.1.4. La normativa di Malta e di San Marino. 264
2.2. Verso un modello di regolazione flessibile? Il punto di vista della Consob sull'emissione e lo scambio di criptoattività. 267
2.2.1. Rilievi critici. 270
3. Abusivismo bancario e finanziario. Profili di rilevanza penale dell'esercizio non autorizzato delle attività e dei servizi di investimento. 273
3.1. Il regime autorizzatorio previsto dal D. Lgs. 90/2017. Limiti esegetici e criticità applicative delle fattispecie di abusivismo previste dal Testo Unico Bancario. 275
3.1.1. Conclusioni in punto di irrilevanza penale dell'esercizio non autorizzato dell'attività di cambiavalute virtuali. 278
3.2. Esercizio non autorizzato di "servizi" e le "attività" di investimento. I vasti orizzonti applicativi dell'art. 166 del Testo Unico della Finanza. 279
3.3. L'ineludibile certezza del diritto. Riflessioni sull'opportunità di regolare l'emissione e lo scambio di criptoattività finanziarie. 283
4. *Trading* di asset virtuali e tutela del mercato finanziario. 286
4.1. L'inapplicabilità delle fattispecie di *market abuse*. 287
4.2. Omissioni informative e falsità in prospetto. 289
5. Prospettive *de iure condendo*. L'assoggettamento dei valori virtuali alla disciplina finanziaria e i riflessi sul versante sanzionatorio. 292

CAPITOLO V

INVESTIGAZIONI INFORMATICHE, *BLOCKCHAIN FORENSICS* E PROCESSO PENALE

1. Introduzione. 295
2. La transnazionalità degli illeciti configurabili. La necessità di strategie di cooperazione internazionale e di coordinamento investigativo. 298
2.1. Iniziative per una *partnership* pubblico-privato. 302
3. Trasferimento illecito di fondi: una esemplificazione operativa. 304
4. Mezzi di ricerca della prova e sequestro probatorio di dati e programmi informatici. 307
5. *Blockchain forensics* e *Open Source Intelligence*. 311

5.1. Tra *publicly available data* e *legitimate expectation of privacy*. Considerazioni in ordine alla necessità di una base normativa per le indagini OSINT. 315
5.2. Indagini *open source* e protezione dei dati personali nelle attività di contrasto. 317
6. Gestione accentrata di fondi: gli *exchange provider* e l'acquisizione della prova digitale. 319
7. Sequestro e confisca di valuta virtuale. 323
7.1. *Key disclosure laws* e diritto al silenzio. 327
7.2. Uno sguardo ai sistemi di *common law*. Il modello britannico. 330
7.3. L'esperienza statunitense. 333
8. Lo strumentario processuale sul banco di prova delle valute virtuali. Luci, ombre e prospettive di riforma. 335

BIBLIOGRAFIA 339

INTRODUZIONE

L'aspetto innovativo, e per molti versi rivoluzionario, della tecnologia a registro distribuito (DLT) consiste nella *valorizzazione* delle informazioni digitali. Fin dalla sua prima comparizione, che comunemente si fa coincidere con la diffusione del codice sorgente di Bitcoin, essa ha mostrato formidabili potenzialità applicative nel settore economico-finanziario.

Le ragioni del successo riscosso in quest'ambito potrebbero, icasticamente, essere ricondotte alle caratteristiche proprie della *blockchain*, che rende artificialmente scarso ciò che, per sua natura, è duplicabile *ad infinitum*, accrescendo la fiducia degli utenti nell'infrastruttura informatica e nella disintermediazione degli scambi. La crittografia asimmetrica, sapientemente combinata con un sistema di incentivi alla partecipazione, ha condotto alla progressiva diffusione di un inedito sistema di pagamenti *peer-to-peer*, alla cui base vi è la volontà di fornire una alternativa all'attuale modello bancocentrico.

In realtà, ad oltre un decennio dalla creazione di Bitcoin, sembra che l'ideale della democratizzazione finanziaria sia prossimo al tramonto, sovrastato dalla consolidata tendenza allo sfruttamento capitalistico della nuova tecnologia. Oggi può parlarsi, senza esagerazione, dell'esistenza di un vero e proprio mercato valutario virtuale, collocato nella macroarea dei servizi della società dell'informazione. L'interesse globale per le criptovalute ha attratto forti investimenti, portando alla nascita di numerose attività economiche *a valle* dello scambio di informazioni mediante registri distribuiti. Basti pensare, in via esemplificativa, a soggetti quali cambiavalute virtuali, gestori di servizi di portafoglio elettronico, fondi d'investimento in criptovaluta, fornitori di servizi fiduciari e di certificazione elettronica, piattaforme per la raccolta di capitali.

La rapida espansione del mercato non smentisce tuttavia l'assunto alla base della creazione della criptomoneta, cioè la possibilità di trasferire valore senza ricorrere all'intermediazione di soggetti terzi. Si delineano così due diversi poli dell'economia della *blockchain*: da un lato la "risonante" proliferazione di servizi digitali basati su nuovi modelli di *business*, dall'altro la "silente" espansione degli scambi *peer-to-peer*.

Esaminando il fenomeno dalla prospettiva giuridica, ci si rende subito conto delle numerose problematiche innescate dalla diffusione dei valori virtuali. I nuovi attori del mercato operano in una dimensione parallela e complementare rispetto ai settori regolamentati (servizi di pagamento, gestione del credito, intermediazione finanziaria), senza incorrere nei limiti e nelle restrizioni della normativa pubblicistica. Sul fronte opposto, la tecnologia a registro distribuito offre ai privati la possibilità di sfuggire al sistema dei controlli statali grazie alla garanzia dell'anonimato e all'assenza di

intermediari. In entrambi i casi l'affermazione di una libertà economica priva di regole reca con sé il *rischio sistemico* della lesione di interessi di primaria importanza, quali l'integrità del patrimonio individuale e del risparmio collettivo, la sovranità monetaria, l'integrità dei mercati finanziari, l'amministrazione della giustizia.

Ecco dunque spiegate le ragioni di un'indagine volta ad approfondire i profili di rilevanza penale delle attività connesse all'utilizzo dei valori virtuali e, più in genale, dei sistemi DLT. Nell'era della *blockchain* la criminalità economica muta veste e, di pari passo con la digitalizzazione dei valori, si trasforma in un fenomeno sempre più nascosto nei meandri della rete. La crittografia, gli scambi *peer-to-peer*, e la tokenizzazione degli *asset* conferiscono una nuova linfa alla *underground economy*, facilitano la dispersione e il reimpiego di capitali illeciti, alimentando l'aspettativa di un elevato rendimento economico degli investimenti.

La dottrina penalistica[1] ha ormai da tempo messo in luce l'elevato potenziale criminogeno di Internet, rilevando come l'assenza di autorità nella rete costituisca un incentivo notevole alla realizzazione di reati *online.* Non sorprende quindi che l'affermazione di una moneta del cyberspazio faccia venire meno il deterrente principale alla commissione di reati economici in rete, rappresentato dal necessario passaggio per i circuiti di pagamento tradizionali e per la dimensione reale dell'economia, dominata dalla presenza di vincoli a carico degli operatori di settore. La moneta *peer-to-peer* diviene così uno strumento formidabile nelle mani dei criminali informatici; se nell'universo virtuale essi già godono della possibilità di agire dietro l'egida dell'anonimato, la creazione della criptomoneta ha offerto un mezzo ancora più sicuro per il compimento di transazioni illecite e la ricezione di valori, beni, e altre utilità provenienti da delitto.

L'utilizzo delle valute virtuali si innesta così su un filone già caratterizzato dalla presenza di gruppi criminali, facendo germogliare nuovi fenotipi criminosi. Basti pensare allo scambio di *token* come strumento per riciclare denaro sporco, trasferire valori in modo fraudolento, finanziare il terrorismo, eludere la riscossione coattiva dei crediti erariali, eludere il monitoraggio fiscale. Le novità introdotte dalla direttiva 2018/843/UE rappresentano soltanto un tassello isolato del mosaico che il legislatore dovrà comporre per vincere le sfide lanciate dall'economia virtuale.

Occorre nondimeno interrogarsi sull'opportunità di reprimere le condotte illecite aventi ad oggetto i valori virtuali e di proteggere l'interesse patrimoniale degli investitori. La tutela della criptomoneta come entità economicamente rilevante ha di recente trovato un primo riconoscimento legislativo con l'emanazione della direttiva 2019/713/UE sul contrasto alle frodi nei mezzi di pagamento diversi dai contanti, che obbliga gli Stati membri dell'Unione alla criminalizzazione delle condotte di indebita sottrazione di valuta virtuale.

Si delineano così due esigenze opposte, ma complementari. Da una parte assicurare la tenuta dell'ordinamento penale dinanzi ai rischi dell'economia virtuale, dall'altra

[1] Per riferimenti bibliografici si rinvia al Cap. II, § 1.1. ss.

garantire la protezione delle oggettività giuridiche emergenti. L'analisi critica delle problematiche qui accennate rappresenta l'obiettivo primario del presente lavoro. Essa sarà condotta analisi sarà condotta collocando il dibattito sorto intorno al fenomeno valutario virtuale negli schemi propri del diritto penale dell'informatica. Si intende così fornire al lettore una valida chiave di lettura per inquadrare l'utilizzo delle criptovalute entro categorie già note alla scienza penalistica.

Sul piano metodologico non è superfluo sottolineare l'importanza della comparazione giuridica per un compiuto esame delle prospettive di regolazione del fenomeno. La transnazionalità dei reati informatici e la diffusione globale delle valute virtuali rendono di per sé evidente la limitatezza di qualsiasi strategia di contrasto circoscritta ai confini nazionali. Sarà pertanto utile guardare oltre i confini nazionali per cogliere similitudini e differenze nell'approccio seguito dai legislatori nazionali, concentrando l'attenzione sulle esperienze più significative come quella svizzera e quella statunitense.

La trattazione si apre con un breve *excursus* sulle origini e sul funzionamento della tecnologia a registro distribuito, che fungerà da premessa per il successivo approfondimento penalistico.

Nel *primo capitolo* saranno esaminati i fondamenti storici del fenomeno, partendo dalla creazione di Bitcoin fino alla nascita del mercato valutario virtuale. Le più recenti evoluzioni dimostrano come la moneta *peer-to-peer* sia divenuta uno strumento di affrancamento dalle regole del mercato, anziché un mezzo di democratizzazione finanziaria. Al modello della *blockchain* pubblica, caratterizzato dalla decentralizzazione della rete in una pluralità di nodi, si contrappone quello delle infrastrutture private governate da un'autorità centrale. Si fa così rientrare dalla finestra la chimera dell'intermediazione degli scambi, che dimostra come il mito della *blockchain* sia spesso sfruttato al solo fine di raccogliere capitali senza passare per le maglie del sistema bancario.

In tempi recenti il legislatore italiano ha accolto con favore le potenzialità offerte dai sistemi DLT. La legge 11 febbraio 2019 n. 12 ha infatti inserito all'interno D.L. 14 dicembre 2018 n. 135 un nuovo art. 8-*ter* che, nel definire le tecnologie basate su registri distribuiti e gli *smart contract*, attribuisce valore legale alle informazioni registrate in *blockchain.* La norma non è esente da rilievi nel delegare all'Agenzia per l'Italia Digitale la determinazione dei requisiti necessari alla validazione temporale elettronica e all'efficacia probatoria delle transazioni mediante *blockchain.*

Al di là degli aspetti tecnici, la novella legislativa non fornisce alcuna indicazione utile a risolvere l'annosa questione circa la natura giuridica delle valute virtuali. Nonostante il legislatore abbia finora prestato maggiore attenzione alla funzione monetaria delle valute virtuali, la tendenza deflazionistica della criptomoneta rende l'opera classificatoria estremamente complessa per via dell'elevata propensione degli attori economici ad acquistarla e scambiarla con l'aspettativa di un ritorno finanziario dell'investimento.

Per far fronte alle possibili criticità il D. Lgs. 125/2019 è intervenuto sulla relativa nozione, ampliandola in modo da ricomprendere anche gli utilizzi degli asset digitali "per finalità di investimento".

Ebbene, la "doppia anima" delle valute virtuali – una monetaria, l'altra speculativa – solleva non pochi dubbi sulla disciplina applicabile e sui profili di responsabilità connessi al superamento dei limiti imposti dalla normativa di settore. Secondo l'opinione condivisa nel presente lavoro, il dilemma della natura giuridica dei valori non ammette una soluzione univoca e va affrontato su basi necessariamente relative.

L'indagine svolta nel *secondo capitolo* si concentra sui profili di parte generale, e in particolare sulle questioni legate alla condotta e all'evento nei reati commessi mediante l'utilizzo di sistemi DLT[2]. Se è vero che l'azione e l'omissione assumono, nello spazio virtuale, dei connotati del tutto peculiari occorre chiedersi se le categorie tradizionali della scienza penalistica siano adeguate a far fronte alle sfide lanciate dalla criminalità informatica. Vista da questa prospettiva, la commissione dei reati mediante *blockchain* altro non rappresenta che la riedizione contemporanea, con un più alto grado di sofisticazione, di problematiche che da sempre caratterizzano la commissione di reati mediante strumenti informatici o telematici.

Le categorie dell'*agere* umano assumono contorni ancor più sfumati dinanzi ai peculiari meccanismi di formazione del consenso e di convalida delle transazioni in *blockchain*. Il concetto penalistico di azione diviene ancor più evanescente a causa dell'automazione dei processi decisionali, mentre la sostituzione del *software* all'uomo determina il venir meno del rapporto di *autoria* tra condotta umana e risultato informatico. L'accertamento del dolo in capo alle parti di un *smart contract* presenta diverse criticità: il programmatore, ad esempio, non può prevedere in anticipo se l'agente contrattuale verrà attivato e, soprattutto, se sarà strumentalizzato per finalità illecite.

Inoltre, la delocalizzazione delle risorse sulla *blockchain* rappresenta un fattore di evidente complicazione. La natura ubiquitaria della tecnologia a registro distribuito ha fornito una ulteriore conferma dell'impossibilità di ricorrere ai criteri tradizionali dettati dal codice penale per determinare giurisdizione e competenza.

Per quel che riguarda, infine, la possibilità di configurare obblighi di garanzia in capo ai soggetti che gestiscono o utilizzano l'infrastruttura decentralizzata, risulta necessario superare il paradigma ascrittivo delineato dall'art. 40, comma 2, c.p. in favore di modelli più flessibili di imputazione della responsabilità per omesso controllo. Dopo aver ripercorso in breve lo stato dell'arte sulla responsabilità penale del *provider*, sarà elaborata una proposta per l'introduzione, all'interno del D. Lgs. 70/2003, di una autonoma fattispecie di agevolazione colposa[3].

L'introduzione di una simile ipotesi di reato sortirebbe un *effetto responsabilizzante* per coloro che gestiscono sistemi *blockchain* privati o ibridi, che attualmente godono di una zona franca da responsabilità penale. Desta infatti forti

[2] Cap. II, § 2 ss.
[3] Cap. II, 7.1.

perplessità la scelta di non sanzionare la violazione degli obblighi di collaborazione imposti dal D. Lgs. 70/2003, che appare in controtendenza rispetto alla necessità di contenere il rischio di un impiego sistematico della nuova tecnologia per propositi criminosi.

Il *terzo capitolo* affronta invece le questioni di parte speciale, esaminando le singole fattispecie di reato in cui la valuta virtuale viene in rilievo come strumento di circolazione della ricchezza. La trattazione si apre con una riflessione sulla natura monetaria dei nuovi valori e sulla opportunità di escludere, quantomeno a fini penalistici, l'inquadramento nel concetto di "denaro".

Dal punto di vista dogmatico, la criptomoneta va considerata *strumento* o *oggetto materiale* del reato quando l'azione delittuosa si realizzi per il tramite di essa ovvero insista su di essa; come *prezzo* del reato, quando si inserisca in un rapporto sinallagmatico quale corrispettivo dato o promesso per la commissione dell'illecito; come *profitto* del reato quando ne costituisca l'utilità economica derivata in via diretta.

Un esempio paradigmatico della valuta virtuale come *strumento del reato* è dato dall'impiego come "denaro-ponte" in grado di interrompere la tracciabilità dei flussi di denaro: la criptomoneta massimizza i benefici del riciclaggio digitale[4], agevolando la movimentazione dei capitali e garantendo un più alto grado di anonimato. Diverse sono le ipotesi delittuose interessate che spaziano dal riciclaggio all'autoriciclaggio, dalle contravvenzioni previste dal D. Lgs. 231/2007 al trasferimento fraudolento di valori. Nei rapporti tra art. 648-*bis* e 648-*ter*1. C.p., emerge una smisurata espansione della sfera dell'autoriciclaggio a causa della facilità con cui i criminali possono procurarsi la disponibilità degli *asset* digitali; ciò porta ad interrogarsi sulla rilevanza penale delle operazioni di mero acquisto di valori e sul titolo di reato da applicare nelle ipotesi di concorso.

Sul fronte della prevenzione, il D. Lgs. 90/2017 aveva incluso i prestatori di servizi relativi all'utilizzo di valuta virtuale tra i destinatari della disciplina antiriciclaggio, ma solo *«limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso»*. Il recente intervento correttivo invece ha esteso il raggio applicativo, affiancando ai prestatori di servizi (nessuno escluso) anche i fornitori di portafoglio digitale. Tali novità incidono in misura significativa sulla responsabilità omissiva del *provider* per concorso in riciclaggio, fondando veri e propri obblighi di garanzia.

L'intestazione fittizia dei valori virtuali rappresenta inoltre un espediente utile per eludere i controlli incrociati e la segnalazione delle operazioni sospette, condotta che potrà assumere rilevanza come trasferimento fraudolenti di valori *ex* art. 512-*bis* c.p.

La criptomoneta si presta, infine, ad essere strumentalizzata per il finanziamento di attività terroristiche e come mezzo di pagamento per eccellenza tra gli utenti della parte oscura della rete (*darknet*). Gli ultimi rapporti dell'*European Cybercrime Center* mettono in evidenza come la propensione verso alcuni reati informatici (ad. es. il

[4] Cap. III, § 3 ss.

compimento di attacchi di *denial of service* su commissione) sia cresciuta di pari passo con la diffusione del circolante virtuale. L'indagine si articolerà lungo due direttrici principali, aventi ad oggetto l'una la descrizione del fenomeno, l'altra la risposta sanzionatoria.

La valuta virtuale sarà studiata anche quale *oggetto materiale* del reato meritevole di tutela, riflettendo sulle fattispecie criminose applicabili ai casi di indebita sottrazione. L'opzione esegetica preferibile appare quella di ricondurre la condotta nell'alveo della frode informatica (art. 640-*ter* c.p.), superando così gli evidenti impedimenti testuali all'applicazione delle ipotesi comuni di furto e di appropriazione indebita. L'utilizzo non autorizzato delle chiavi crittografiche può inoltre venire in rilievo come abuso dell'identità digitale, fatto idoneo a integrare l'aggravante speciale di cui al terzo comma dell'art. 640-*ter*. Emergono poi alcune tecniche d'attacco nuove e decisamente peculiari come il *mining* abusivo che, a seconda dei casi, potrebbe essere assimilato al c.d. allaccio abusivo, idoneo ad integrare gli estremi del reato di furto aggravato di energia elettrica, oppure alla truffa contrattuale rilevante *ex* art. 640 c.p.

La trattazione proseguirà con l'analisi dei profili fiscali delle criptovalute, rilevanti per la configurabilità dei reati previsti dal D. Lgs. 74/2000. Gli investimenti sul mercato virtuale producono spesso plusvalenze molto generose, tali da rendere possibile il superamento delle soglie di punibilità previste per i reati di omessa dichiarazione e omesso versamento. Numerose sono le questioni che si pongono all'attenzione dell'interprete, dovendosi ad esempio stabilire se la mancata indicazione in dichiarazione delle cripto-attività rilevi come dichiarazione infedele ovvero sia *ex se* idonea a rendere fraudolenta la dichiarazione, oppure se il pagamento di un corrispettivo in valuta virtuale costituisca una operazione esente ai fini IVA per i reati di omessa dichiarazione e omesso versamento.

D'altro canto, la virtualizzazione dei valori attribuisce ai contribuenti uno strumento nuovo per porre in essere complesse operazioni negoziali finalizzate Ad aggirare le norme tributarie e vanificare le procedure di riscossione coattiva dei crediti erariali. Occorrerà pertanto esaminare non solo il fenomeno dell'elusione fiscale e le ipotesi di sottrazione fraudolenta al pagamento delle imposte, ma anche le violazioni della normativa sul monitoraggio fiscale nei rapporti con l'estero.

Nessun dubbio, infine, che la moneta virtuale possa rientrare nel lato concetto penalistico di *profitto* che rileva, oltre che per l'integrazione di alcune fattispecie di reato, ai fini della confisca dei proventi delittuosi. Le questioni più controverse riguardano il *modus operandi* della misura ablatoria che dovrà essere adattata alle peculiarità degli *asset* virtuali, caratterizzati dalle obiettive difficoltà di apprensione e dalla elevata volatilità del prezzo nominale di cambio. Quanto alla confisca del profitto derivante dalla commissione di un reato tributario, si ritiene che l'equiparazione compiuta dalla sentenza *Gubert* tra il denaro e gli altri beni fungibili renda possibile la confisca in forma diretta degli *asset* virtuali anche nel caso in cui questi siano posseduti dalla società.

L'analisi svolta nel *quarto capitolo* guarda alle complesse interazioni tra il mercato valutario virtuale e i mercati finanziari tradizionali, interrogandosi sulle realtà e le prospettive di regolazione del fenomeno. I valori virtuali vengono qui in rilievo (non in funzione monetaria bensì) come strumento per il finanziamento di progetti imprenditoriali, finalizzato alla raccolta di risparmio e alla successiva quotazione su mercati secondari di scambio. L'interrogativo di fondo è dato dalla riconducibilità delle cripto-attività alla nozione di strumento finanziario *ex* MiFID II o alla categoria nazionale dei prodotti finanziari. La soluzione al dilemma classificatorio rileva non soltanto per l'assoggettamento alle disposizioni del TUF, ma anche per la possibilità di applicare le fattispecie penali poste a tutela degli investitori e dell'integrità dei mercati finanziari[5].

Per una efficace tutela del risparmio collettivo occorre fare in modo che la circolazione dei nuovi valori non contravvenga alle prerogative di controllo pubblico sull'attività degli emittenti e degli intermediari finanziari. Si ritiene a tal fine necessario un intervento del legislatore per disciplinare l'attività delle piattaforme di negoziazione e di scambio di titoli virtuali, nonché al fine di stabilire precise regole in materia di prospetto informativo.

La regolazione della materia è in grado di sortire effetti positivi anche in termini di prevedibilità della risposta sanzionatoria in caso di inosservanza delle norme di disciplina. Risulterebbe infatti più chiara la responsabilità per abusivismo finanziario *ex* art 166 nelle ipotesi di esercizio non autorizzato di servizi e attività di investimento.

In un contesto regolamentato si disporrebbe inoltre della base normativa necessaria per contrastare le condotte di *market abuse* commesse sul mercato valutario virtuale. La previsione di sanzioni contro forme di manipolazione renderà verosimilmente più solido il meccanismo di formazione dei prezzi, accrescendo la fiducia degli investitori e incentivando la crescita del Fintech.

La trattazione svolta nell'*ultimo capitolo* avrà ad oggetto gli strumenti di contrasto alle nuove frontiere della criminalità economica. Sul piano processuale penale la diffusione delle criptovalute pone numerose questioni relative alla cooperazione investigativa, all'acquisizione della prova e alle misure di ablazione patrimoniale aventi ad oggetto valori virtuali.

Di recente, gli Stati e le istituzioni sovranazionali hanno iniziato a elaborare strategie coordinamento investigativo e di cooperazione giudiziaria, che appaiono indispensabili per far fronte all'elevato grado di complessità delle indagini e alla dimensione spesso transnazionale degli illeciti connessi all'utilizzo della criptomoneta.

La disintermediazione degli scambi nel cyberspazio pone problemi di rilievo sul versante probatorio, che scaturiscono dal tramonto della figura del *provider* quale referente principale nell'acquisizione della *digital evidence*. Per supplire alle carenze istruttorie la *blockchain forensics* mette a disposizione degli inquirenti innovative tecniche d'indagine, che si affiancano agli ordinari mezzi di ricerca della prova.

[5] Cap. IV, § 4 ss.

Occorre tuttavia domandarsi, sulla scorta delle opinioni espresse dalla dottrina più autorevole[6], se e in che misura le indagini "ad alto contenuto tecnologico" – quali ad esempio l'intelligence su dati *open source* mediante potenti software di *data analytics* – possano ritenersi legittime in assenza di tipizzazione normativa.

Le criticità maggiori si rinvengono, tuttavia, nell'esecuzione delle misure cautelari reali, a causa delle peculiari caratteristiche delle valute virtuali, che rendono talvolta indispensabile la collaborazione della persona sottoposta alle indagini per ottenere la *password* d'accesso al portafoglio digitale. La richiesta da parte degli inquirenti di comunicazione della chiave segreta dovrebbe, a stretto rigore, essere coperta dalle garanzie processuali contro l'autoincriminazione ed essere preceduta dall'avviso di cui all'art. 64, comma 3, lett. b) c.p.p. sulla facoltà di rimanere in silenzio. Per far fronte alle profonde limitazioni alla speditezza ed effettività delle indagini molti ordinamenti ricorrono all'istituto della *key disclosure* obbligatoria, a cui sarà dedicata una ampia riflessione in chiave comparatistica.

La disciplina codicistica degli strumenti di ablazione patrimoniale appare comunque insufficiente a far fronte alle criticità sollevate dalla diffusione della moneta *peer-to-peer*. L'indagine si concluderà quindi con l'elaborazione di una proposta di riforma delle disposizioni del codice di procedura penale per far fronte alle particolari modalità esecutive del sequestro di valuta virtuale.

[6] Per riferimenti bibliografici si rinvia alla letteratura citata nel Cap. V, § 5 ss.

CAPITOLO I

DALLA DISINTERMEDIAZIONE DEGLI SCAMBI ALLA NASCITA DEL MERCATO DELLA CRIPTOMONETA.

SOMMARIO: 1. Le origini. Dal movimento crittoanarchico alla creazione di Bitcoin. – 1.1. La forza centrifuga: *dominium* crittografico e disintermediazione degli scambi. – 1.2. L'opposta forza centripeta: capitalismo e concorrenzialità nel mercato dei *token*. – 2. Il funzionamento tecnico della *blockchain.* – 2.1. Incentivi economici e validazione delle transazioni. – 2.2. Le diverse tipologie di infrastruttura. – 2.3. Mercato valutario virtuale ed economia della tokenizzazione. Alcune considerazioni preliminari. – 3. Fondamenti giuridici della tecnologia a registro distribuito. Realtà e prospettive di regolazione del fenomeno. – 3.1. La definizione legislativa di DLT nella legge di conversione del decreto semplificazioni. – 3.2. *Smart contract*, efficacia probatoria e validazione temporale dei documenti registrati in *blockchain*. – 4. La "poliforme" natura giuridica dei valori virtuali e le nuove frontiere della criminalità economica.

1. Le origini. Dal movimento crittoanarchico alla creazione di Bitcoin.

Sul finire del 2008 Satoshi Nakamoto pubblicava, in una nota *mailing list* dedicata ad esperti di crittografia, un articolo relativo a una nuova valuta digitale intitolato «Bitcoin: A Peer-to-Peer Electronic Cash System»[1], con cui annunciava l'avvento di un nuovo sistema di globale per effettuare pagamenti basato su un protocollo di comunicazione *peer-to-peer*.

Il documento si apre con una ricognizione delle criticità del modello attualmente dominante fondato sulla intermediazione bancaria che, oltre a richiedere una costante fiducia nelle autorità centrali, non ammette la realizzazione di transazioni totalmente irreversibili. A causa di una scelta ormai condivisa a livello internazionale, le istituzioni finanziarie hanno perduto ogni connotato di neutralità nella gestione delle risorse loro affidate; l'intermediazione aumenta inoltre i costi di transazione facendo gravare sui clienti l'utile dell'attività d'impresa. Ciò pone le basi per la creazione di un sistema di pagamento elettronico basato sull'affidabilità delle tecniche di criptazione, anziché sulla fiducia in un soggetto, che consenta alle parti di negoziare direttamente tra loro senza la necessità di un terzo intermediario[2].

[1] NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, in https://bitcoin.org disponibile in diverse lingue, tra cui quella italiana. Il documento fu inizialmente pubblicato nella *mailing list* di metzdowd.com.

[2] Così, testualmente, si legge nel documento: *«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»*.

La soluzione elaborata da Satoshi si basa sulla "valorizzazione" di dati informatici univoci e non replicabili, che le parti possono scambiare in modo sicuro e pubblicamente verificabile grazie alla combinazione della crittografia con un meccanismo di validazione diffusa delle transazioni. Il sistema si basa sulla tenuta di un registro decentralizzato, nel quale tutte le transazioni sono ordinate e accorpate in blocchi, previa marcatura temporale delle stesse, grazie all'opera prestata, a titolo oneroso, da soggetti terzi validatori. Si vuole così generare fiducia nel sistema in sé, o meglio del codice di programmazione che ne è alla base[3].

Sebbene i primi anni di storia della criptovaluta siano stati caratterizzati da forti oscillazioni del prezzo, nel lungo periodo si è avuta una vertiginosa crescita della capitalizzazione di Bitcoin che ha condotto, *medio tempore*, alla nascita di un vero e proprio mercato valutario virtuale. Risale al gennaio del 2009 la chiusura del primo blocco della *blockchain*, cui fece seguito alcuni giorni dopo il rilascio della prima versione ufficiale del *software*[4]. Nell'ottobre dello stesso anno Bitcoin fu quotato presso la piattaforma New Liberty Standard a un tasso di cambio di 0.0007 dollari, pari al costo dell'energia elettrica che un computer deve consumare per estrarre la valuta. Si dovrà attendere sino al maggio 2010 per la prima compravendita di beni in Bitcoin di cui si abbia memoria: due pizze a domicilio al prezzo di 10.000 BTC, acquisto che, col senno di poi, non si avrebbe remore a definire come il più costoso della storia. Qualche mese dopo fu aperta la piattaforma Mt. Gox, specializzata in *trading* di valuta virtuale, che raccolse un bacino d'utenza tale da portare il prezzo della valuta da qualche centesimo fino alla parità con il dollaro statunitense. Da quel momento la vita di Bitcoin proseguì sotto una buona stella, giungendo a risultati incredibili, che neppure il più ottimista degli investitori avrebbe potuto sperare.

Nel secondo quinquennio dalla sua creazione, il prezzo nominale del titolo iniziò a contarsi in centinaia, e poi in migliaia[5], per toccare l'apice agli inizi del 2018. In questo periodo la febbre del Bitcoin provocò una rapida proliferazione dei progetti concorrenti, gettando le basi per la creazione di un vero e proprio mercato di scambio di valori virtuali basati sulla tecnologia *blockchain*[6].

La crescita del mercato è proseguita di pari passo con l'affermazione di molte altre valute virtuali, ciascuna dotata di proprie caratteristiche e particolari funzioni. Alle note statistiche sulla tendenziale volatilità del prezzo della criptomoneta, si contrapposero segnali di indubbia stabilità del mercato, rimasti costanti negli anni, quali il numero

[3] Cfr. DE FILIPPI P., WRIGHT A., *Blockchain and the law, The Rule of Code*, *Harvard*, 2018, 10 ss.; ID., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 10 marzo 2015, in https://ssrn.com, 16 ss.

[4] Per una cronistoria della crescita di Bitcoin v. LEMME G., PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, in *Rivista di diritto bancario*, 2016, 11, 27 ss.

[5] Per statistiche aggiornate sull'andamento del tasso di cambio si veda https://bitcoincharts.com

[6] In pochi anni il mercato ha raggiunto una capitalizzazione globale di quasi 250 miliardi di dollari (di cui oltre il 60% è occupata da Bitcoin), con un volume giornaliero di transazioni di oltre 50 miliardi. Cfr. https://coinmarketcap.com, consultato il 01 agosto 2019.

delle criptomonete attive, la diffusione di nuove piattaforme di scambio e il volume di moneta reale scambiata per quella virtuale[7].

Il mito della decentralizzazione monetaria ha aperto scenari rivoluzionari, facendo presa su un'opinione pubblica divisa tra fedeli, scettici e detrattori. Tra i primi vi è chi paragona l'irruzione di Bitcoin nella *new economy* all'affissione sulla porta della cattedrale di Wittemberg delle novantacinque tesi di Martin Lutero: con la pubblicazione del codice sorgente Nakamoto ha permesso alla gente di movimentare ricchezza senza una banca, che è come dialogare con Dio senza il tramite di un sacerdote[8]. Alcuni recenti avvenimenti storici dimostrano come l'idea di un'alternativa al sistema bancario non sia del tutto destituita di fondamento; l'esempio più noto è quello del Bail-In cipriota nel marzo del 2013, che condusse i risparmiatori a un massivo acquisto di Bitcoin per sfuggire agli effetti del prelievo forzoso[9].

In realtà, che la *blockchain* possa *«fare alle banche ciò che l'email ha fatto all'industria postale»*[10] è uno scenario decisamente futuribile, smentito dal crescente utilizzo della tecnologia da parte degli istituti di credito per regolare alcuni processi aziendali. Per limitarci alla cronaca nazionale, basti pensare al recente comunicato con cui l'Associazione Bancaria Italiana (ABI) ha annunciato che a partire dal marzo 2020 le banche italiane inizieranno a utilizzare la tecnologia basata sui registri distribuiti per la tenuta dei conti reciproci tra banche per quanto riguarda la c.d. *spunta interbancaria*[11]; oppure alle statistiche dell'ultimo Rapporto ABI Lab 2019, che dimostrano come la tecnologia a registro distribuito sarà applicata ai servizi di notarizzazione e certificazione, e al *trading* finanziario[12].

La disintermediazione degli scambi è il mezzo per la progressiva dismissione della sovranità monetaria[13] grazie all'utilizzo di una valuta *peer-to-peer* decentralizzata, comune a tutti gli utenti della rete. A ben vedere, però, l'ideale della democratizzazione finanziaria ha fornito il solo input iniziale, per poi retrocedere di fronte alle istanze di

---

[7] Delle 1500 diverse criptovalute emerse a partire dal 2013, sembra che ben 600 di queste siano attivamente scambiate sul mercato. Le prospettive future sembrano rivolgersi verso una sempre maggiore "concorrenzialità" dell'offerta di criptomoneta, a causa dell'esistenza di una domanda estremamente diversificata in base all'utilizzo che ciascun investitore intende farne.

[8] Così GUTTMANN B., *The Bitcoin Bible. Gold edition*., Norderstedt, 2013, 368: «*Today's Martin Luther is Satoshi Nakamoto [who] revealed the open-source code for Bitcoin in 2009. […] Nakamoto wanted to give people the ability to move money without using a bank, and doing this like talking to God without a priest*».

[9] Cfr. FERRELL M., *Bitcoin prices surge post-Cyprus bailout,* 28 marzo 2013, in https://money.cnn.com

[10] Metafora attribuita al politico svedese Rick Falkvinge e riportata da vari quotidiani *online* di informazione finanziaria.

[11] La spunta interbancaria è il procedimento che verifica la corrispondenza delle attività che interessano due banche diverse per regolare le reciproche rimesse a chiusura di un periodo di conto. Secondo il comunicato sarà attuato il passaggio graduale dalla spunta tradizionale a quella basata sulla tecnologia DLT *blockchain*. Il sistema assicurerà piena visibilità alla movimentazione delle partite, rapidità nella gestione dei flussi relativi ai conti reciproci, con riconciliazione su base giornaliera invece che mensile, condivisione delle regole di spunta dei movimenti in modo simmetrico tra le banche controparti e gestione integrata delle comunicazioni e dei processi in caso di sbilancio. Cfr. Comunicato stampa del 15 giugno 2019, in https://www.abi.it

[12] *Rapporto ABI Lab 2019*, in https://www.abilab.it

[13] Cfr. HAYEK F. A., *Denationalisation of Money*, London, 1976

sfruttamento capitalistico del nuovo fenomeno. Potremmo descrivere il ciclo di vita della criptomoneta ricorrendo alla metafora della combinazione di due forze contrapposte: una centrifuga, prevalente nelle prime fasi di crescita del mercato, e una centripeta via via sempre più intensa e soverchiante.

1.1. La forza centrifuga: *dominium* crittografico e disintermediazione degli scambi.

A partire dai primi anni Novanta alcuni cultori della crittografia diedero vita a un movimento noto come Cryptoanarchy con l'intento di garantire l'anonimato e la piena libertà di navigazione in *internet* al riparo da forme di controllo statuale[14]. Si stimava che le procedure di validazione pubblica *peer to peer* fossero dotate di potenzialità tali di democratizzazione dei mercati, da poter perfino destabilizzare il monopolio statuale del sistema economico. In quest'ordine di idee, alcuni autori vedono nella creazione del Bitcoin – al pari delle altre criptovalute – la concretizzazione di una ideologia[15]. Esso, infatti, non solo fa venir meno la necessità dell'intermediazione di soggetti terzi nelle transazioni tra privati, ma, vieppiù, minimizza l'ingerenza dello Stato sul mercato della moneta e, in generale, nella gestione dei sistemi digitali di pagamento.

Fu dunque il mito della democratizzazione finanziaria a ispirare gli ideatori della moneta *peer to peer* nel dar vita ad un sistema di condivisione non governato da alcuna Autorità centrale. La soluzione proposta da Nakamoto si muoveva fu un terreno già battuto da alcuni precursori che, tuttavia, videro naufragare i loro progetti probabilmente a causa della scarsa diffusione globale dei mezzi di comunicazione.

Il primo tentativo risale agli inizi degli anni ottanta, quando David Chaum, pioniere della moneta elettronica, fondò DigiCash[16], sviluppando una serie di protocolli crittografici per lo scambio di valore digitale tra privati[17]. Il progetto ebbe tuttavia vita breve: dopo qualche anno di attività la società dichiarò fallimento a causa del disinteresse degli istituti bancari americani per il progetto e fu acquisita dalla concorrente eCash Technologies.

---

[14] La letteratura sul tema è ampia, specialmente in ambito sociologico. Si vedano, senza pretese d'esaustività, SCELSI R. (a cura di), *Cyberpunk. Antologia di testi politici*, Milano, 1990; DORN J. A., *The future of money in the information age*, (trad. it.), Milano, 1998; GIUSTOZZI C., MONTI A., ZIMUEL E., *Segreti Spie Codici cifrati. Crittografia: la storia, le tecniche, gli aspetti giuridici*, Milano, 1999; PACCAGNELLA L., *La comunicazione al computer. Sociologia delle reti telematiche*, Bologna, 2000.

[15] *«The main reason behind Bitcoin* is *ideology […] The origin of Bitcoin can be found in cryptoanarchy»,* in questi termini LEE D. KUO CHEN, *Handbook of Digital Currency. Bitcoin innovations, financial instruments and big data*, San Diego, 2015, 11.

[16] Per approfondimenti sulla storia di DigiCash v. https://www.chaum.com; CHAUM D., *Blind Signatures for Untraceable Payments*, in CHAUM D., RIVEST R.L., SHERMAN A.T. (eds), Advances in Cryptology, Boston, 1983, 199 ss.;

[17] Per effettuare le transazioni gli utenti potevano utilizzare chiavi crittografiche asimmetriche per inviare e ricevere "cyberbucks", valuta digitale emessa dalla società in cambio di denaro contante. Conosciuta come Blind Signature, l'invenzione di Chaum rendeva i pagamenti elettronici non rintracciabili dall'esterno.

Il movimento crittoanarchico trovò comunque la sua più compiuta definizione nel Manifesto del 1992, con cui Timothy May svelava l'esistenza di un temibile spettro, che avrebbe permesso ai consociati di effettuare scambi in modo totalmente anonimo al di fuori di ogni possibilità di controllo statale[18]. Come l'invenzione della stampa ridusse il potere delle gilde medievali e favorì il cambiamento sociale – afferma May – così anche la crittografia sovvertirà ogni forma di controllo pubblico sulle transazioni economiche. Nel momento in cui l'economia sarà basata sul mercato dell'informazione, l'anarchia crittografica *«creerà un mercato liquido per qualsiasi merce che può essere rappresentata in parole e immagini»*[19].

I sostenitori della "dottrina Cyberpunk" rifiutano l'idea dell'identità anagrafica in rete, incoraggiando l'utilizzo di pseudonimi nei rapporti tra liberi individui: la chiave pubblica diventa così l'unico referente univoco dell'identità digitale del soggetto[20]. Il *dominium* tecnologico segnerà la fine della moneta statualista e dei sistemi fiscali nazionali: tutte le transazioni economiche avverranno attraverso la rete, tra attori anonimi e con una forma di denaro contante digitale[21].

In questo scenario, l'avvento della crittografia a doppia chiave ha segnato l'inizio della "apocalisse statale". Contrariamente alla crittografia tradizionale, in cui la chiave di codifica è la stessa necessaria in seguito per decodificare il messaggio, la crittografia asimmetrica prevede due chiavi distinte: una chiave "pubblica" e una "privata"[22]. La prima potrà essere diffusa liberamente e servirà a chiunque vorrà codificare un messaggio in modo tale che solo l'utente in possesso della seconda potrà poi decodificarlo. In tal modo si rende superfluo lo "scambio delle chiavi", necessario laddove le parti cifrino il messaggio con lo stesso codice segreto[23].

---

[18] MAY T. C., *The Crypto Anarchist Manifesto*, 1992, in https://activism.net, nel quale si leggono parole per molti versi profetiche: *«A specter is haunting the modern world, the specter of crypto anarchy. Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation*». Il movimento tecno-anarcoide è anche noto con la dicitura Cypherpunk, utilizzata per definire gli attivisti anarchici (*punk*) particolarmente abili nell'utilizzo delle nuove tecnologie (*cyber*). Si veda al riguardo HUGHES E., *A Cypherpunk's Manifesto*, 1993, in https://activism.net.

[19] MAY, ibidem.

[20] Cfr. PACCAGNELLA L., *Il potere dei codici: crittografia, cypherpunk e movimenti sociali,* in *Quaderni di sociologia*, 2000, 23, § 4

[21] L'informatizzazione dei processi sociali è descritta come un moto lento ma inesorabile, destinato ad assorbire progressivamente il potere dei governi.

[22] Le due chiavi sono collegate tra loro da una relazione matematica tale che, pur permettendo l'associazione della coppia di codici, non consente di risalire all'una conoscendo l'altra, e viceversa.

[23] Lo scambio delle chiavi private rischierebbe di vanificare la segretezza e l'efficienza della corrispondenza telematica, esponendosi al pericolo di intercettazione dolosa e rendendo più farraginosa la comunicazione a distanza specie nei casi in cui manchi un rapporto di fiducia tra le parti. Con la crittografia a chiave pubblica non è più necessario che gli interlocutori condividano alcuna chiave

La crittografia asimmetrica permette inoltre di certificare la provenienza di un documento informatico mediante la firma digitale; il mittente potrà utilizzare la sua chiave segreta per generare un certificato, legato da relazioni matematiche alla rispettiva chiave pubblica, grazie al quale il destinatario potrà sincerarsi che il messaggio provenga effettivamente da una determinata persona (paternità dell'informazione) e che non sia stato modificato dopo la firma del suo autore (integrità dell'informazione). Una simile forma di crittografia è utilizzata nei sistemi *blockchain* per garantire la sicurezza degli scambi e impedire l'alterazione delle informazioni.

Considerata da questa prospettiva la moneta *peer-to-peer* sembrerebbe incarnare appieno gli ideali del movimento crittoanarchico, essendo non solo sottratta al controllo statale ma anche "pseudonima" nel senso sopra citato. Sennonché, gli sviluppi più recenti del mercato valutario virtuale dimostrano come la forza centrifuga della disintermediazione sia divenuta sempre più flebile, finendo per essere soverchiata dalla contrapposta spinta allo sfruttamento capitalistico della tecnologia a registro distribuito. La diffidenza sociale per il fenomeno, indotta probabilmente da una non corretta informazione sulla legalità delle criptovalute, ha finora ostacolato la diffusione della criptomoneta circoscrivendone l'utilizzo a una ristretta cerchia di utenti. Non da ultimo, vi è il sospetto di un impiego sistematico per finalità criminose che induce anche i più curiosi a non utilizzare il contante digitale.

1.2. L'opposta forza centripeta: capitalismo e concorrenzialità nel mercato dei *token*.

Che alla base di Bitcoin vi fosse la volontà di erodere la sovranità monetaria statale è una tesi tutta da dimostrare, o comunque nient'affatto scontata. Vi sono numerosi elementi a sostegno dell'opposta visione capitalistica del fenomeno, suffragata dal lancio di numerosi altri progetti concorrenti in *blockchain* anch'essi fondati sull'offerta di *token* e sulla remunerazione dell'attività prestata dai nodi della rete[24].

Quanto alla prima, è ormai risaputo come l'intero mercato valutario sia *de facto* governato dalle piattaforme di *exchange*, che offrono un servizio di cambio in tempo reale tra valute virtuali e tra queste e moneta avente corso legale. Il modello attualmente dominante è quello del *trading* centralizzato: la piattaforma mette a disposizione un portafoglio elettronico per il deposito della moneta, utilizzando le proprie riserve per acquistare e vendere in base agli ordini impartiti dagli utenti[25]. Questi soggetti operano esattamente come istituti bancari, offrendo servizi di custodia e di cambio a fronte del pagamento di una commissione sulle singole operazioni. Attualmente i colossi del

segreta, essendo sufficiente lo scambio delle rispettive chiavi pubbliche, che possono essere intercettate da terze parti senza alcuna compromissione dei successivi messaggi codificati. Cfr. PACCAGNELLA, *ibidem*.

[24] Si vedano *ex plurimis* i progetti Ethereum, EOS, Litecoin, Monero, Dash, Stellar.

[25] *Amplius*, Cap. III, § 3.3.1.

trading rappresentano senza esagerazione i "motori" dell'economia virtuale[26]; la quotazione di una valuta virtuale su una piattaforma di scambio può determinare il successo di un progetto o, viceversa, il suo completo fallimento. Non sembra dunque peregrina l'affermazione degli *exchange* come poli di centralizzazione dell'economia disintermediata, vere e proprie banche virtuali non soggette a vincoli normativi sull'esercizio dell'attività. Appare del resto quasi paradossale che il sito Intenet di Bitcoin indichi nominativamente i più importanti *exchange* presso cui poter acquistare la valuta[27], non considerando la palese contraddittorietà di un sistema di pagamenti *peer-to-peer* basato sull'intermediazione di multinazionali finanziarie.

La svolta capitalista è stata segnata anche dalle restrizioni all'accesso e dalle crescenti difficoltà "estrattive" della criptovaluta. Come si dirà approfonditamente nel prosieguo, il sistema Bitcoin, e in generale tutte le infrastrutture totalmente o parzialmente decentralizzate, richiedono una potenza computazionale e requisiti *hardware* sempre maggiori per poter prendere parte al processo di validazione delle transazioni. Ciò ha dato luogo a uno sbarramento di fatto alla libera partecipazione alla rete, finendo con il riservare l'attività di *mining* a una ristretta cerchia di facoltosi investitori. La gestione oligarchica del sistema di pagamenti incide sul meccanismo della formazione dei prezzi della valuta, che difficilmente scenderà al di sotto della soglia di convenienza dell'attività estrattiva. Essa rappresenta, inoltre, un pericolo per la neutralità e la decentralizzazione della rete, in grado di incidere sui meccanismi di formazione del consenso e sulla alterazione della catena dei blocchi[28]. Per far fronte all'incremento dei costi di produzione molti operatori hanno deciso di consorziarsi dando luogo a vere e proprie "centrali minerarie".

Lo scenario attuale dipinge un quadro profondamente diverso da quello prospettato dai fautori dell'anarchia crittografica, in cui la moneta *peer-to-peer* – come l'ideologia ad essa sottesa – è sfruttata per fini di profitto dai pochi capitalisti che sovrintendono all'emissione e allo scambio della ricchezza digitale. Può ancora parlarsi di decentralizzazione e disintermediazione?

Pur considerando la partecipazione alla rete e l'intermediazione negli scambi come un mercato chiuso, deve comunque darsi atto dell'opposta spinta concorrenziale data dal lancio di numerosi progetti *blockchain*[29]. Nel corso degli ultimi anni l'emissione di *token* virtuali ha rappresentato un efficace strumento per la raccolta di finanziamenti, favorita dalle aspettative degli investitori di una rapida e consistente remunerazione del capitale. La novità è rappresentata dal superamento dei limiti imposti dalle forme ordinarie di finanziamento dell'impresa quale il ricorso al capitale di rischio e il credito bancario. Esaminata da questa prospettiva, la criptomoneta pare aver aperto nuove

[26] Pur non essendo edite statistiche ufficiali, si può ragionevolmente presumere che oltre la metà dell'intero volume di transazioni sia processato dalle prime cinque piattaforme globali di *exchange.*
[27] Cfr. https://bitcoin.org/it, nella sezione "Borsa".
[28] Per approfondimenti sui meccanismi di formazione del consenso v. *infra*, § 2.2. e Cap. III, § 2.3.
[29] In argomento v. TASCA P., WIDMANN S., *The challenges faced by blockchain technologies*, in *Journal of Digital Banking*, 2017, 2, 132 ss.; TASCA P., TESSONE C., *Taxonomy of Blockchain Technologies. Principles of Identification and Classification*, 31 marzo 2018, in https://papers.ssrn.com

frontiere al *crowdfunding* favorendo l'accesso al mercato di fondi di investimento e start-up innovative. Al di là dei numerosi punti di tensione sul versante normativo, emerge piuttosto chiaramente l'ennesima deriva capitalistica dei sistemi di pagamento decentralizzati, impiegati per "fare finanza" su una piazza controllata dai gestori delle piattaforme di *trading*.

Le considerazioni fin qui espresse portano a ritenere che, probabilmente, la criptomoneta non fu concepita come *strumento di lotta al potere*, bensì quale *strumento del potere*. E seppure fosse stata creata con l'intento di liberalizzare il mercato degli scambi, l'esperienza fin qui maturata ha smentito clamorosamente questo assunto tanto da far apparire non del tutto inverosimile l'eventualità di un passaggio all'oligopolio privato dei sistemi di pagamento. Senza entrate nel merito di questioni politiche che mal si concilierebbero con gli obiettivi del presente lavoro, basti qui ricordare come, dopo una iniziale atteggiamento di chiusura, l'economia della *blockchain* abbia attratto anche i grandi poteri del mercato globale. L'esempio più noto è dato dal progetto Libra, capitanato da Facebook Inc. e governato dalla Libra Association, per l'emissione di una *stablecoin* universale da scambiare su una infrastruttura distribuita costituita da circuiti di pagamento, imprese, organizzazioni non profit, istituzioni accademiche di tutto il mondo[30]. Ecco che, per l'ennesima volta, il mito della decentralizzazione viene sapientemente impiegato per il perseguimento di scopi lucrativi – se non addirittura politici – superando i rigidi schemi imposti dalla regolazione pubblica in materia bancaria e finanziaria. È dunque da accogliere con favore la scelta del legislatore di estendere la nozione di valuta virtuale (rilevante ai fini antiriciclaggio, ma estensibile ad altri ambiti del diritto) anche alle rappresentazioni digitali di valore utilizzate per finalità di investimento[31].

L'impressione è che la moneta *peer-to-peer* sia divenuta un elegante strumento politico di affrancamento dalle regole del mercato, anziché un mezzo di democratizzazione finanziaria. La vera minaccia per le prerogative di controllo pubblico non giunge dunque dal basso, dagli ideali crittoanarchici e dalla ribellione dei consociati all'economia bancaria, quanto piuttosto dai principali portavoce della *digital economy*. Per questo motivo la risposta regolatoria degli Stati sarà uno dei fattori determinanti per valutare il reale impatto della *blockchain* sui sistemi economici.

2. Il funzionamento tecnico della *blockchain.*

La *blockchain* nasce dunque dalla combinazione di due tecnologie diverse, la crittografia asimmetrica e i protocolli di comunicazione *peer-to-peer*, all'interno di una rete interconnessa di elaboratori.

[30] La valuta sarà emessa previa costituzione di riserve di beni reali (valute nazionali, titoli di debito pubblico, *commodities* finanziarie) per abbracciare un bacino di oltre due miliardi di potenziali utenti. Per approfondimenti si legga il *white paper* di libra, https://libra.org

[31] Cfr. Art. 1, comma 2, lett. qq) D. Lgs. 231/2007, come modificato dal D. Lgs. 125/2019 (*infra*, Cap. III, § 1 e 3.4.).

Per descrivere brevemente il suo funzionamento si farà riferimento all'esempio più noto, quello di Bitcoin. In esso la creazione di nuova moneta è un fenomeno condiviso dalla comunità, che accresce la sicurezza e garantisce la continuità operativa del sistema di pagamenti. Non essendovi alcuna autorità centrale, il processo di emissione si basa su un meccanismo *peer-to-peer* puro, alla cui base vi è un algoritmo che definisce le modalità e i limiti alla creazione di nuova ricchezza per remunerare coloro che prendono parte alla validazione delle transazioni[32].

Il *white paper* di Bitcoin definisce il sistema di pagamenti come una "catena di firme digitali"[33]. Per trasferire la valuta ciascun proprietario dovrà firmare digitalmente un *hash* della transazione precedente e associarlo alla chiave pubblica del destinatario[34]. Per verificare l'effettiva disponibilità della valuta da parte del disponente e impedire fenomeni di *double spending*, le transazioni sono "annunciate" e registrate su un libro mastro pubblico che fa fede tra i partecipanti sull'ordine dei trasferimenti e sugli indirizzi tra i quali sono intervenuti. Più precisamente, i computer impegnati nel *mining* raggruppano tutte le transazioni degli ultimi minuti in un blocco, verificando che i precedenti "passaggi di mano" della valuta attribuiscano al disponente un ammontare di valuta sufficiente a coprire il *quantum* da trasferire.

La soluzione proposta da Nakamoto si basa sulla marcatura temporale delle transazioni, raggruppate progressivamente in blocchi per formare una vera e propria catena. Le nuove transazioni sono trasmesse a nodi della rete che, previa verifica della validità del trasferimento, si attivano per trovare un numero casuale che possa risolvere una predeterminata funzione algebrica. Per creare differenti valori finali a partire dai medesimi dati iniziali, rappresentati dall'insieme di transazioni riunite in blocco, il sistema Bitcoin usa un *nonce*, cioè un numero casuale che si aggiunge ai dati iniziali prima dell'applicazione della funzione di criptazione[35]. Una volta rivenuta la soluzione crittografica, il blocco viene aggiunto alla catena solo se ottiene un numero sufficiente di conferme da parte degli altri nodi[36].

---

[32] In argomento, AMATO M., FANTACCI L., *Per un pugno di Bitcoin*, Milano, 2016, 16 ss.; ROSEMBUJ T., *Bitcoin*, Barcelona, 2016, 24 ss.

[33] NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, cit., 2

[34] La funzione crittografica di *Hash* trasforma i dati del blocco in elaborazione in una stringa alfanumerica di caratteri, di ammontare predeterminato, detto valore di *hash.*

[35] Il codice sorgente di Bitcoin richiede che il nuovo valore debba iniziare con un certo numero di zeri. Non essendo possibile stabilire *ex ante* quale sarà numero che, applicata la funzione di *hash*, darà come risultato un valore che inizi con il numero predeterminato di zeri, i *computer* impegnati nel *mining* dovranno continuare a generare valori di *hash* cambiando di volta in volta, in modo causale, il numero *nonce* finché non verrà trovato il valore che soddisfa i requisiti previsti dal sistema. *Amplius,* v. Cap. V, § 3.

[36] I nodi della rete esprimono "tacitamente" la propria accettazione mediante il tentativo di creare il prossimo blocco nella catena a partire dall*'hash* del blocco precedente. Nell'ipotesi in cui venissero trovate più soluzioni matematiche allo stesso problema (*accidental fork*), sarà ritenuta corretta la catena più lunga, mentre la più breve sarà destinata a decadere. Una tale eventualità può risultare problematica per l'integrazione di alcune fattispecie di reato, nel caso in cui si debba accertare l'esistenza di un pericolo derivante dalla condotta illecita (cfr. Cap. II, § 2.3.).

Si suole definire la *blockchain* come un registro tendenzialmente inalterabile[37], poiché nessuno dei nodi dispone – né potrà mai ragionevolmente disporre – di una potenza computazionale sufficiente a imporre un "monopolio" sul processo di verifica delle transazioni. La decentralizzazione diviene così un presidio contro il c.d. attacco del 51%, che si verificherebbe laddove uno o più soggetti, avendo il controllo della maggioranza dei nodi, potessero falsificare *ex post* le registrazioni, decidere unilateralmente quali trasferimenti validare o eludere i presidi contro il *double spending*.

Per prevenire accordi fraudolenti tra i nodi della rete, i sistemi DLT fanno leva su incentivi economici di varia natura che rendono la gestione onesta del sistema decisamente più conveniente rispetto ai vantaggi che si potrebbero ottenere falsando le "regole del gioco".

2.1. Incentivi economici e validazione delle transazioni.

Nel sistema Bitcoin la prima transazione che forma il blocco "conia" una quantità predeterminata di nuova moneta che, contestualmente, viene attribuita al soggetto che ha risolto l'equazione matematica[38]. Questa forma di retribuzione, detta *Proof-of-Work* (PoW), fornisce un incentivo affinché i nodi continuino a sostenere la rete, regolando al tempo stesso l'emissione di nuovo circolante; in gergo tecnico si parla di *mining* accomunando, metaforicamente, l'emissione di nuova valuta all'estrazione dell'oro dai giacimenti minerari. Una forma di remunerazione integrativa è data dai costi marginali di transazione (*transaction fees*) che col tempo assumerà una importanza crescente fino a sostituire del tutto l'incentivo del Proof-of-Work[39].

L'incentivo economico alla validazione delle transazioni, comunemente considerato come una esternazione del rapporto di cooperazione nella *teoria dei*

[37] Una volta che il blocco è stato "minato" non può essere modificato senza ripetere nuovamente il lavoro a ritroso. Tenuto conto che i blocchi successivi sono incatenati al precedente mediante una funzione matematica, ogni variazione dovrebbe importare il rifacimento contestuale dell'intera catena di blocchi, azione che teoricamente nessun elaboratore è in grado di svolgere.

[38] Ogni quattro anni la ricompensa che i *miners* ricevono per la risoluzione del blocco si dimezza in modo da ridurre il ritmo di emissione di nuovi Bitcoin. Considerato che la convalida delle transazioni diventa progressivamente sempre più costosa, è necessario che il valore di mercato continui a crescere per rendere conveniente l'attività di *mining.* In argomento v. LEMME- PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin,* cit., 23.

[39] Considerato che il numero totale di Bitcoin è limitato a 21 milioni di unità e che la velocità di estrazione si riduce nel tempo per effetto del dimezzamento quadriennale, arriverà il giorno in cui il sistema dovrà reggersi interamente sui costi di transazione.

giochi[40], incoraggia i nodi a rimanere onesti[41]. Si postula che, anche laddove un soggetto riuscisse ad ottenere la maggioranza della potenza di calcolo della rete, troverà comunque più redditizio giocare secondo le regole, anziché rischiare di compromettere la sicurezza del sistema e il valore della propria ricchezza.

Gli incentivi economici per la partecipazione al *network* variano anche in base alla tipologia di infrastruttura considerata e alla natura pubblica o privata della stessa. Alcuni sistemi si basano su processi di selezione casuale del nodo che dovrà validare il blocco successivo. Tra questi vi è l'incentivo del *Proof-of-Stake* (PoS) attraverso cui viene distribuito un premio in forma di commissioni sulle transazioni al soggetto che ha "forgiato" il blocco[42]. Coloro che intendono prendere parte al processo di validazione delle transazioni sono tenuti a depositare una certa somma di monete (*stake*) a garanzia; le dimensioni della posta in gioco determinano le probabilità di un nodo di venir selezionato come validatore[43].

Il modello del *Proof-of-Authority* (PoA) fa leva invece su un criterio di tipo reputazionale. La previa verifica dell'identità dei componenti della rete fa venir meno la necessità di un deposito "cauzionale", potendosi presumere che i soggetti in possesso di determinati requisiti siano validatori affidabili. I sistemi che ricorrono alla PoA presentano un numero limitato di nodi, circostanza che rende la rete altamente scalabile ed efficiente ma al contempo fa venire meno le garanzie della decentralizzazione[44].

2.2. Le diverse tipologie di infrastruttura.

[40] Nella matematica applicata la teoria dei giochi analizza le decisioni individuali finalizzate ad ottenere il massimo profitto in situazioni di interazione strategica con altri soggetti. Il "gioco" è concepito come un contesto interattivo, quindi i giocatori tendono ad agire in modo razionale quando rispondono alle regole del gioco o all'influenza degli altri player. Nei giochi c.d. essenziali – a cui *mutatis mutandis* può essere paragonata la corsa all'oro digitale – i giocatori ottengono grazie alla collaborazione un guadagno superiore a quello che potrebbero ottenere giocando individualmente. Con ogni probabilità la fiducia nelle criptovalute (e dunque il loro valore di mercato) verrebbe meno se si diffondesse il timore per il compimento di azioni fraudolente da parte dei nodi della rete. Per un approfondimento sulle applicazioni matematiche della teoria dei giochi in *blockchain* v. LIU Z.,CONG LUONG N. *et al*., *A Survey on Applications of Game Theory in Blockchain*, 15 marzo 2019, in https://arxiv.org; SINGH R., DWIVEDI A.D., SRIVASTAVA G., *Bitcoin Mining: A Game Theoretic Analysis*, in https://semanticscholar.org.

[41] Coloro che partecipano alla creazione della ricchezza non hanno interesse alla commissione di illeciti, poiché se venisse meno la fiducia da parte degli utenti nel sistema ciò comporterebbe una contrazione della domanda di valuta virtuale, con conseguente decremento del prezzo di scambio.

[42] Si parla di *forging* e non di *mining* poiché, a differenza del sistema Bitcoin, la valuta preesiste al processo di validazione delle transazioni e viene distribuita sul mercato mediante *coin offering* o altre forme similari. Le infrastrutture che utilizzano la PoS vendono le valute attraverso le piattaforme di *exchange* o utilizzando *smart contract*, oppure sfruttano l'algoritmo Proof-of-Work e in seguito passano alla Proof-of-Stake (come avvenuto di recente per il protocollo di Ethereum).

[43] Tuttavia, per fare in modo che questo processo non escluda del tutto i nodi meno abbienti del *network*, il processo di selezione presenta alcuni correttivi. Un esempio è dato dal metodo della "coin age selection" facente leva su un criterio misto che accorda preferenza anche alla priorità temporale della creazione della posta.

[44] Il protocollo gode di ampie possibilità applicative soprattutto nelle *blockchain permissioned* private che si caratterizzano proprio per la selezione all'ingresso dei partecipanti e per la gestione parzialmente accentrata dell'infrastruttura.

La *blockchain* di Bitcoin rappresenta il prototipo al quale molti altri sistemi si sono ispirati per la creazione di sistemi DLT. In base alla struttura e alla titolarità dell'infrastruttura si è soliti distinguere tra *blockchain* pubbliche e private da cui discendono conseguenze significative in punto di imputazione degli effetti giuridici[45].

La *blockchain* pubblica – alla quale si è finora fatto riferimento – si caratterizza per l'assenza di titolari del sistema: il connotato essenziale è la decentralizzazione dell'infrastruttura in una pluralità di nodi gestiti da soggetti diversi[46]. L'accesso alla rete può essere *permissionless* o *permissioned:* nel primo caso chiunque può prendere parte alla rete, semplicemente scaricando il *software* base e mettendo a disposizione un *hardware* connesso al sistema; nel secondo caso sono previste particolari condizioni per il rilascio dell'autorizzazione da parte di una autorità che verifica il rispetto delle condizioni di accesso e definisce il ruolo di ciascun partecipante.

Nei sistemi totalmente decentralizzati nessun utente ha privilegi sugli altri, o può controllare le informazioni che vengono memorizzate nei registri, modificarle o eliminarle. Nei sistemi pubblici la fiducia nella rete sembra giustificarsi proprio in virtù della disintermediazione negli scambi, che rappresenta un fattore di garanzia contro i possibili abusi da parte dell'autorità centrale.

Le *blockchain permissioned* sono al contrario controllate da un'autorità centrale che determina le condizioni di accesso ed è in grado di intervenire sui dati registrati nel sistema. Si rende così possibile una *governance* dell'infrastruttura, attraverso il recupero dell'idea di centralizzazione in una rete che nasce come decentralizzata e distribuita. La fiducia degli utenti o di coloro che vi operano non è tanto (o soltanto) nell'infrastruttura in sé, ma nell'organizzazione che ne ha il controllo, ritenuta altamente affidabile e imparziale. Il gestore della rete inoltre, ha inoltre il potere di modificare le regole di funzionamento e il protocollo di formazione del consenso[47].

Le infrastrutture totalmente private non presentano differenze significative rispetto ai tradizionali protocolli di comunicazione *client-server* (*network* centralizzati) dai quali si distinguono soltanto per l'utilizzo della crittografia come strumento per la verifica e creazione di blocchi di transazioni. Benché la presenza di una autorità centrale tradisca l'ideale della disintermediazione alla base dei sistemi DLT, la creazione di questi apparati ha riscosso un notevole successo. La gestione privata della rete garantisce una migliore efficienza e permette alle imprese di accedere ai vantaggi della tecnologia a registro distribuito (sicurezza e trasparenza degli scambi, fruibilità

[45] *Amplius*, Cap. II, § 6.3. ss.

[46] Il più delle volte il sistema è supervisionato da un team di sviluppo che, dopo aver programmato e diffuso il *software* di base, sovrintende al corretto funzionamento del protocollo e agli eventuali aggiornamenti.

[47] La differenza sostanziale tra sistemi *permissioned* e *permissionless* risiede nei meccanismi di formazione del consenso: l'infrastruttura sarà tanto più centralizzata quanto minore è il numero di partecipanti in grado di prendere parte alle decisioni. La concentrazione di "potere" raggiunge l'apice nelle *fully private blockchain* nelle quali vi è una organizzazione che ha il controllo esclusivo sulla convalida delle transazioni e sulla tenuta dei registri.

di *smart contract*, emissione di *token*, accesso al mercato valutario virtuale) per il finanziamento di progetti *blockchain* in vari settori[48].

Il fenomeno deve pertanto essere esaminato in un contesto più ampio, calandolo in quella che è stata definita "economia della tokenizzazione". Il termine *blockchain* perde qui il suo significato profondo – strettamente legato all'utopia della democratizzazione finanziaria – per divenire sinonimo di innovazione, affidabilità, semplificazione ed efficienza. Una tecnologia che ha aperto nuovi orizzonti di *business* e rivoluzionato alcuni settori di mercato, tra cui quello dei servizi di certificazione informatica e dell'intermediazione finanziaria.

2.3. Mercato valutario virtuale ed economia della tokenizzazione. Alcune considerazioni preliminari.

Il vertiginoso aumento del prezzo delle più note criptovalute ha alimentato una tendenza fortemente speculativa, mettendo in evidenza l'esistenza di una florida economia di scambio dei *token*. Occorre precisare fin da ora che con il termine *token* (o anche *criptoasset*, valore virtuale, oppure *cripto-attività*) si farà riferimento all'informazione digitale, univocamente individuata grazie all'impiego di meccanismi crittografici, registrata e scambiata mediante tecnologie basate su registri distribuiti (protocolli DLT o *blockchain*).

In alcuni casi il possesso dell'informazione attribuisce al titolare un diritto ad ottenere una prestazione o a ricevere la consegna di una cosa determinata; in altri rappresenta uno o più beni reali sottostanti, ma il possessore non può esercitare sugli stessi alcuna facoltà; in altri ancora si ha una totale astrazione dall'economia tangibile, tale per cui l'*asset* è accettato e scambiato come valore in sé. Si è detto che nelle infrastrutture totalmente decentralizzate i *token* fungono da incentivo economico per coloro che partecipano al processo di validazione delle transazioni[49]. Per contro, nelle *blockchain* private o ibride esiste un titolare della rete (o amministratore di sistema) in capo al quale far gravare i rapporti giuridici derivanti dall'acquisto e dallo scambio di valori virtuali; questi ultimi potranno dunque rappresentare diritti e/o crediti da far valere nei suoi confronti.

Nel gergo tecnico si parla di "tokenizzazione" per indicare la procedura di incorporazione di una risorsa o un diritto in un *asset* informatico. Trattandosi, per dirlo altrimenti, di una sorta di "cartolarizzazione" dell'era digitale non sorprende che i *token*

[48] Si pensi ad esempio alle applicazioni della *blockchain* alla registrazione dei trasferimenti di proprietà, al tracciamento dei prodotti agricoli, alla gestione dei diritti di proprietà intellettuale, alle rimesse interbancarie etc.

[49] Trattandosi di sistemi privi di *governance* centralizzata l'informazione digitale non può rappresentare beni reali o crediti nei confronti dell'emittente, per il semplice fatto che manca un centro di imputazione dei rapporti giuridici attivi o passivi (soggetto titolare dei beni o obbligato alla prestazione).

abbiano un ambito di applicazione molto più vasto di quello delle valute virtuali, essendo fruibili per una molteplicità di utilizzi diversi da quello di pagamento[50].

Le statistiche sulla crescita del mercato dei *token* rendono ormai evidente come l'economia della *blockchain* abbia ormai raggiunto uno stadio di piena maturità[51]. Che la tokenizzazione rappresenti una delle nuove frontiere del mercato mobiliare è dimostrato dalla quantità di capitali raccolti mediante l'offerta al pubblico di valori virtuali (*Initial Coin Offering* e modelli derivati). La creazione di tali valori avviene in modo diverso in base alla tipologia di infrastruttura considerata: nelle *blockchain* pubbliche il meccanismo delle ricompense è alla base della creazione di nuovo valore; nelle reti private *permissioned*, siano esse parzialmente decentralizzate o centralizzate, la decisione sugli elementi essenziali dell'offerta di *token* (natura, tipologia e quantità) spetta solitamente al titolare del sistema[52].

In entrambi i casi l'informazione sarebbe del tutto inservibile, chiusa e autoreferenziale, se non vi fossero alcuni operatori in grado di creare una economia di scambio per l'acquisto e la vendita di *token* virtuali. La più grande debolezza dei sistemi *peer-to-peer* è notoriamente quella di non poter fare a meno di una sede d'incontro tra la domanda e l'offerta di utenti remoti. Considerando la *blockchain* per quello che è, ossia una infrastruttura tecnologica per fare scambi, ogni riflessione di natura economica non potrà che avere ad oggetto il mercato di capitali creatosi a valle dei sistemi DLT, che in più parti dell'opera indicheremo con la locuzione "mercato valutario virtuale".

La negoziazione dei valori permette di stabilire quanto gli operatori economici siano disposti a pagare per avere la disponibilità delle informazioni o per fruire dei servizi digitali. Per questo motivo gli intermediari del mercato (cambiavalute virtuali, gestori di sedi di negoziazione, fornitori di servizi di investimento in valuta virtuale) divengono una leva essenziale dell'economia della tokenizzazione, il vero fulcro del mercato valutario. Non è pertanto un caso che i primi interventi regolatori abbiano insistito proprio sulla disciplina dell'attività svolta da questi soggetti per tentare un recupero della centralizzazione in una dimensione economica che, almeno inizialmente, è stata concepita per disintermediare gli scambi tra privati.

---

[50] Il *token* è una informazione digitale preziosa poiché artificialmente scarsa, univocamente identificabile, non duplicabile e trasferibile all'interno di un sistema di registri distribuiti. Trattasi di una nozione che solo in parte riflette quella di "valuta virtuale", dalla quale si differenzia per l'assenza di una funzione necessariamente monetaria. Essi fungono più in generale da veicolo per la circolazione di diritti o da titolo di legittimazione a determinate prestazioni. Se il *token* impiegato è meramente rappresentativo di uno strumento di pagamento, sarà pienamente riconducibile allo statuto di disciplina delle valute virtuali previsto dal D.lgs. 21 dicembre 2007, n. 231 così come modificato dal D.lgs. 90/2017. Laddove invece il *token* impiegato sia rappresentativo di un qualsiasi altro diritto si porrà il problema del suo inquadramento nella categoria dei valori mobiliari ovvero degli strumenti finanziari, oppure tra i titoli di legittimazione (art. 2002) o promesse di pagamento (art. 1988 c.c.). *Amplius*, Cap. III, § 2.2. e Cap. IV, § 1.4.

[51] Dai dati pubblicati sul portale CoinDesk emerge che mediante ICO sono stati raccolti 256 milioni di dollari con 43 progetti nel 2016, 5 miliardi con 343 progetti nel 2017e 17 miliardi USD con 650 progetti nel 2018. Cfr. https://www.coindesk.com/ico-tracker

[52] *Amplius*, Cap. III, § 3.3.

3. Fondamenti giuridici della tecnologia a registro distribuito. Realtà e prospettive di regolazione del fenomeno.

La breve disamina dei profili tecnici ed economici della *blockchain* consente ora di rivolgere l'attenzione al tema che più interessa l'oggetto della presente trattazione: il superamento dei limiti imposti dal diritto pubblico. I connotati di decentralizzazione e di transnazionalità della DLT consentono di superare il modello di fruizione dei servizi mediante la presenza di un soggetto terzo che svolga il ruolo di erogatore o intermediario, consentendo un diretto collegamento tra gli utenti. Ciò che rende realmente rivoluzionaria la *blockchain* è dunque l'attitudine a rendere scarse risorse illimitate, creando fiducia nell'infrastruttura in sé o nel soggetto che la governa.

Osservando la diffusione dei valori virtuali con le lenti del giurista, affiorano numerosi interrogativi sul *se* e sul *come* il fenomeno debba essere regolato. È sufficiente rivolgere lo sguardo alle prime applicazioni in campo economico-finanziario per rendersi conto dei numerosi punti di tensione con normativa di settore che disciplina i servizi di pagamento e le attività di investimento, la raccolta del pubblico risparmio, la prevenzione del riciclaggio e del finanziamento del terrorismo, la tutela dei consumatori, la tassazione dei redditi di capitale e il monitoraggio fiscale. Le scelte di regolazione fino a questo momento intraprese sono il frutto di un cauto bilanciamento tra due contrapposte esigenze: da un lato contenere i rischi legati alla diffusione delle valute virtuali, dall'altro incentivare lo sfruttamento delle potenzialità offerte dalla tecnologia a registro distribuito.

Sul primo fronte si registra una diffusa tendenza dei regolatori ad includere nel perimetro del controllo statuale tutte le attività connesse all'utilizzo dei valori virtuali[53]. Dinanzi a un fenomeno di portata globale la creazione di una base normativa comune si rivela essenziale per evitare lo spiacevole fenomeno della concorrenza tra ordinamenti e impedire che le legislazioni più permissive divengano lo strumento per eludere il circuito dei controlli pubblici sui flussi transfrontalieri di capitali.

Sul versante opposto non potrebbe non darsi conto dell'esistenza di un certo *favor* legislativo per lo sviluppo di modelli di *business* basati su sistemi DLT. Basti pensare, per limitarci all'ordinamento nazionale, alla recente emanazione del c.d. Decreto crescita per la concessione di agevolazioni finanziarie dirette a sostenere la realizzazione di progetti di trasformazione tecnologica[54] , e alla precedente legge di conversione del Decreto semplificazioni che ha definito e riconosciuto valore legale alla *blockchain*.

[53] Nell'ordinamento nazionale basti pensare all'adozione del D. Lgs. 90/2017 e all'emanazione della Quinta Direttiva antiriciclaggio, contenenti disposizioni sulla prevenzione del riciclaggio e sull'esercizio dell'attività di cambiavalute virtuali (v. Cap. III, § 3.4). Numerosi sono anche gli esempi provenienti da altre giurisdizioni, tra cui USA, Canada, Giappone, Malta (V. Cap. IV, § 2.1. ss.)

[54] Decreto Legge 30 aprile 2019, n. 34 recante «Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi» (art. 29, comma 6).

3.1. La definizione legislativa di DLT nella legge di conversione del decreto semplificazioni.

La legge 11 febbraio 2019 n. 12 ha convertito con emendamenti il D.L. 14 dicembre 2018 n. 135 (c.d. Decreto Semplificazioni), inserendo un nuovo art. 8-*ter* rubricato «Tecnologie basate su registri distribuiti e *smart contract*». La norma ha seguito un *iter legis* decisamente insolito[55]: fu inizialmente introdotta, anche se con diversa formulazione, nello schema di decreto legge trasmesso al Consiglio dei Ministri, per poi essere espunta dal testo definitivo; venne dunque riproposta tra i numerosi emendamenti alla legge di conversione, e superando indenne lo stralcio effettuato a seguito dei moniti lanciati dal Presidente della Repubblica[56], è confluita nell'articolato finale della legge di conversione.

L'art. 8-*ter* esordisce con la seguente definizione di DLT *«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».*

Alla disposizione si deve il merito di aver finalmente positivizzato concetti di significativa importanza per la materia che ci occupa e di aver posto le basi per attribuire valore legale alle registrazioni di dati informatici in *blockchain*. Ciononostante, occorre dare atto di alcuni evidenti difetti redazionali che lasciano propendere per lettura estensiva della norma al fine di non frustrare le reali intenzioni del legislatore.

Il primo comma dell'art. 8-*ter* annovera la non alterabilità e l'immodificabilità dei dati tra gli elementi qualificanti la tecnologia a registro distribuito, senza alcuna ulteriore specificazione. Ciò rischia di produrre l'effetto paradossale di escludere dal perimetro classificatorio la stragrande maggioranza dei sistemi DLT, elevando a connotato essenziale una proprietà non declinabile in termini assoluti.

---

[55] Per approfondimenti v. D'AGOSTINO L., PISELLI R., *La definizione di tecnologia a registro distribuito e di smart contract nella legge di conversione del "Decreto semplificazioni". Un primo commento critico*, in NUZZO A. (a cura di), *Blockchain e autonomia privata. Fondamenti giuridici*, Roma, 2019, 15 ss.

[56] Dalla cronaca si apprende che il Governo avrebbe rinunciato a inserire il riconoscimento giuridico dei sistemi di DLT nel decreto legge perché, forse, troppo eccentrico rispetto all'oggetto della decretazione d'urgenza, circostanza che avrebbe spinto il Quirinale a suggerirne l'eliminazione. Come noto, l'esame in commissione della legge di conversione al Decreto semplificazioni è stato accompagnato da accese polemiche sulla natura *omnibus* del provvedimento e da denunce di presunta illegittimità costituzionale dell'inserimento di disposizioni non giustificate dai presupposti di necessità e urgenza. A quanto si apprende da fonti parlamentari, la decisione di dare un netto taglio agli emendamenti e alle integrazioni proposte sarebbe stata assunta a seguito della diffusione della notizia che la disomogeneità delle norme avrebbe potuto impedire la firma del Presidente della Repubblica.

Sebbene l'utilizzo della crittografia garantisca, in linea di principio, la non modificabilità delle informazioni, le regole sul consenso in *blockchain* ammettono – o quantomeno non escludono – la possibilità di intervenire sui dati registrati nella catena dei blocchi[57]. Se nelle reti pubbliche questa eventualità può sembrare remota o comunque difficilmente realizzabile, lo stesso non può dirsi per infrastrutture private a gestione centralizzata in cui vi è un soggetto che ha il controllo dell'intero sistema informatico.

Qualora ci si attenesse a stretto rigore alla definizione in commento si fornirebbe una *interpretatio abrogans* del dettato normativo. Appare pertanto preferibile ricorrere a un canone ermeneutico più elastico che valorizzi le reali intenzioni del legislatore, considerando la non modificabilità un requisito non assoluto, ma soltanto relativo.

3.2. *Smart contract*, efficacia probatoria e validazione temporale dei documenti registrati in *blockchain*.

Il secondo comma dell'art. 8-*ter* introduce la nozione di *smart contract* quale «*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*». La definizione valorizza il solo aspetto "esteriore" dell'esecuzione di un programma in *blockchain*[58] senza considerare l'aspetto più innovativo dato dalla traduzione in codice della volontà dei contraenti e dalla totale automazione della fase esecutiva del contratto.

Leggendo con la dovuta attenzione le parole del legislatore, sembra che ciascuna delle parti sia vincolata soltanto al momento dell'esecuzione del programma, e non fin da quello dell'attivazione dello *smart contract*[59]. Se così fosse, si avrebbe una curiosa discrasia temporale tra il momento in cui le parti esprimono la propria volontà negoziale – mediante l'invio di *token* o con altre modalità di "attivazione" dell'agente *software* – e quello in cui sorge un vincolo giuridico per effetto della verificazione di condizioni. In realtà, le problematiche maggiori sorgono proprio in conseguenza dell'adesione al regolamento contrattuale codificato che spoglia le parti del potere di adempiere alla prestazione. Tale circostanza solleva questioni di non poco conto anche

[57] Il protocollo alla base del funzionamento dell'infrastruttura detta le regole di *governance* (c.d. meccanismi del consenso), a cui i nodi della rete devono necessariamente attenersi. In tal senso, la maggioranza (o un numero qualificato di partecipanti, in misura ponderata rispetto alla quantità di *token* detenuta o alla potenza di calcolo che esprimono) potrebbero teoricamente deliberare una modifica dei dati registrati sulla *blockchain*.

[58] Sembra che il legislatore abbia condiviso la tesi dello *smart contract* come "contractware", cioè uno strumento per fornire agli elaboratori termini e clausole di un accordo e in grado di garantire l'adempimento dell'obbligazione. Cfr. RASKIN M., *The Law and Legality of Smart Contracts*, in *Georgetown Law & Tech Review*, 2017, 1, 311.

[59] Volendo descrivere in estrema sintesi il funzionamento di questi agenti-*software*, basterà ricordare che al verificarsi di certe condizioni, predeterminate dal programmatore e "attivate" dalle parti, l'algoritmo darà esecuzione al contratto, eseguendo in modo automatico la prestazione in esso dedotta (*amplius* v. Cap II., § 3 ss.).

per l'accertamento del dolo penalistico, che dovrà retroagire al momento della conclusione del contratto, stante l'impossibilità per la parte obbligata di recuperare il controllo sulla fase esecutiva[60].

Il secondo periodo della disposizione prevede che gli *smart contract* soddisfino il requisito della forma scritta *«previa identificazione informatica delle parti interessate»*, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia Digitale (AgID) con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge.

La norma non chiarisce se la forma scritta a cui fa riferimento debba intendersi *ad substantiam* o soltanto ai fini dell'efficacia probatoria. Il richiamo alla previa identificazione dei sottoscrittori è un indice rivelatore della volontà legislativa di saldare il contenuto della definizione alle regole dettate dal Codice dell'Amministrazione Digitale sull'efficacia probatoria dei documenti informatici validati digitalmente[61]. Non pare tuttavia doversi escludere l'efficacia probatoria del contratto *smart* che non si sia adeguato allo standard, laddove consenta in diverso modo di identificare la parte contro cui è prodotto[62].

La novella attribuisce infine rilevanza alla memorizzazione di un documento informatico su un registro distribuito, estendendo ad essa gli *«effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014»*, qualora siano parimenti conformi agli standard tecnici individuati dall'AgID. La materia è oggi disciplinata dal Regolamento 910/2014/UE che, in un'ottica di armonizzazione delle legislazioni nazionali, individua i requisiti e gli effetti giuridici della validazione temporale elettronica[63].

---

[60] Si affronterà in particolare il tema della responsabilità a titolo di bancarotta preferenziale per pagamenti effettuati tramite *smart contract* (v. Cap. II, § 3.1.).

[61] Più precisamente il requisito della forma scritta indicata nell'art. 8-*ter* in commento potrebbe essere inteso come "medesima efficacia probatoria della scrittura privata ai sensi dell'art. 2702 c.c.". Delle diverse tipologie di firma digitale che possono soddisfare i vincoli di forma indicate dal Codice dell'amministrazione digitale (D. Lgs. n. 82/2005), la tecnologia *blockchain* sembrerebbe basarsi sull'impiego della firma digitale di cui all'art. 1, lett. *s),* CAD, vale a dire un «*particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico*».

[62] La lettera della legge non reca alcuna indicazione di segno contrario né alcun elemento testuale da cui dedurre l'attribuzione in via esclusiva all'AgID del "monopolio" sulla efficacia probatoria del contratto. Essa individua soltanto una delle possibili modalità con cui i contraenti possono stipulare un accordo in linguaggio computazionale che soddisfi il requisito della forma scritta *ex* art. 2702 c.c. In argomento, D'AGOSTINO- PISELLI, *La definizione di tecnologia a registro distribuito e di smart contract*, cit., 18

[63] Il Codice dell'Amministrazione Digitale definiva la validazione temporale come «*il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi*». Oggi il Regolamento 910/2014/UE prevede che ad essa «*non possano essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali».* Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora, e di integrità dei dati ai quali tale data e ora sono associate. A tal fine è necessario che il dispositivo o la procedura informatica assicurino il rispetto di alcuni requisiti tra cui l'apposizione mediante firma elettronica avanzata con un sigillo elettronico avanzato del prestatore di servizi fiduciari (artt. 41 ss.).

4. La "poliforme" natura giuridica dei valori virtuali e le nuove frontiere della criminalità economica.

Il dualismo tra funzione monetaria e speculativa dei valori scambiati in *blockchain* pone un "dubbio amletico" sull'inquadramento giuridico del fenomeno[64]. La natura dei valori virtuali rimane tuttora avvolta da dubbi e incertezze, da cui promanano interrogativi di non poco conto sull'assoggettamento alle disposizioni di settore che regolano i servizi di pagamento, l'intermediazione finanziaria, o le attività di natura diversa. La questione assume una notevole importanza pratica al fine di individuare la disciplina sostanziale applicabile e i profili di responsabilità connessi al superamento dei limiti imposti dalla regolazione settoriale.

Non essendo chiaramente possibile stabilire in astratto se la funzione monetaria sia prevalente o recessiva rispetto a quella finanziaria, si dovrà necessariamente considerare la *ratio* di ciascun istituto e i principi che regolano le singole materie[65]. In tal modo, anche l'ambito di rilevanza penale di determinate condotte dipenderà dalla previa qualificazione giuridica dei valori virtuali.

Le tecnologie e i protocolli basati su registri distribuiti creano dunque l'apparenza di un ordinamento autonomo nello spazio virtuale basato sulla fiducia nei sistemi informatici e nella valorizzazione delle informazioni digitali. Le applicazioni della *blockchain* in ambito finanziario, inizialmente concepite come una "via di fuga" dai rigidi schemi del sistema bancario, rappresentano un polo di attrazione per ingenti quantità di capitali. Questa inedita forma di "capitalismo digitale" apre nuovi orizzonti alla criminalità economica, alimentando la già di per sé spiccata tendenza alla commissione di reati informatici.

I valori virtuali saranno dapprima considerati dalla prospettiva del loro utilizzo come mezzo di pagamento e di circolazione della ricchezza, che rivela straordinarie potenzialità di sfruttamento per finalità illecite. Successivamente si rivolgerà l'attenzione al loro impiego in funzione speculativa che solleva criticità di non poco conto per la tutela del mercato finanziario e dell'interesse patrimoniale degli investitori.

[64] Nonostante il legislatore abbia preso in considerazione la sola natura monetaria delle valute virtuali, omettendo di considerare la possibilità di un impiego per finalità speculative, la tendenza deflazionistica della criptomoneta rende l'opera classificatoria estremamente complessa per via dell'elevata propensione degli attori economici ad acquistarla e scambiarla per finalità meramente speculative.
[65] *Amplius,* Cap III § 1; Cap. IV, § 1.

CAPITOLO II

AZIONE, OMISSIONE ED EVENTO IN *BLOCKCHAIN*.

SOMMARIO: 1. Rilievi introduttivi. La potenzialità criminogene della tecnologia a registro distribuito. – 1.1. Le caratteristiche del cyberspazio e la commissione di reati *online*. – 1.2. Transnazionalità degli illeciti e garanzia dell'anonimato. Le ragioni dell'utilizzo delle applicazioni economico-finanziarie della *blockchain* per propositi criminosi. – 1.3. Cybercriminalità economica e desensibilizzazione soggettiva. – 2. La tecnologia a registro distribuito e il diritto penale nel cyberspazio. – 2.1. Azione ed evento nel diritto penale dell'informatica. – 2.2. Azione ed evento in *blockchain*. – 2.3. Omessa convalida, regole del consenso e caducazione del blocco. – 3. *Smart contract* e agenti *software* autonomi. Considerazioni sul rapporto di autoria tra transazione illecita e operatore economico. – 3.1. Esecuzione automatica del contratto e responsabilità penale. – 3.2. Azione automatica del *software* e condotta penalmente rilevante. Un quadro di sintesi. – 3.3. *Criminal smart contract* e *dual use software*. – 4. L'evento in *blockchain* (rinvio) – 5. Registri distribuiti e *locus commissi delicti*. – 5.1. Principio di territorialità, reati informatici e luogo di commissione del reato – 5.1.1. Il punto delle Sezioni Unite sul luogo di commissione dell'accesso abusivo a sistema informatico. – 5.1.2. Rilievi critici. Le questioni irrisolte sul luogo di commissione del reato informatico. – 5.2. L'ubiquità nell'infrastruttura. Problematiche relative all'individuazione del luogo di commissione del reato in *blockchain*. – 5.3. Registri distribuiti e disciplina della continuazione *ex* art. 81 c.p. – 5.4. Registri distribuiti e *tempus commissi delicti*. – 5.5. *Locus commissi delicti* e natura ubiquitaria dell'infrastruttura. Alcune considerazioni conclusive. – 6. Obblighi di controllo e omesso impedimento di reati. La posizione di garanzia in *blockchain*. – 6.1. La causalità omissiva e la posizione di garanzia nel diritto penale. – 6.1.1. Le fonti dell'obbligo giuridico impeditivo. Sintesi dello stato dell'arte. – 6.1.2. Obbligo di garanzia e teoria del rischio. Cenni. – 6.2. *Internet Service Provider* e libertà nella rete – 6.2.1. I modelli di responsabilità dell'ISP – 6.2.2. In particolare: la responsabilità *per omissionem*. – 6.3. *Blockchain* private e ibride. – 6.3.1. *Blockchain permissioned* e titolarità del sistema. – 6.3.2. *Blockchain permissioned* e posizione di garanzia. – 6.4. Organizzazioni autonome decentralizzate, *governance* interna, e controlli societari. Alcuni spunti di riflessione. – 6.5. *Blockchain* pubbliche. Alla ricerca di un garante? – 6.6. La responsabilità dell'*exchange* e del *wallet provider* a titolo di concorso omissivo in riciclaggio. – 7. Considerazioni finali e prospettive *de lege ferenda*. – 7.1. Una proposta per l'introduzione di una fattispecie di reato propria del *provider*. – 8. Azione, omissione ed evento in *blockchain*. Un quadro di sintesi.

1. Rilievi introduttivi. La potenzialità criminogene della tecnologia a registro distribuito.

La tecnologia a registro distribuito rende possibile la creazione di una rete decentralizzata di elaboratori interconnessi, in grado di eseguire una molteplicità di funzioni e di programmi grazie all'opera prestata dai singoli nodi che la costituiscono.

La reale novità di questa tecnologia è nell'utilizzo di avanzati algoritmi crittografici per ordinare, in modo sicuro e tendenzialmente immodificabile, il libro mastro pubblico

(*ledger*) detenuto simultaneamente da ciascun partecipante alla rete. Come si è avuto modo di evidenziare[1] la *blockchain* pubblica è il sistema di delocalizzazione delle risorse informatiche per eccellenza: chiunque intenda servirsene – per effettuare transazioni, registrare documenti, o compiere qualsiasi altra attività giuridica – può contare sull'efficienza e sulla continuità operativa del sistema. Il meccanismo delle ricompense (*proof of work, proof of stake, proof of authority*), la libertà di accesso e di recesso e la distribuzione geografica dei nodi sono fattori che garantiscono la stabilità dell'infrastruttura e accrescono la fiducia nel sistema in sé.

Diversamente dal protocollo di comunicazione tradizionale (c.d. modello *client-server*), basato sulla connessione remota a un *database* unico di informazioni, i registri distribuiti sono immuni alle vulnerabilità che derivano dall'accentramento delle informazioni. Tra i difetti principali del modello *client-server* vi è la soggezione degli utenti alla volontà del titolare del sistema che – *ad nutum* o per ordine dell'Autorità – potrebbe impedire l'accesso ai contenuti o rendere definitivamente inservibili i dati archiviati. A simili conseguenze si addiverrebbe anche nell'ipotesi in cui il *server* sia bersagliato da un attacco informatico idoneo ad impedirne il funzionamento o a danneggiare il sistema o i dati informatici.

La decentralizzazione delle informazioni e la tenuta di una copia identica del registro da parte dei singoli nodi fa venir meno la figura del titolare del sistema e, con essa, la possibilità di individuare un "controllore" della rete e un destinatario dei provvedimenti dell'Autorità. Se da un lato ciò rappresenta un fattore di garanzia per gli utenti – che possono davvero contare in una *net neutrality*, al riparo da ingerenze dei *provider* del servizio – dall'altro costituisce un fattore di rischio, incrementando la già di per sé spiccata tendenza alla commissione di reati *online*. La disintermediazione negli scambi e l'assenza di una autorità centrale radicano nei criminali informatici la convinzione che le condotte illecite commesse mediante la tecnologia a registro distribuito possano più facilmente rimanere impunite. Qualora il fatto di reato consista in una transazione *peer to peer*, gli organi investigativi vedono sottratta ogni possibilità di acquisire la *notitia criminis* o le evidenze informatiche dai fornitori del servizio (*provider*). Chi agisce può inoltre contare sullo schermo dell'anonimato (o pseudo anonimato) garantito dall'utilizzo di una piattaforma *blockchain* in cui le attività compiute vengono registrate sotto forma di indirizzi alfanumerici non nominativi, dai quali è impossibile risalire all'identità dell'autore.

A tal riguardo, è opportuno precisare fin da ora che a destare maggiore preoccupazione sono le applicazioni della tecnologia a registro distribuito nel settore economico-finanziario. La diffusione delle valute virtuali e l'affermazione della criptomoneta come bene economicamente valutabile ha aperto nuovi orizzonti al fenomeno del riciclaggio e del finanziamento del terrorismo, spianato la strada alla compravendita di beni illegali sul *dark web*, incentivato nuove forme di evasione fiscale. È questa la ragione per cui riteniamo di assoluta importanza un

[1] *Supra*, Cap. I, § 2

approfondimento del tema dalla prospettiva del diritto penale. La trattazione avrà dunque ad oggetto, con le precisazioni che dappresso seguiranno, l'utilizzo della DLT per la commissione di reati connotati da un movente di lucro soggettivo o, comunque, da una marcata componente patrimonialistica. Le ipotesi di reato riconducibili alla sfera della criminalità economica sono quelle che per prime hanno suscitato l'interesse della dottrina[2], che, prontamente, ha evidenziato le straordinarie potenzialità criminogene della moneta *peer to peer*[3]. Prima di entrare nel merito delle numerose questioni che si prospettano all'attenzione del penalista, si dovranno anzitutto indagare le cause dell'impiego sistematico dei valori virtuali per finalità illecite.

1.1. Le caratteristiche del cyberspazio e la commissione di reati *online.*

Le tecnologie e i protocolli basati su registri distribuiti creano una sorta di "ordinamento" nello spazio virtuale: una infrastruttura alla quale gli utenti possono accedere liberamente oppure a determinate condizioni per compiere diverse attività giuridicamente rilevanti[4]. La tendenziale "autonomia" di cui gode ciascun sistema *blockchain* rispetto alla rete Internet nel suo complesso non vale tuttavia ad escludere la presenza di caratteristiche comuni, riconducibili alla dimensione totalmente virtuale delle relazioni interpersonali. La dottrina penalistica[5] ha ormai da tempo messo in luce come l'assenza di autorità nella rete e l'impossibilità di individuare confini spaziali definiti costituiscano un incentivo notevole alla realizzazione di reati *online*: una vera

[2] Sul tema ACCINNI G.P., *Profili di rilevanza penale delle "criptovalute*", in *Arch. Pen*., 2018, 1, 2 ss.; LUCEV R., BONCOMPAGNI F., *Criptovalute e profili di rischio penale nella attività degli exchanger*, in *Giurisprudenza penale web*, 2018, 3, 3 ss.; DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, in *Dir. pen cont. – Riv. trim*, 2018, 9, 87; FERRARI E., *Bitcoin e criptovalute: la moneta virtuale tra fisco ed antiriciclaggio,* in *Il Fisco*, 9, 2018; GALMARINI S., *Monete virtuali e antiriciclaggio: terreni dai confini incerti*, *www.dirittobancario.it*, 11 ottobre 2018; STURZO L., *Bitcoin e riciclaggio 2.0*, Dir. Pen. Cont., 5, 2018. Sia altresì consentito rinviare a 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*, 2018, 1, 3 ss.

[3] In argomento, SEVERINO P., *Sicurezza informatica e prevenzione del cybercrime*, in *LuissOpen*, 8 settembre 2017, 11, 6; PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ*., 2018, 3-4, 596 ss.

[4] Alcuni autori hanno parlato di recente del sistema *blockchain* inteso quale "istituzione". Una tale chiave di lettura, che ricorda la teoria formulata da Santi Romano (OLIVARI A., *Santi Romano ontologo del diritto*, Milano, 2016, 103 che richiama ROMANO S., *L'ordinamento giuridico*, Firenze, 1917), non è del tutto nuova nel campo del diritto della comunicazione e dell'informazione, in cui una parte della dottrina sostiene una originale interpretazione dell'algoritmo come "istituzione". Cfr. NAPOLI P., *The Algorithm as Institution: Toward a Theoretical framework for automated Media Production and Consumption*, Paper presented at the Media in Transition Conference, Massachusetts Institute of Technology, 2013, Cambridge, in https://papers.ssrn.com.

[5] In argomento, In argomento, PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 39 ss.; ID., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 26; FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc.*, 2015, 10, 1296.

e propria "terra di mezzo" della criminalità[6], uno *wild west*[7] in cui tutto ciò che è tecnicamente possibile diviene di fatto giuridicamente lecito[8].

La spinta criminogena maggiore è data dalla possibilità di preservare l'anonimato, da cui deriva la convinzione – per molti versi fondata – che l'azione sulla rete è difficilmente "giustiziabile"[9], a causa delle evidenti difficoltà nell'individuazione del responsabile. A ciò si aggiunga che i criminali agiscono spesso da Stati tecnologicamente arretrati, sfruttando a loro vantaggio l'assenza di reparti specializzati e di strumenti investigativi efficaci a disposizione delle autorità locali.

Date queste premesse, è possibile cogliere una perfetta simmetria tra le caratteristiche dello spazio virtuale e i connotati tipici della criminalità informatica: dall'assenza di confini spaziali in Internet deriva la dimensione transnazionale del *cybercrime*, dall'anonimato degli utenti la tendenza alla desensibilizzazione soggettiva, dall'assenza di autorità di vigilanza la maggiore propensione all'utilizzo per finalità illecite. Sono queste le ragioni per cui, tanto in sede internazionale[10] quanto a livello

---

[6] SEVERINO, *Sicurezza informatica e prevenzione del cybercrime*, cit., 12.

[7] L'espressione è di FLOR, *I limiti del principio di territorialità nel cyberspace*, cit., 1296

[8] Secondo alcuni autorevoli studiosi la difficoltà di regolazione della rete segnerebbe il passaggio dalla *rule of law* alla *rule of code:* in Internet è consentito tutto ciò che è tecnicamente possibile. Se si volesse impedire un utilizzo per scopi criminosi si dovrebbe trovare l'espediente tecnico più efficace, anziché concentrarsi sullo stigma penale di determinate condotte. «*And finally code regulates behavior in cyberspace. The code, or the software and hardware that makes cyberspace as it is, constitutes a set of constraints on how one can behave. The substance of these constraints may vary, but they are all experienced as conditions on one's access to cyberspace, he code or software or architecture or protocols set these features; they are features selected by code writers; they constrain some behavior by making other behavior possible, or impossible. They imbed certain values, or they make certain values impossible. In this sense, they too are regulations, just as the architectures of real space code are regulations*» (LESSIG L., *The Law of the Horse. What Cyberlaw Might Teach*, in *Harvard Law Review*, 1999, 4).

[9] Il problema della effettiva "giustiziabilità" dei reati informatici ha portato la dottrina a suggerire un mutamento di prospettiva nella lotta al fenomeno, valorizzando il momento della prevenzione nell'ottica del superamento di un intervento del legislatore in chiave meramente repressiva. Cfr. SEVERINO, *Sicurezza informatica e prevenzione del cybercrime*, cit., 10; D'AGOSTINO L., *Cybersecurity, (auto)regolazione e governance del rischio. Quid de iure poenali*?, in *Luiss Law Review*, 2017, 1, 129 ss.

[10] La dimensione transnazionale del *cybercrime* ha incentivato forme di cooperazione spontanea tra Stati e l'adozione di importanti accordi internazionali, ai quali va riconosciuto il merito dell'evoluzione normativa del sistema penale italiano. Fu in particolare il Consiglio d'Europa con Raccomandazione del 1989 a focalizzare l'attenzione sulla necessità di contrastare, su basi comuni, alcuni "tradizionali" *computer crimes*. All'epoca l'ordinamento italiano era sfornito di fattispecie sanzionatorie *ad hoc*, anzi soltanto alcuni sporadici interventi avevano interessato, in maniera più o meno diretta, la criminalità informatica. Soltanto con la legge 23 dicembre 1993 n. 547 il legislatore nazionale ha tentato di "mettere a sistema" i reati informatici, sulla falsariga delle indicazioni del Consiglio d'Europa. Un decisivo passo avanti nell'attività di contrasto del computer crime è stato compiuto nel 2001 con la stipula della Convenzione di Budapest sul *cybercrime*. Essa rappresenta il primo accordo internazionale vincolante in materia ed ha il dichiarato obiettivo di realizzare una politica comune fra gli stati membri mediante la criminalizzazione di determinate condotte e l'apertura di canali di comunicazione tra le autorità investigative degli Stati firmatari. Sebbene l'ordinamento italiano fosse già per larga parte conforme alle disposizioni pattizie, la legge di ratifica della Convenzione (Legge 18 marzo 2008, n. 48), rinnovò profondamente il sistema prevedendo per i reati informatici la responsabilità dell'ente ex D. Lgs.231/2001 (art. 24-*bis*) e interpolando molte disposizioni procedurali sulla competenza, sui poteri dell'Autorità nella repressione dei crimini informatici e sulle modalità di conservazione della prova

dell'Unione Europea[11], si è avvertita la pressante esigenza di una armonizzazione delle legislazioni nazionali di contrasto alla criminalità informatica. La fissazione di uno standard comune nella definizione degli illeciti assicura una base normativa comune per l'attivazione delle misure di cooperazione giudiziaria e di coordinamento investigativo, risolvendo in *limine* il problema della doppia incriminazione[12].

1.2. Transnazionalità degli illeciti e garanzia dell'anonimato. Le ragioni dell'utilizzo delle applicazioni economico-finanziarie della *blockchain* per propositi criminosi.

La descritta morfologia della criminalità informatica aiuta a comprendere le ragioni per cui, fin dalla sua prima apparizione, la tecnologia a registro distribuito sia stata utilizzata per finalità illecite. L'attenzione andrà rivolta, in particolare, alle applicazioni economico-finanziarie della *blockchain*, non potendosi in alcun modo dubitare della

informatica. Per approfondimenti, PECORELLA C., voce *Reati informatici*, in *Enciclopedia del Diritto*, ann. X, Milano, 2017, 707 ss.; ID., *Diritto penale dell'informatica,* Padova, 2006, 7 ss.; PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa – Profili sostanziali*, in *Dir. pen. proc.*, 2008, 6, 700 ss.; SARZANA DI S. IPPOLITO C., *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. proc*, 2008, 12, 1562 ss.

[11] Nell'ambito del c.d. terzo pilastro della Comunità Europea era stata adottata la Decisione Quadro 2005/222/GAI, con il deliberato intento «di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione» (considerando n. 1). Con essa si gettarono le basi per uno standard minimo di criminalizzazione in materia di criminalità informatica. Successivamente, abolita la struttura a pilastri con il Trattato di Lisbona, il referente normativo fondamentale della materia è divenuto l'art. 83 del TFUE che consente oggi di stabilire, mediante direttive adottate secondo la procedura legislativa ordinaria, *minimum rules* in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale, fra le quali rientra, appunto, la criminalità informatica.
Da ultimo la Direttiva 2013/40/UE ha modificato e ampliato le disposizioni contenute nella decisione quadro 2005/222/GAI, stabilendo norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione, con l'obiettivo di facilitare la prevenzione di tali reati e migliorare la cooperazione fra autorità giudiziarie e altre autorità competenti, compresi la polizia e i servizi degli Stati membri incaricati dell'applicazione della legge, nonché le competenti agenzie e gli organismi specializzati dell'Unione, come Eurojust, Europol e l'Agenzia per la sicurezza delle reti e dell'informazione (ENISA). La Direttiva, mantenendo ferme la maggior parte delle disposizioni contenute nella decisione quadro 2005/222/GAI, detta alcune norme integrative rispetto alla Convenzione di Budapest, che riconosce come *framework* fondamentale di lotta contro la criminalità informatica. In dottrina, v. PICOTTI L., *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec*., 2011, 4, 827 ss.; SEVERINO, *Sicurezza informatica e prevenzione del cybercrime*, cit., 13.

[12] L'armonizzazione delle legislazioni nazionali di contrasto al *cybercrime* risulta assolutamente necessaria anche al fine di contrastare lo spiacevole fenomeno del *forum shopping*. L'esistenza di asimmetrie nella repressione di determinate condotte potrebbe infatti indurre i criminali informatici ad agire da Paesi in cui il fatto sia privo di rilevanza penale, circostanza che osterebbe, nella maggior parte dei casi, all'esecuzione di una richiesta di estradizione o più semplicemente di un ordine indagine a carico dei responsabili.

dimensione assolutamente preponderante dell'impiego di quest'ultima quale strumento di scambio di valori virtuali[13].

Guardando al fenomeno della moneta *peer to peer*, ci si rende subito conto come essa sia uno strumento quasi perfetto nelle mani dei criminali informatici. Se nell'universo virtuale essi già godono della possibilità di agire dietro l'egida dell'anonimato[14], la creazione della criptomoneta ha offerto un mezzo ancora più sicuro per il compimento di transazioni illecite e la ricezione di valori, beni, e altre utilità provenienti da delitto. Le valute virtuali assommano in sé le caratteristiche del cyberspazio: garantiscono l'anonimato, possono essere inviate in pochi secondo in ogni parte del mondo, il loro flusso sfugge al controllo di una autorità centrale.

Un recente rapporto dell'*European Cybercrime Center* (EC3) costituito presso Europol ha evidenziato un rapporto di diretta proporzionalità tra l'aumento di capitalizzazione del mercato delle criptovalute e lo sviluppo del *cybercrime*, specialmente con riferimento alle condotte di diffusione di *ransomwares* e al dilagare sulla parte oscura della rete di *criminal markets*[15] per la compravendita di droga, armi, materiale pedopornografico. La dottrina[16] ha inoltre evidenziato come la diffusione delle criptovalute abbia aperto nuove frontiere per il *cyberlaundering*, costringendo i regolatori a un rapido adeguamento delle normative di contrasto al riciclaggio[17]. L'affermazione di una moneta del cyberspazio – disintermediata, anonima e affidabile – ha fatto venir meno il deterrente principale alla commissione di reati economici in rete, vale a dire il necessario passaggio per i circuiti di pagamento tradizionali e per la dimensione reale dell'economia, sottoposta al controllo dell'autorità e dominata dalla presenza di vincoli a carico degli operatori di settore[18]. Sebbene la maggioranza dei protocolli basati su registri distribuiti consentano una perfetta tracciabilità dei flussi, le

[13] La limitazione del campo d'indagine non deve tuttavia far ritenere che questa nuova tecnologia non sia compatibile con la commissione di reati estranei alla dimensione economica. Per il tramite della *distributed ledger technology* è possibile realizzare qualsiasi reato informatico in senso lato; si pensi, ad esempio, alla condivisione di notizie su una infrastruttura che, tramite un sistema di *rating* decentralizzato, indicizzi le notizie giornalistiche per distinguerle dalle *fake news*. In un sistema di questo tipo si potrebbero diffondere, aumentandone la visibilità, anche notizie di cui sia vietata la divulgazione (artt. 261, 262, 621 c.p.). Sulla distinzione tra reati informatici in senso stretto e in senso lato, PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 75; FLOR R., *Cyber-criminality: Finding a Balance between Freedom and Security*, nella raccolta di scritti del convegno *Cybercrime: Global Phenomenon and its Challenges*, tenutosi a Courmayeur il 2-4 dicembre 2011, pubblicata sul sito International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC), 13 ss.

[14] Di recente sul tema dell'anonimato nell'utilizzo delle valute virtuali si veda PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2018, 3-4, 596 ss.

[15] *Internet Organised Crime Threat Assessment* (IOCTA) per l'anno 2017, in https://europol.europa.eu, 60 ss.

[16] Sul tema v. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta*, cit., 2; DI VIZIO, *Le cinte daziarie del diritto penale*, cit. 92.

[17] Sulla disciplina preventiva e sanzionatoria del riciclaggio in forma digitale, con specifico riferimento alle operazioni compiute mediate valori virtuali, si rinvia al prosieguo della trattazione (*infra*, Cap. III § 3 ss.).

[18] Ci si riferisce agli obblighi di identificazione e profilazione della clientela, di segnalazione delle operazioni sospette (cfr. artt. 10 ss. Direttiva 2015/849/UE; artt. 15 ss. D. Lgs. 231/2007) e, in genere, di prevenzione di reati commessi nell'interesse o a vantaggio dell'ente (art. 24 ss. D. Lgs. 231/2001).

moderne tecniche investigative non permettono di risalire dall'indirizzo di una transazione all'autore della stessa[19]. La crittografia e la disintermediazione divengono così un salvacondotto a cui i criminali, verosimilmente, faranno sempre più spesso riferimento[20].

Per opporre un ostacolo all'impiego sistematico dei valori virtuali per finalità illecite, si dovrebbe recuperare un controllo statuale sull'economia virtuale. L'unica strada percorribile in questa direzione conduce alla responsabilizzazione degli operatori che professionalmente operano sul mercato valutario. L'attività svolta da questi soggetti permette la conservazione e la spendita di asset virtuali, favorisce l'incontro tra la domanda e l'offerta, assicura la bidirezionalità del flusso della criptomoneta. Essi operano, in buona sostanza, come "intermediari di una economia disintermediata" offrendo una vasta gamma di servizi per la fruizione, l'acquisto e la conversione dei valori virtuali. L'importante ruolo svolto da questi soggetti non è sfuggito all'attenzione del legislatore italiano e di quello sovranazionale che, con provvedimenti di recente emanazione, hanno esteso a costoro gli obblighi previsti dalla normativa antiriciclaggio[21].

1.3. Cybercriminalità economica e desensibilizzazione soggettiva.

La moneta virtuale possiede dunque delle proprietà tali da favorirne l'utilizzo, su scala globale, in operazioni economiche di natura illecita. Volendo esaminare fino in fondo le ragioni della sua natura criminogena, non potremmo non considerare l'elemento della totale virtualizzazione degli *asset* e delle procedure di acquisizione, conservazione e spendita. Tale elemento induce, sul piano prettamente criminologico, alla desensibilizzazione degli utilizzatori delle valute virtuali i quali non avvertono (o avvertono in misura decisamente ridotta) il disvalore dell'azione criminosa che compiono. L'utilizzo di risorse totalmente informatizzate fa venir meno il contatto con il contante, ingenerando la convinzione per cui l'azione antigiuridica sia meno grave rispetto alla corrispondente azione commessa nei modi ordinari.

[19] Come sarà chiarito in sede più opportuna (*infra*, Cap. V, § 5), le tecniche di *blockchain forensics* si basano sulla aggregazione di indirizzi e sulla raccolta di informazioni *open source*. Dette tecniche potrebbero rivelarsi in molti casi inidonee all'individuazione degli autori di una transazione illecita.
[20] PICOTTI, *Profili penali del cyberlaundering*, cit., 615 il quale sottolinea la necessità di un adeguamento degli strumenti di prevenzione e contrasto per reprimere l'utilizzo delle valute virtuali per propositi illeciti.
[21] *Amplius*, § Cap. III, § 3.2.

Quello della desensibilizzazione[22] è un tema tutt'altro che nuovo nel dibattito politico[23]. Esso è stato affrontato in relazione al tema della diffamazione telematica, per descrivere la diffusa tendenza all'utilizzo non responsabile dei *social media*, attraverso i quali vengono talvolta espresse opinioni eccedenti i limiti della continenza espositiva e del diritto di critica[24].

Di recente la dottrina[25] ha rimarcato come la predetta tendenza sia comune a tutti gli illeciti commessi mediante strumenti informatici, che si caratterizzano proprio *«per la ridotta percezione dell'offesa e per le minori remore morali connesse all'assenza di un contatto "fisico" tra il colpevole e la vittima»*, che si uniscono alla *«diffusa consapevolezza da parte degli autori delle obiettive difficoltà di essere identificati»*[26].

Tale tesi, sicuramente condivisibile, permette di comprendere appieno le ragioni per cui alcuni fenomeni criminosi – quali ad esempio il riciclaggio digitale c.d. integrale – abbiano avuto una diffusione così capillare, arrivando a coinvolgere anche soggetti incensurati e del tutto insospettabili. L'utilizzo della criptomoneta ha permesso ai gruppi criminali di assoldare facilmente *money mules* – utenti talvolta ben consapevoli della provenienza delittuosa del denaro – ai quali viene richiesto di detenere i valori virtuali per un periodo di tempo e di trasferirli poi verso uno o più indirizzi di destinazione. Trattandosi di attività apparentemente innocue, semplici da eseguire e ben remunerate, si produce un effetto desensibilizzante su larga scala, tale da indurre l'utente medio a prendere parte all'operazione anche in presenza di un evidente *fumus* di illiceità.

La perdita di contatto con la realtà comporta un drastico abbassamento della soglia di percezione del disvalore di azione, ampliando in modo significativo la schiera dei possibili concorrenti nel reato. Non è dunque un caso che la figura tipica del cybercriminale assuma connotati peculiari, profondamente differenti dagli altri stereotipi criminologici[27].

---

[22] La desensibilizzazione può assumere due forme. La *desensibilizzazione soggettiva* si riferisce alla percezione che ha il reo della propria condotta, avvertita di minor disvalore sociale poiché intermediata dallo schermo. La *desensibilizzazione oggettiva* fa riferimento al livello di credibilità o di gravità delle offese, che dipende dal contesto in cui è commesso il fatto. In tal senso la commissione di un reato *online* sarebbe per ciò solo meno grave, poiché è risaputo come Internet sia un luogo privo di regole e di controlli.

[23] Si veda il resoconto stenografico della seduta del 26 novembre 2014 disponibile su https://camera.it, relativo all'indagine conoscitiva della Camera dei Deputati in merito all'esame della proposta di legge AC-925-B.

[24] Resoconto stenografico della seduta del 26 novembre 2014, audizione di Nello Rossi, procuratore aggiunto presso il Tribunale di Roma, coordinatore del Gruppo di lavoro criminalità informatica, cit., 10 ss.

[25] Sulla desensibilizzazione soggettiva come nota caratterizzante della criminalità informatica, v. in genale PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, IN CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 39 ss.

[26] SEVERINO, *Sicurezza informatica e prevenzione del cybercrime*, cit., 11

[27] La questione sarà approfondita nel paragrafo successivo, allorché ci occuperemo dei diversi profili di criminali coinvolti nei traffici illeciti di valori virtuali-

2. La tecnologia a registro distribuito e il diritto penale nel cyberspazio.

Una trattazione che avesse ad oggetto unicamente i diversi titoli di responsabilità penale connessi all'utilizzo della tecnologia a registro distribuito peccherebbe di parzialità e di incompletezza. Se potessimo guardare trasversalmente le potenzialità del nuovo ritrovato tecnologico – non limitandoci dunque alle applicazioni di tipo economico-finanziario – ci renderemmo subito conto della moltitudine di problematiche che, a vario titolo, discendono dall'utilizzo della *blockchain*.

Le questioni relative alla configurabilità di una specifica ipotesi di reato ci sembrano, a ben vedere, recessive rispetto alle ben maggiori criticità che si pongono sul piano dei principi della materia penale. Basti pensare al dilemma, tutt'ora irrisolto, del luogo di commissione del reato informatico che diviene ancor più intricato allorché un delitto venga commesso per il tramite di un sistema *peer to peer*; alla tematica del tempo del commesso reato, rispetto alla quale si dovrà chiarire l'incidenza del requisito della validazione temporale di cui all'art. 8-*ter*, comma 3, del D.L. 14 dicembre 2018 n. 135[28]; alla possibilità di configurare una posizione di garanzia in capo ai gestori di *blockchain* private oppure obblighi di controllo preventivo da parte dei soggetti che validano le transazioni. La soluzione di questi problemi ci consentirà di porre alcuni punti fermi, preparando così il campo per l'esame delle singole fattispecie di reato.

Una premessa di ordine metodologico ci sembra tuttavia opportuna. Il terreno che si apprestiamo a percorrere è reso estremamente scivoloso non solo dalla novità e dalla complessità del tema, ma anche dalla mancanza di una compiuta ricostruzione dogmatica delle categorie rilevanti nell'ambito del diritto penale dell'informatica[29]. Le riflessioni svolte nei paragrafi successivi avranno pertanto carattere sperimentale e non vantano alcuna pretesa di esaustività. Il tema sarà affrontato sulla falsariga delle opinioni espresse dalla dottrina e dell'elaborazione giurisprudenziale più recente, da cui partiremo per esaminare la tenuta degli schemi tradizionali dinanzi alle sfide lanciate dalla tecnologia a registro distribuito.

2.1. Azione ed evento nel diritto penale dell'informatica.

Una prima questione che viene all'attenzione dello studioso del diritto penale è la particolare conformazione che assumono le categorie dell'azione e dell'evento nel cyberspazio. È questo un tema che ha suscitato l'interesse di parte autorevole della dottrina[30], che ormai da tempo si interroga sul superamento degli schemi tradizionali,

[28] Per un primo commento alle novità introdotte dalla legge 11 febbraio 2019 n. 12 v. Cap. I, § 3.1.

[29] A differenza di altri rami dell'ordinamento penale (diritto penale dell'economia, dell'ambiente, della pubblica amministrazione), la dottrina non ha finora operato alcun riordino sistematico degli istituti e delle ipotesi di reato che compongono il diritto penale dell'informatica. Si tratta di una materia che gode, allo stato attuale di una unità soltanto "virtuale". Cfr. FULVI F. R., *L'unità virtuale del diritto penale dell'informatica*, in PICOTTI L, RUGGIERI F. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, Torino, 2011, 167 ss.

[30] PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, cit., 842; PICOTTI, *Diritto penale e tecnologie informatiche*, cit., 45.

troppo antropomorfi per essere adattati alla dimensione virtuale. Secondo questa corrente di pensiero, nel diritto penale dell'informatica si delinea una inevitabile sovrapposizione tra azione ed evento, poiché l'azione dell'uomo è mediata dalla macchina, all'interno della quale si produce un risultato della condotta non percepibile in termini naturalistici, ma soltanto di logica binaria.

Con riferimento alla nozione di azione, concepita quale attività materiale dell'utente che produce effetti esterni lesivi o pericolosi, è stato condivisibilmente osservato che la sua definizione non può prescindere dall'associazione uomo-macchina: atti dell'uomo possono pur esserci ma *«non appaiono quelli decisivi sotto il profilo della tipicità del 'fatto di reato' cibernetico, apparendo piuttosto determinante, per la sua rilevanza ed offensività penale, la successiva o concomitante azione automatica […] da parte del o dei software che concretamente operano in rete»*. Soltanto in questo modo si può *«'esteriorizzare' l'intenzione e/o direzione dell'attività voluta o consentita dalla persona fisica, alla quale deve giuridicamente imputarsi come 'agente'»*[31]. Nella rete il concetto di azione penalmente rilevante subisce una *«accentuata rarefazione, modellandosi secondo evanescenti forme di trasmissione, immissione, gestione di dati, che a loro volta, svaniscono in impulsi elettronici»*[32], che potrebbero dar luogo a una espansione incontrollabile degli effetti della condotta, travalicando le intenzioni dell'agente[33].

Parimenti, anche la nozione di evento acquisisce caratteristiche peculiari di astrazione ed ubiquità quando sia riferito non al risultato naturalistico della condotta – sia pur intermediata dall'elaboratore – ma alla modificazione di dati o programmi informatici.

All'uopo è opportuno distinguere i reati informatici in due categorie: quelli di *evento in senso proprio* come il danneggiamento di sistemi informatici (art. 635-*quater* e 635-*quinquies*, comma 2), la truffa comune via web (art. 640 c.p.), la frode informatica (art. 640-*ter* c.p.), lo *stalking* informatico (art. 612-*bis*, comma 2 c.p.) rispetto ai quali la consumazione è legata alla realizzazione del risultato fenomenico della condotta; quelli ad *evento c.d. informatico* come l'accesso abusivo a sistema informatico (art. 615-*ter* c.p.) e la distruzione di dati o programmi informatici (art. 635-*bis* e 635-*ter*,secondo periodo, c.p.) la cui integrazione è legata alla modificazione o all'intervento sui dati informatici. In questo secondo caso la produzione di un evento a

[31] PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, ibidem

[32] Così, RESTA F., *La responsabilità penale del* provider*: tra* laissez faire *ed obblighi di controllo,* in *Giur. mer.*, 2004, 9, 1733

[33] Secondo una parte della dottrina l'impossibilità di governare gli effetti della propria azione 'virtuale' genera non poche tensioni sul piano della personalità della responsabilità penale. Il soggetto non potrebbe infatti essere ritenuto autore "diretto" di un'azione così dilatata nei suoi confini, che sembrerebbe fuoriuscire dallo schema tradizionale del rapporto fatto-autore. Cfr. PICOTTI L., *Internet e responsabilità penali*, in PASCUZZI G., *Diritto e informatica,* Milano, 2002, 117; RESTA, *La responsabilità penale del provider*, ibidem.

carattere informatico[34] rende estremamente complessa l'opera classificatoria. Se, da una parte, sembra innegabile che l'azione dell'uomo produca un risultato esterno (*sub specie* di magnetizzazione parziale di un supporto elettronico), dall'altra non si potrebbe non considerare la dimensione soltanto logico-informatica degli effetti, non percepibili *in rerum natura*. In tal senso il concetto di "evento informatico" tende a sovrapporsi, fin quasi a coincidere, con l'azione che lo ha provocato, attribuendo un significato decisivo alla condotta piuttosto che al risultato di essa. Coglie dunque nel segno l'affermazione di chi ritiene che l'accezione naturalistica di evento *«subisce nel mondo virtuale uno svuotamento ed una trasfigurazione, a motivo dell'impossibilità di individuare, spazialmente e temporalmente, un evento smaterializzato, automaticamente riproducibile in quantità pari alle possibilità di percezione da parte di terzi; sostanzialmente privo di autonomia concettuale ed ontologica rispetto all'azione»*[35].

L'interprete è dunque costretto a fare i conti con categorie concettuali pensate per l'agire umano della realtà naturale, che dovranno essere adattate a fatti commessi in una dimensione totalmente dematerializzata, sottratta alle leggi della fisica. Appaiono del resto evidenti le ricadute pratiche dell'inquadramento della fattispecie sul luogo di commissione del reato e, di conseguenza, sulla punibilità di condotte realizzate in tutto o in parte all'estero[36].

2.2. Azione ed evento in *blockchain*.

Ci si chiede, a questo punto, se le criticità messe luce dalla dottrina a proposito dell'azione e dell'evento nel cyberspazio possano in qualche modo interessare gli illeciti commessi su una piattaforma *blockchain.* La risposta non può che essere affermativa: le azioni commesse in una rete *peer to peer*, virtualizzate e intermediate dal mezzo tecnologico, hanno caratteristiche analoghe a quelle realizzate per il tramite di un sistema di reti telematiche.

Esaminando da vicino la questione è tuttavia possibile cogliere alcuni elementi differenziali, che derivano dai connotati particolari della DLT rispetto alle

[34] Le condotte di alterazione, soppressione, cancellazione di dati o programmi informatici sono elencate seguendo la tecnica descrittiva del danneggiamento comune (art. 635 c.p., nella formulazione precedente all'emanazione del D. Lgs. 15 gennaio 2016, n. 7), pacificamente ritenuto un reato di evento. In tal senso anche l'eliminazione dei dati informatici, a stretto rigore, dovrebbe essere inquadrata come reato di evento: il risultato naturalistico della condotta consiste infatti nella modifica delle informazioni immagazzinate sotto forma di BIT sul supporto informatico (*flash drive, hard disk, server* etc.). Più complesso è invece l'inquadramento della condotta di accesso nel reato di cui all'art. 615-*ter* c.p. poiché, pur non essendo dubitabile la possibilità di rintracciare un risultato informatico della condotta (quale, ad es., l'avvenuta registrazione dell'accesso nei file di log), la fattispecie sembra far leva sul mero accesso ai dati *ex latere agentis.* La giurisprudenza, in modo pressoché unanime, considera l'accesso abusivo a sistema informatico un reato di mera condotta (v. Cass. Pen., Sez. Un., 24 aprile 2015, n. 17325, in *Dir. pen. proc*., 2015, 10, 1296 con nota di in FLOR R., *I limiti del principio di territorialità nel cyberspace*).
[35] In questi termini, RESTA, *La responsabilità penale del* provider, cit., 1734
[36] *Amplius*, § 2.2

infrastrutture comuni. Le categorie dell'*agere* umano assumono qui contorni ancor più sfumati non solo per la presenza di una moltitudine di registri interconnessi, ma anche a causa della previsione di precise regole sul consenso e sulla convalida delle transazioni.

Si pensi al caso in cui due soggetti si accordino per trasferire un determinato ammontare di valuta virtuale proveniente da delitto. L'operazione illecita si conclude, all'esito di una complessa procedura tecnica, con la chiusura del blocco ad opera del *miner* che per primo ha trovato la soluzione crittografica in grado "mettere ordine" alle *unconfirmed transactions*[37]. L'esecuzione dell'ordine di pagamento – o, più precisamente, dell'*input* di transazione – è sottoposta alla condizione del positivo superamento della convalida. Vi sono inoltre circostanze che potrebbero causare una sopravvenuta caducazione del blocco, nel caso, tutt'altro che scolastico, in cui la soluzione crittografica sia rinvenuta contemporaneamente da più validatori[38] oppure vi sia la volontà conforme di una percentuale qualificata di partecipanti secondo le regole del consenso[39].

La realizzazione del fatto di reato non dipende quindi dalla sola attività del mittente o del ricevente, ma dalla concomitante azione dei soggetti che partecipano alla rete, i quali pongono in essere le condizioni positive perché la transazione abbia luogo.

2.3. Omessa convalida, regole del consenso e caducazione del blocco.

La disciplina del consenso e il funzionamento tecnico della *blockchain* sottolineano come l'azione dell'uomo possa assumere tratti estremamente peculiari nel cyberspazio. Solitamente l'agire umano viene in considerazione, dalla prospettiva del diritto penale, come un fatto storico-naturalistico esternamente percepibile[40]. Nel dominio della fisica non si pone alcuna via mediana tra l'azione e l'inazione, né sarebbe possibile immaginare una retroazione della realtà materiale o un ripristino coatto dello *status quo ante*. Sebbene, a stretto rigore, anche la condotta realizzata mediante l'ausilio del computer si estrinsechi – sia pur in minima parte – in una attività di tipo materiale, non si potrebbe non considerare come l'offensività e la tipicità del fatto dipendano in misura

[37] Per una esemplificazione più accurata della procedura di convalida di una transazione v. Cap. I, § 2 e Cap. V § 4).

[38] Si realizza in questi casi una c.d. forchetta (*fork*), vale a dire uno sdoppiamento della catena di blocchi. Per evitare le conseguenze negative che discenderebbero dalla divisione, alcuni protocolli di base prevedono le condizioni in presenza delle quali una delle due catene (solitamente quella più breve) verrà meno.

[39] La disciplina del consenso è la caratteristica che, più di ogni altra, conferisce una connotazione autonoma alle infrastrutture decentralizzate. Se il protocollo di base lo prevede, anche la decisione di modificare la catena dei blocchi è in linea di principio possibile; per questo motivo abbiamo ritenuto che il requisito della non modificabilità contenuto nella recente definizione legislativa di cui all'art. 8-*ter* D.L. 135/2018 debba essere inteso in senso relativo e non assoluto (v. *supra*, Cap. I, § 3.1.).

[40] In questo senso è la dottrina classica di ANTOLISEI F., *Manuale di diritto penale – Parte generale*, Milano, 2003, 223.

significativa dall'elaborazione automatica di dati da parte di un sistema informatico o telematico.

Ritornando al caso pocanzi esemplificato, l'accertamento della responsabilità penale del mittente e del destinatario (per riciclaggio, art. 648-*bis* c.p.) non può prescindere dall'analisi dell'*exitus* informatico della transazione, da quale dipenderà il concreto pericolo[41] di dispersione dei fondi illeciti. Potrebbe infatti darsi che l'operazione non giunga a compimento per fatti simultanei (omessa convalida) o sopravvenuti (caducazione della catena dei blocchi). Nel qual caso si dovrà stabilire quali siano le conseguenze sul piano della responsabilità penale dei soggetti coinvolti, che, per fattori indipendenti dalla loro volontà, non siano riusciti a trasferire i valori virtuali. Più precisamente bisognerà delineare con precisione i limiti del delitto tentato rispetto alla consumazione del reato, resi piuttosto opachi dalla possibilità di una retroazione della *blockchain*. La questione sarà esaminata sulla falsariga del caso affrontato nell'esempio, ma le considerazioni potrebbero essere estese a qualunque altra ipotesi di reato-transazione[42] quale, ad esempio, il finanziamento del terrorismo (art. 270-*quinquies*.1 c.p.) o la sottrazione fraudolenta al pagamento delle imposte (art. 11 D. Lgs. 74/2000)[43].

In caso di omessa convalida ci si domanda quando possano sussistere gli estremi del tentativo punibile rispetto alla figura del reato impossibile *ex* art. 49, comma 2, c.p. Secondo la dottrina prevalente[44], il riciclaggio in forma tentata è configurabile alla stregua dei principi generali (art. 56 c.p.). Si è però rilevato come non sia agevole stabilire quali possano essere gli atti idonei diretti in modo non equivoco a sostituire o trasferire i capitali in modo da ostacolarne l'individuazione della provenienza illecita[45]. Nel caso in esame, per quanto sia inequivoca la volontà di trasferire i fondi, si potrebbe discutere circa la concreta idoneità dell'azione. Come noto, la moderna scienza penalistica aderisce alla teoria c.d. della *prognosi postuma*, secondo cui il giudizio di idoneità degli atti dovrebbe essere operato tenendo conto delle cognizioni dell'uomo medio, ed eventualmente delle superiori conoscenze specifiche dell'agente, posto nel

[41] Sulla natura di reato di pericolo concreto del riciclaggio si veda ZANCHETTI M., *Sub art. 648- ter c.p.*, in CRESPI A., STELLA F., ZUCCALÀ G. (a cura di), *Commentario breve al codice penale*, Padova, 2003, p. 2297; MEZZETTI E., *Reati contro il patrimonio*, Milano, 2013, p. 653 ss.; ZACCHIA A., *La natura del reato di riciclaggio. Nota a Cass. sez. II pen. 13 luglio 2016, n. 29611*, in *Cass. Pen.*,2017, 7, 2824 ss. Per una disamina più approfondita della struttura del delitto di riciclaggio di rinvia al Cap. III, § 3.1.

[42] Per reato-transazione si intende quel delitto che può essere commesso mediante l'invio di fondi virtuali. Più precisamente, possiamo definire tale la transazione che, tenuto conto dell'intenzione delle parti o dei presupposti della condotta, costituisce di per sé reato.

[43] Sulle problematiche applicative di questi reati ai trasferimenti in criptovaluta v. Cap. III; §§ 4.1. e 6.4.

[44] Cfr. ZANCHETTI M., *Il riciclaggio di denaro proveniente da reato*, Milano, 1997, 209 ss.; CERQUA L.D., CAPPA E., *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*, Milano, 2012, 128 ss.; MAGRI P., *I delitti contro il patrimonio mediante frode*, in MARINUCCI G., DOLCINI E. (diretto da), *Trattato di diritto penale – Parte speciale,* Padova, 2007, 468 ss.

[45] Una parte della dottrina ha ipotizzato operazioni di ostacolo di natura negoziale, come l'apertura di un conto corrente o di depositi preordinati al frazionamento delle operazioni, volte a rendere più difficoltosa l'identificazione del soggetto agente (c.d. *smurfing*). Sul punto CERQUA L.D., *Il delitto di riciclaggio nel sistema penale italiano*, in *Revista brasileira de estudios politicos*, 2015, 1, 14.

luogo e al tempo della condotta[46]. Seguendo questa tesi, risulterà davvero arduo negare che, nell'ipotesi di omessa convalida, l'azione non fosse *ex ante* idonea al compimento dell'operazione di riciclaggio, specie nel caso in cui il mittente fosse l'effettivo titolare dell'ammontare di valuta virtuale speso[47]. Si deve infatti considerare che, secondo l'*id quod plerumque accidit*, una transazione tra indirizzi esistenti per un ammontare "spendibile" di valuta virtuale viene di regola convalidata. Appaiono invece del tutto residuali le ipotesi di rifiuto dell'operazione, dovute a fattori contingenti e spesso imprevedibili, come il sovraccarico della rete o il malfunzionamento tecnico del sistema. Possiamo dunque concludere che, nel caso di omessa convalida, il solo fatto dell'*input* di transazione integra gli estremi del tentativo punibile.

Ben più complessa è la questione relativa alle conseguenze giuridiche della caducazione di un blocco. Dall'annullamento della transazione potrebbe derivare una sorta di "riduzione in pristino", tale per cui il mittente rientra in possesso dell'ammontare di valuta inizialmente trasferito.

Proseguendo con il caso esemplificato, si pone un dubbio sulla forma consumata o soltanto tentata del reato di riciclaggio. Sebbene l'*iter criminis* sia stato condotto a termine[48], il successivo ritorno della ricchezza nelle mani del mittente rende piuttosto incerto l'inquadramento teorico[49]. Da una parte si potrebbe sostenere che l'avvenuto trasferimento del contante virtuale, da cui deriva la disponibilità delle somme per il destinatario, evidenzi di per sé l'esistenza di un concreto pericolo di dispersione dei valori: il reato si consuma dunque con la positiva convalida della transazione, momento che segna l'irrilevanza di ogni avvenimento posteriore. Dall'altra sembrerebbe irragionevole non tener conto del successivo rientro dei capitali nella disponibilità del mittente: in un reato di pericolo concreto non è infatti sufficiente il perfezionamento dell'effetto traslativo, dovendosi piuttosto accertare la reale incidenza dell'operazione sulla ricostruzione dell'origine delittuosa dei fondi.

---

[46] In argomento di recente SEMINARA S., *Delitto tentato e reato impossibile: in confini dell'azione punibile*, in *Spazio filosofico*, 2016, 16, 2 ss.; ID., *Il delitto tentato*, Milano, 2012, 645 ss.; GIACONA I., *Il concetto d'idoneità nella struttura del delitto tentato,* Torino, 2000, 138 ss.

[47] Si potrebbe ipotizzare un tentativo inidoneo di riciclaggio – e quindi un reato impossibile – nel caso in cui un soggetto trasferisca una quantità di valuta della quale non può disporre (si pensi al fenomeno del *double spending*, per impedire il quale la maggior parte dei sistemi decentralizzati prevedono meccanismi di validazione *by design* molto accurati). In tal caso l'impossibilità tecnica si traduce in impossibilità giuridica dell'evento di pericolo, con conseguente applicazione del regime di cui all'art. 49, comma 2, c.p.

[48] Con la convalida della transazione le utilità trasferite sono entrate nella piena disponibilità del destinatario, che avrebbe potuto compiere su di esse qualsiasi ulteriore operazione volta ad ostacolare l'identificazione della provenienza delittuosa della provvista. Nello specifico, le *blockchain* pubbliche più rinomate prevedono che il destinatario acquisisca il potere di spendita non appena la transazione raggiunga un numero sufficiente di conferme da parte dell'infrastruttura; di regola il numero di conferme necessarie cresce in base alla quantità di valuta oggetto di trasferimento.

[49] La caducazione di un blocco e il ripristino della situazione pregressa sono ipotesi che non potrebbero dirsi eccezionali. Specialmente nelle *blockchain* private o ibride può facilmente accadere che una percentuale qualificata di partecipanti concordi sulla scelta di un "ritorno al passato", per esigenze di carattere pratico o per ripristinare l'ordine violato (ad. es da un attacco informatico che abbia sottratto un cospicuo ammontare di *token*).

A nostro modo di vedere, la questione non può che essere risolta in modo relativo in base alle circostanze di fatto. Più precisamente, si dovrà aver riguardo al tempo intercorso tra la convalida della transazione e la successiva retroazione del blocco: laddove il trasferimento sia posto nel vuoto in un ristretto arco temporale[50], tale da non concretizzare un pericolo di ulteriore dispersione delle somme, il reato si arresterà allo stato del tentativo; viceversa, l'annullamento intervenuto a lunga distanza di tempo[51] non farà venir meno il perfezionamento della fattispecie.

La soluzione del problema dipenderà del resto anche dalla struttura della fattispecie considerata. Così, ad esempio, il reato di sottrazione fraudolenta al pagamento delle imposte potrà dirsi integrato soltanto nel caso in cui il trasferimento dei valori abbia concretizzato un pericolo effettivo per la riscossione coattiva dei crediti erariali[52], circostanza difficilmente configurabile nel caso di ritorno del capitale virtuale nelle mani del reo. Al contrario, perché si configuri il delitto di favoreggiamento reale (art. 379 c.p.), la condotta d'ausilio potrebbe anche non accrescere in concreto le possibilità di consolidamento dei proventi criminosi[53]: per l'integrazione del reato sarebbe sufficiente anche la sola comunicazione dell'indirizzo al quale inviare i valori, accompagnato dalla manifestazione di volontà di detenere le somme per conto del mittente. L'eventuale rientro degli *asset* virtuali nella disponibilità dell'autore della transazione non potrà in alcun modo incidere sul perfezionamento della fattispecie, che si realizza in un momento antecedente alla ricezione dei valori[54].

---

[50] Il caso tipico è quello della *acciedental fork*, che viene risolto con la caducazione automatica del blocco, solitamente nel giro di pochi minuti (*amplius*, Cap. I, § 2).

[51] Si pensi al caso in cui, a seguito di una lunga petizione, i partecipanti decidano di modificare la *transaction chain*. In tal caso potrebbero intercorrere anche diverse settimane tra il trasferimento dei fondi e l'annullamento delle operazioni.

[52] Ai fini del perfezionamento del reato di cui all'art. 11 D. Lgs 74/2000 è richiesta la concreta idoneità della condotta a rendere inefficace la procedura di riscossione coattiva. La fattispecie è infatti tesa a proteggere l'interesse alla percezione dei tributi nella fase del recupero coattivo e si presenta come reato di pericolo concreto. Sul tema, di recente SOANA G., *I reati tributari*, Milano, 2018, 445; DI VIZIO F., *Il delitto di sottrazione fraudolenta del pagamento delle imposte ed i rapporti con i reati di bancarotta fraudolenta per distrazione e di riciclaggio*, in *Discrimen*, 1 ottobre 2018, 39. *Infra*, v. Cap. III, § 6.3.

[53] Per integrare la condotta materiale del reato di favoreggiamento reale è sufficiente il semplice aiuto all'autore di un reato finalizzato da parte di costui al conseguimento dell'utilità illecita, indipendentemente dal fatto che il favoreggiato riesca effettivamente a conseguire il prodotto, il profitto o il prezzo del reato. Cfr. Cass. Pen., sez. VI, 08 ottobre 1998 n. 778 in *Cass. Pen.*, 2000, 605 ss., in cui la Corte ha ritenuto che ricorresse l'ipotesi del reato di favoreggiamento reale, consumato e non tentato, nella condotta di un soggetto che aveva aiutato altra persona ad assicurarsi il parziale provento della vendita di refurtiva facendole accendere depositi vincolati o conti correnti a nome proprio. Il caso affrontato dalla Corte presenta forti similitudini con la condotta di favoreggiamento consistente nella creazione di un indirizzo (Bitcoin, Ethereum, Monero etc.) per la ricezione dei valori: il reato si consuma con la creazione e la messa a disposizione dell'indirizzo, senza che assuma rilevanza l'effettivo inoltre dei proventi delittuosi ai conti di destinazione.

[54] Secondo la posizione consolidata della S.C. (v. tra le sentenze storiche Cass. Pen., sez. III, 26 maggio 1981, in *Riv. Pen*., 1982, 189; di recente Cass. Pen. sez. VI, 07 giugno 2018, n.3608) l'elemento oggettivo del reato di favoreggiamento reale è costituito da qualsiasi comportamento idoneo a far definitivamente conseguire al favorito il provento della sua precedente attività criminosa e tale condotta non deve implicare necessariamente un contatto fisico tra il soggetto attivo del reato e la *res* da assicurare, essendo sufficiente qualsiasi azione od omissione obiettivamente idonea allo scopo.

3. *Smart contract* e agenti *software* autonomi. Considerazioni sul rapporto di autoria tra transazione illecita e operatore economico.

L'evanescenza del concetto penalistico di azione nei reati commessi mediante la tecnologia a registro distribuito si deve anche alla progressiva emersione degli agenti *software* autonomi che operano in *blockchain*.

Il tema degli *smart contract* ha suscitato un grande interesse nella dottrina internazionale[55], spingendo alcuni autori a interrogarsi sulla natura giuridica e sulla disciplina applicabile a questi particolari programmi informatici[56]. Il riconoscimento giuridico dei contratti *smart* – specie per quel che riguarda i requisiti di forma e di validazione temporale[57] – ha segnato un importante passo verso la totale automazione di molte relazioni negoziali. Volendo descrivere in estrema sintesi il funzionamento di questi agenti-*software*, basterà ricordare che al verificarsi di certe condizioni, predeterminate dal programmatore e "attivate" dalle parti, l'algoritmo darà esecuzione al contratto, eseguendo in modo automatico la prestazione in esso dedotta. Il compimento di attività giuridicamente rilevanti per il tramite del *software* solleva questioni di non poco conto sul piano della responsabilità penale, allorché il contratto sia utilizzato per scopi illeciti ovvero sia esso stesso il mezzo esecutivo del reato. È questo un tema che ha già catturato l'attenzione della dottrina penalistica più avanguardista[58] che, guardando più in generale alle applicazioni dell'intelligenza

[55] SKLAROFF J.M., *Smart Contracts and the Cost of Inflexibility*, in *University of Pennsylvania Law Review*, 166, 2017, 262; BOURQUE S. – FUNG LING TSUI S., *A lawyer's introduction to smart contract*, in *Scientia Nobilitat – Review of legal studies*, 2014, 4; SWANSON T., *Great Chain of Numbers: A guide to Smart Contracts, Smart Property and Asset Management*, Oxford, 2014, 16; SURDEN H., *Computable Contracts*, in *UC Davies Law Review*, 2012, 46, 629; DE FILIPPI P. - HASSAN S., *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, in *First Monday*, 2016, 21, 12 ss.

[56] Cfr. CUCCURU P., *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *Nuova Giurisprudenza Civile Commentata*, 2017, 1, 107 ss.; SARZANA DI S. IPPOLITO F. – NICOTRA M., *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018.

[57] Si richiama il contenuto dell'art. 8-*ter* del D.L. 135/2018, come modificato dalla legge di conversione n. 12/2019 (v. *supra*, Cap. I, § 3.2.).

[58] BURCHARD C., *Artificial intelligence and law*, in WOLFF B., *Whiter artificial intelligence? Debating the policy challenges of the upcoming transformation*, Science Policy Fellowship Program Paper 03/2018, Frankfurt am Main, 14 ss.; HILDEBRANDT M., *Criminal liability in smart environments*, in DUFF R. A., GREEN S., *Philosophical foundations of criminal law*, Oxford, 2011, 212; ID., *Smart technologies and the end(s) of the law*, Cheltenham, 2016; HALLEVY G., *The criminal liability of artificial intelligence entities – from science fiction to legal social control*, in *Akron Intellectual Property Journa*l, 2010, 4, 171 ss.

artificiale, ha ravvisato alcuni possibili profili critici[59]. Alcuni autori[60] hanno posto in evidenza le problematiche derivanti dall'utilizzo degli algoritmi di *trading* sui mercati finanziari[61] e le relative implicazioni su piano della responsabilità penale per *market abuse.* Si è rilevata una tendenziale rottura del rapporto di *autoria* tra transazione finanziaria e operatore fisico, che rende complessa la ricostruzione delle condizioni di responsabilità della persona fisica che si avvale degli *high frequency traders*. L'aspetto più problematico riguarda l'attualizzazione delle istruzioni fornite dal programmatore, che è rimessa alla "scelta" dell'algoritmo[62]. Ne deriverebbe l'assenza del *dolo del fatto,* inteso come singola negoziazione o complesso di negoziazioni illecite, non potendo l'elemento psicologico del reato essere ridotto a una sorta di *dolus generalis* di perturbazione del mercato[63]. La stessa dottrina ipotizza due distinti modelli di responsabilità, facenti leva su istituti già noti alla scienza penalistica italiana.

Il primo meccanismo di imputazione considera la messa in funzione dell'algoritmo una *actio libera in causa*. Ai fini della responsabilità penale si potrebbe valorizzare l'attivazione consapevole di un rischio poi concretizzatosi in evento lesivo che, altrimenti, non potrebbe essere posto a carico dell'agente a causa dell'incapacità di rispondere delle proprie azioni[64]. Sennonché l'istituto codicistico di riferimento (art. 87 c.p.) è applicabile ai soli casi di ubriachezza e intossicazione per l'assunzione di

[59] Si è posta in particolare la questione relativa alla responsabilità per danni causati dagli agenti *software,* in punto di imputazione degli effetti dannosi e di rimproverabilità soggettiva. Di qui l'interrogativo circa l'opportunità di "riadattare" le concezioni tradizionali dell'autorìa, della causalità e del dolo ovvero di rinunciare all'applicazione del diritto penale in una materia che supera i confini della volontà umana. *«If these nonhuman or hybrid 'agents' cause harm to others a series of questions come to mind: to what extent can such agency be identified as 'causing' harm; what is the meaning of 'intent', 'intention' and 'mens rea' in the case of nonhuman agency; do we need to revise our conceptions of agency, causality, intent, intention and mens rea to accommodate the fact that nonhuman or hybrid 'agents' do not fit our traditional conceptual framework, or, alternatively, should we reject applicability of the criminal law in cases that fall outside the scope of human intention as we presently understand it»* (HILDEBRANDT, *Criminal liability in smart environments,* cit., 212).

[60] CONSULICH F., *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato,* in *Banca, borsa e titoli di credito,* 2018, 2, 195 ss.

[61] Gli operatori algoritmici ad alta frequenza assumono decisioni di investimento sulla base di analisi matematiche quantitative attinenti alle oscillazioni dello strumento finanziario in un dato periodo oppure a seconda della captazione del nome dell'emittente sui mezzi di informazione. Sono queste informazioni che non riguardano le variabili economiche a cui si atterrebbe un investitore professionale: si verifica così una dissociazione tra azione di mercato e informazione finanziaria che fa venir meno la figura dell'investitore ragionevole. In tal senso, v. CONSULICH, *Il nastro di Möbius,* cit., 218

[62] Secondo la dottrina da ultimo citata, il programmatore determina soltanto il modello di comportamento a cui l'algoritmo deve attenersi, ma non anche il tipo e l'identità del titolo da negoziare, il momento e il contesto in cui agire.

[63] CONSULICH, *Il nastro di Möbius,* cit., 219, che descrive in questi termini la componente psicologica dell'abuso di mercato commesso mediante *high frequency traders*: «*un dolo frammentato e insufficiente al rimprovero penale […] il diritto penale si presenta impreparato all'appuntamento con le transazioni algoritmiche, privo degli 'anticorpi concettuali' necessari alla repressione di siffatte tipologie di abuso*».

[64] In argomento, VENDITTI M., *Actio libera in causa,* in *Enc. Dir.,* 1958, I, 53 ss.; BATTAGLINI G., CRIFÒ G., voce *Imputabilità,* in *Noviss. Dig.,* 1962, VIII, 455; CRESPI A., voce *Imputabilità (dir. pen.),* in *Enc. Dir*., 1970, XX, 781; ROMANO M., GRASSO G., *Commentario sistematico al codice penale*, Sub *art. 87*, Milano 2012, 30; da ultimo si veda anche la monografia di MENGHINI A., *Actio libera in causa*, Padova, 2015.

stupefacenti, limitatamente alle ipotesi in cui vi sia una corrispondenza tra il reato commesso e il proposito criminoso maturato[65].

Un secondo paradigma ascrittivo ruota attorno al modello delineato dall'art. 8 del D. Lgs. 231/2001. Sul punto si è osservato – sempre con riferimento ai reati di *market abuse* – che i criteri di imputazione della responsabilità dell'ente riescono meglio a sopportare *«le tensioni suscitate dal fenomeno della disumanizzazione delle offese»*[66]. Applicando il principio espresso dalla norma al fatto compiuto dal *trader* algoritmico, l'ente risulterà responsabile tanto nel caso in cui lo "schermo del *software*" non abbia reso possibile l'individuazione del programmatore o dell'utilizzatore, quanto nell'ipotesi – testé richiamata – di mancanza dell'elemento soggettivo del dolo in capo a questi ultimi[67].

Il rischio di "rottura" del rapporto di autoria tra transazione e operatore economico emerge con tutta evidenza nelle condotte poste in essere dagli agenti *software* autonomi[68] che operano in *blockchain.* I contratti *smart* eseguono la prestazione in essi dedotta al verificarsi di determinate condizioni, che non dipendono direttamente ed esclusivamente dalla volontà del predisponente, né da quella del beneficiario.

Le parti possono concordare sul contenuto di un contratto già registrato in *blockchain* ad opera di un terzo (*smart contract* improprio o di terza parte), ovvero concludere da sé un accordo in linguaggio computazionale (*smart contract* proprio).

Nel primo caso si pensi alla pubblicizzazione di un contratto *smart* che, al verificarsi di determinate condizioni, compia attività. di *mixing*[69], movimentando le valute virtuali su più conti intermedi per poi permettere di recuperare le somme su un conto di destinazione. Gli utenti ricorrono a un simile agente contrattuale per disperdere la tracciabilità dei flussi di transazioni iscritti sul registro pubblico, al precipuo fine di riciclare proventi di origine delittuosa. Anche qui, però, non vi è alcun dolo del fatto, poiché il programmatore non è in grado di predeterminare *ex ante* se lo *smart contract* verrà attivato e, soprattutto, se sarà strumentalizzato per fini di riciclaggio. Detto altrimenti, il programmatore non ha alcuna rappresentazione e volizione del flusso di

[65] L'art. 87 c.p. regola il caso in cui lo stato di incapacità sia preordinato alla commissione di un reato, vale a dire quelle condotte sorrette da intenzionalità rispetto al reato che si intende commettere. L'estensione della disciplina dell'*actio libera in causa* alle condotte di *market abuse* conseguenti alle scelte di investimento dell'algoritmo concreterebbe una violazione del divieto di analogia in *malam partem*.

[66] In questi termini, CONSULICH, *Il nastro di Möbius,* cit., 224

[67] La stessa dottrina definisce l'art. 8 come norma avente *«una inaspettata funzione preventiva, proprio nei contesti più avveniristici del reato economico, consentendo l'intervento penalistico rispetto alle ipotesi di irresponsabilità organizzata»*.

[68] Sul tema degli agenti *software* autonomi – sia pur in relazione ai profili civilistici della responsabilità – fondamentale TEUBNER G., *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten*, in *Ancilla Iuris*, 2018, vol. 35, 38 ss.; ID., *Ibridi e attanti, Attori collettivi ed enti non umani nella società e nel diritto*, Milano, 2015.

[69] Per la definizione di *mixing* e le varie tipologie esistenti si rinvia al prosieguo della trattazione (v. infra, Cap. III § 3.4.2.).

transazioni che saranno processate dall'algoritmo, né dell'illiceità dei capitali impiegati per rendere eseguibile il contratto[70].

3.1. Esecuzione automatica del contratto e responsabilità penale.

Quanto alla predisposizione in forma computazionale della volontà dei contraenti (*smart contract* proprio), si dia il caso della prestazione di valute virtuali come contratto autonomo di garanzia, tale per cui di fronte all'inadempimento della prestazione da parte del debitore verrà effettuato un accredito in favore del creditore garantito. Qualora l'operazione economica fosse preordinata alla distrazione del patrimonio della società garante, l'utilizzo di un agente contrattuale autonomo non manderà di certo esente l'amministratore da responsabilità penale per bancarotta patrimoniale o preferenziale (art. 322 D. Lgs. 14/2019). Sarà tuttavia complesso provare la sussistenza del dolo in capo a tutti i soggetti coinvolti, dal momento che, una volta concluso il contratto, le parti si spogliano interamente della discrezionalità nella relativa esecuzione. Pertanto, in assenza di sintomi del dissesto economico alla data del perfezionamento dell'accordo, non si potrebbe muovere all'amministratore della società garante alcun rimprovero né per aver distratto i beni della società[71], né per aver indebitamente preferito il pagamento di alcuni creditori[72]. Egli infatti non conserva alcun margine di scelta nel dare esecuzione o meno alle obbligazioni contratte, la cui prestazione si auto-esegue alla verificazione delle condizioni stabilite.

---

[70] Si potrebbe far leva sul concetto di dolo eventuale per rendere applicabile la disposizione sul concorso di persone nel reato. A tal fine, secondo una autorevole opinione dottrinale, è sufficiente che il concorrente si rappresenti la concreta possibilità dell'azione delittuosa che altri hanno intenzione di commettere, accompagnata dalla volontà di concorso e dall'apporto causale, di tipo materiale o morale, alla commissione del reato. Cfr. ANTOLISEI, *Manuale di diritto penale – Parte generale*, cit., 569. In giurisprudenza sulla responsabilità concorsuale per riciclaggio a titolo di dolo eventuale v. Cass. Pen., sez. II, 14 gennaio 2016, n. 9472, in *Rivista di diritto bancario*, 18 marzo 2016.

[71] Cfr. Cass. pen., Sez. V, 23 giugno 2017 n. 38396 secondo cui le ipotesi di bancarotta fraudolenta patrimoniale puniscono non già, indifferentemente, qualsiasi atto in diminuzione del patrimonio della società ma soltanto *«tutti quelli che quell'effetto sono idonei a produrre in concreto, con esclusione, pertanto, delle operazioni realizzate […] quando la società era* in bonis*, tali da non essere capaci di comportare una alterazione sensibile della funzione di patrimonio»*. Nell'accertamento dell'elemento soggettivo deve valorizzarsi, in particolare, la ricerca di "indici di fraudolenza" necessari a dar corpo alla prognosi postuma di concreta messa in pericolo dell'integrità del patrimonio dell'impresa funzionale ad assicurare la garanzia dei suoi creditori e alla relativa proiezione soggettiva, ossia all'accertamento, in capo all'agente, della consapevolezza e della volontà della condotta in concreto pericolosa. Per gli opportuni approfondimenti bibliografici si rinvia a MUSCO E., ARDITO F., *Diritto penale fallimentare*, Bologna, 2018, 22 ss.

[72] Poiché l'adempimento di un debito rappresenta una condotta pur sempre doverosa per l'imprenditore, ciò che caratterizza la bancarotta fraudolenta preferenziale (oggi, art. 322, comma 3, D. Lgs. 14/2019) risiede nel particolare *animus* dell'agente, ovverosia nell'essere la sua condotta precisamente orientata allo *«scopo di favorire, a danno dei creditori, taluno di essi»*. Più precisamente, la giurisprudenza ritiene che l'elemento soggettivo del reato sia costituito da un dolo composito: non solo il dolo specifico di far conseguire ad un creditore l'indebito vantaggio, ma anche il dolo eventuale costituito dall'accettazione dell'eventualità di determinare, così facendo, un danno alla massa dei creditori nella consapevolezza dello stato di dissesto patrimoniale. Cfr. *ex plurimis*, Cass. Sez. V, 13 novembre 2014 n. 2286 e, da ultimo, Trib. Milano, Sez. I, 31 maggio 2018, n. 6456.

Non si potrà dunque ipotizzare alcuna responsabilità per l'esecuzione fraudolenta dell'accordo ma soltanto per la precedente pattuizione illecita. Detto altrimenti, occorre che l'intera operazione economica fosse *ab origine* strumentale alla commissione di un reato fallimentare; non assumerà invece alcuna rilevanza l'eventuale proposito, successivamente sorto, di giovarsi della prestazione futura per realizzare fatti di bancarotta fraudolenta. L'automazione dell'*enforcement* del contratto comporta così delle deroghe all'ordinario regime di responsabilità penale, che dovrà essere parametrato all'impossibilità per la parte obbligata di recuperare il controllo sulla fase esecutiva.

Per esprimere un giudizio sulla responsabilità delle altre parti coinvolte, si dovrà inoltre aver riguardo alle singole clausole contrattuali. Nel caso in esame l'esecuzione del contratto *smart* dipende dalla condizione dell'omesso pagamento delle somme da parte del debitore[73]. Trattandosi di una condizione potestativa dipendente dalla volontà di un soggetto terzo, potrebbe ben darsi che i contraenti si accordino con questi per far sì che l'evento futuro si realizzi. Ove le parti giungano a un *pactum sceleris* – precedente alla esecuzione automatica della prestazione ma successivo alla conclusione dello *smart contract* – finalizzato ad assicurare la verificazione della condizione dell'inadempimento del terzo, saranno tutte responsabili del reato fallimentare eventualmente commesso. Il creditore e il terzo garante non potranno qui invocare a propria discolpa l'esecuzione automatica della prestazione, avendo essi stessi indotto il debitore a non adempiere, nella piena rappresentazione dello stato di dissesto patrimoniale del garante. Al contrario, ove l'inadempimento si verifichi per causa imputabile esclusivamente al soggetto obbligato e nel frattempo la società garante, inizialmente *in bonis*, manifesti uno stato di dissesto, l'esecuzione del contratto non potrebbe essere assunta a fondamento della responsabilità per bancarotta prefallimentare.

3.2. Azione automatica del *software* e condotta penalmente rilevante. Un quadro di sintesi.

I casi appena esaminati lasciano chiaramente intravedere come le preoccupazioni espresse dalla dottrina circa la disumanizzazione dell'azione del cyberspazio[74] trovino conferma nelle applicazioni più avveniristiche della tecnologia a registro distribuito. Numerose sono le questioni che si affacciano all'attenzione del penalista, relative per lo più alla presenza di intermediari tecnologici tra l'azione dell'uomo e il risultato dell'elaborazione automatica di dati.

[73] Il *software* contiene infatti una clausola secondo cui, se in un determinato tempo non è stata ancora trasferita una somma di denaro all'indirizzo appartenente al creditore (circostanza riscontrabile dalle risultanze del registro pubblico delle transazioni), allora sarà disposto in favore di quest'ultimo un versamento dall'indirizzo del fideiussore per il medesimo ammontare.

[74] Si richiama la tesi di PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, cit., 842

Gli *smart contract* sono un esempio emblematico dell'emersione di una sorta di "associazione uomo-macchina"[75], probabilmente destinata a dominare un quadro normativo tuttora concepito in chiave antropocentrica. Quale che sia l'attività giuridica in concreto eseguita dal *software*, non può negarsi la progressiva perdita del *dominium* dell'uomo nella produzione di determinati effetti giuridici quali, ad esempio, la scelta del contraente, la volontà di concludere l'accordo e di eseguire la prestazione in esso dedotta.

Queste attività sono di significativa importanza per l'integrazione di alcune fattispecie di reato. Nel caso dell'offerta al pubblico di un programma per elaboratore utilizzabile per propositi criminosi – che una parte della dottrina ha denominato *criminal smart contract*[76] – si pongono dubbi sulla scissione del rapporto di autoria tra la transazione illecita e programmatore. Non vi è infatti alcun legame psicologico – se non indiretto e soltanto potenziale – con le condotte delittuose eventualmente poste in essere da terzi.

L'assenza di un *dolo del fatto* induce a far leva paradigmi ascrittivi più flessibili, tra cui quello basato sulla responsabilità autonoma o vicaria dell'ente[77]. La predisposizione di un *software-as-a-service*, utilizzabile dietro il pagamento di una commissione sulle singole transazioni, permette di ricondurre i reati eventualmente commessi dalla persona fisica[78] che agisce nell'interesse o a vantaggio della persona giuridica nell'alveo della criminalità economica d'impresa (società di programmazione e di brevettazione di *software*, *service provider*, gestori di infrastrutture decentralizzate etc.). Non sarebbe del resto necessaria neppure una estensione del catalogo dei reati presupposto, atteso che molte delle condotte illecite realizzabili mediante un contratto *smart*[79] sembrano già ricomprese nella lunga lista di cui agli artt. 24 ss. D. Lgs. 231/2001.

Quando un contratto *smart* è utilizzato per regolare i rapporti economici tra le parti interessate l'azione automatica del programma – non ripudiabile né eliminabile al verificarsi delle condizioni prestabilite – potrebbe integrare di per sé una condotta

---

[75] L'espressione è di TEUBNER, *Ibridi e attanti, Attori collettivi ed enti non umani nella società e nel diritto*, cit., 32

[76] JUELS A., KOSBA A., SHI E., *The Ring of Gyges: Investigating the Future of Criminal Smart Contracts, Conference Paper on Computer and Communication Security*, Vienna, 2016, 2 ss.

[77] Tale è la soluzione proposta da una parte della dottrina, sia pur con riferimento al diverso tema dell'utilizzo degli algoritmi di *trading* sui mercati finanziari (*supra*, § 2.1.3). La tesi fa leva su una lettura dell'art. 8 in combinato disposto con i precedenti artt. 6 e 7, tale per cui qualora la persona fisica sia identificata, ma carente di dolo, l'ente deve potersi discolpare provando, a seconda dei casi, l'elusione fraudolenta del modello o la sua adozione ed efficace attuazione (in base alla qualifica di apicale o subordinato dell'autore del fatto).

[78] La colpa in organizzazione sussisterebbe indipendentemente dalla responsabilità a titolo monosoggettivo o concorsuale dell'autore dell'illecito: non occorrerebbe quindi la prova del dolo del fatto e del dolo di partecipazione della persona fisica.

[79] Basti pensare al caso, già esemplificato, dell'offerta di servizi di *mixing* (riciclaggio o autoriciclaggio, art. 25-*octies* D. Lgs. 231/2001); oppure alle ipotesi in cui uno *smart contract* regoli i rapporti economici relativi alla diffusione di una opera dell'ingegno protetta (violazioni del diritto d'autore, art. 25-*nonies*) o al *trading* di strumenti finanziari (abusi di mercato, art. 25-*sexies*), o al finanziamento del terrorismo (delitti di cui all'art. 25-*quater*), o al danneggiamento di sistemi informatici (art. 24-*bis*).

penalmente rilevante. Guardata da questa prospettiva, l'"azione concomitante"[80] del *software* assume caratteri di profonda autonomia, evidenziando una possibile sfasatura tra il *task* eseguito dal programma e la volontà dei soggetti obbligati. Così, nel caso in cui i pagamenti siano eseguiti in modo automatico, i presupposti soggettivi della bancarotta fraudolenta preferenziale dovranno ricorrere al momento della conclusione dell'accordo, a partire dal quale la parte debitrice perde il controllo sull'adempimento della prestazione.

A nostro modo di vedere, la progressiva automatizzazione delle relazioni socioeconomiche farà perdere alla volontà umana la posizione di assoluta centralità che oggi occupa. Dinanzi a questa "rivoluzione copernicana" il diritto penale dovrà dimostrare una certa flessibilità nell'adeguare i tradizionali paradigmi di imputazione alle nuove forme di manifestazione del reato, in cui la condotta umana è intermediata dai programmi informatici e dalla contestuale azione degli altri utenti della rete.

3.3. *Criminal smart contract* e *dual use software*.

Nel paragrafo precedente si è detto che, grazie alla DLT, è possibile mettere a disposizione del pubblico programmi per elaboratore che consentono alle parti di regolare in modo automatico determinati rapporti economici. La locuzione *criminal smart contract è* utilizzata per descrivere quei programmi utilizzati per l'esecuzione di condotte costituenti reato. Se da un lato si tratta di *software* "neutri", la cui illiceità dipende sostanzialmente dall'uso che ne viene fatto, dall'altro non si potrebbe negare l'oggettiva pericolosità degli stessi. Ci si domanda, pertanto, a quali condizioni le condotte consistenti nella creazione e messa a disposizione del pubblico di questi programmi possano assumere rilevanza penale. Nel quadro normativo attualmente vigente vi sono alcune disposizioni che, in un'ottica anticipatoria della tutela penale, puniscono azioni consistenti nel procurarsi o diffondere programmi per elaboratore intrinsecamente pericolosi[81]. Per definire questa tipologia di reati la dottrina tedesca ha

[80] Si richiamano le parole di PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza*, cit., 842

[81] L'art. 615-*quater* c.p. punisce chi «al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza»; il successivo art. 615-*quinquies* c.p., come modificato dalla legge 18 marzo 2008, n. 48, punisce chi, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento *«si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici»*. Rivolgendo lo sguardo all'ordinamento sovranazionale, l'art. 6 della Convenzione di Budapest obbliga gli Stati a criminalizzare la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione e qualsiasi altra condotta consistente nella messa a disposizione di apparecchiature o programmi per *computer* principalmente concepiti o adattati al fine di commettere uno dei reati di cui agli artt. 2 e 5 della Convenzione. Di recente la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione (art. 7) ha imposto agli Stati membri di perseguire penalmente *«la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione di uno dei seguenti strumenti […] un programma per computer, destinato o modificato*

coniato l'espressione "*software-Delikte*"[82] che secondo alcuni[83] rende bene l'idea di un disvalore penale collegato alla pericolosità del programma in sé, piuttosto all'azione concretamente posta in essere[84].

Il tema in esame può essere collocato nell'ambito del dibattito relativo ai *dual-use software*, vale a dire quei programmi informatici che, possedendo un elevato potenziale offensivo, possono essere impiegati non solo per finalità illecite, ma anche per scopi legittimi. Senza entrare nel merito delle scelte di politica criminale compiute dal legislatore[85], possiamo qui limitarci a descrivere sinteticamente i margini di rilevanza penale delle condotte aventi ad oggetto programmi multifunzionali.

Da una parte vengono incriminati comportamenti che si sostanziano nell'esercizio di un pieno controllo sul *software* (produzione, fabbricazione, acquisto, importazione), anche se non sorrette dal fine specifico di commettere un reato[86]. Dall'altra il legislatore tipizza in via autonoma comportamenti espressivi di una pericolosità indiretta (diffusione, consegna, messa a disposizione di terzi), che offrono ad altri occasione per delinquere o agevolino l'esecuzione di determinate condotte[87]. Il legislatore individua l'oggetto materiale del reato ricorrendo a diverse formule linguistiche, che valorizzano, a seconda dei casi, l'intenzione che muove l'agente (nozione soggettiva)[88] o l'idoneità

principalmente al fine di commettere uno dei reati di cui agli articoli da 3 a 6» della Direttiva. In argomento v. CAPPELLINI A., *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 762 ss.

[82] ALBRECHT M., *Die Kriminalisierung von Dual-Use-Software*, Berlin, 2014; POPP A., *§202c StGB und der neue Typus des europäischen «Software-Delikts»*, in *Goltdammer's Archiv für Strafrecht*, 2008, 375.

[83] SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tutela penale. L' incriminazione dei "dual-use software"*, in *Riv.it. dir. proc. pen*., 2017, 2, 750

[84] Si puniscono infatti comportamenti prodromici alla commissione di ulteriori reati, anticipando la soglia di rilevanza penale di fatti che potrebbero reca un'offesa al patrimonio, alla riservatezza informatica, alla integrità e alla disponibilità dei dati e dei sistemi informatici.

[85] Per approfondimenti si rinvia all'analisi svolta da SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale,* cit., 767

[86] Tale fine è presente, ad esempio, nel reato di cui all'art. 615-*quinquies,* ma manca nel precedente art. 615-*quater* c.p.

[87] La stessa dottrina ritiene che l'incriminazione in via autonoma di tali condotte rappresenti una deroga alla disciplina del concorso di persone nel reato, poiché attribuisce rilevanza penale a contributi atipici che resterebbero altrimenti impuniti (ad es. nel caso in cui il reato non venga commesso, oppure nel caso in cui manchi il dolo di partecipazione). Vengono in tal modo stigmatizzate condotte che non raggiungerebbero neppure la soglia minima del tentativo.

[88] In questa categoria rientrano le nozioni che ricollegano la rilevanza penale del programma all'utilizzo che il soggetto intende farne. Ad esempio, la direttiva 2001/29/UE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (art. 6, par. 2, lett. c) prescrive che gli Stati membri debbano assicurare *«una adeguata protezione contro la fabbricazione, l'importazione, la distribuzione, la vendita, il noleggio […] di prodotti o componenti che siano principalmente progettate, prodotte, adattate o realizzate con la finalità di rendere possibile o di facilitare l'elusione di efficaci misure tecnologiche»*. Similmente, l'art. 6, par. 1, della Convenzione di Budapest (cfr. *supra*) fa riferimento ai programmi per *computer* principalmente concepiti o adattati al fine di commettere un reato. Il legislatore nazionale ha sperimentato la "formula soggettiva" in alcune fattispecie a tutela del diritto d'autore, tra cui l'art. 171-*bis* l. 22 aprile 1941, n. 633 nella parte in cui prevede la rilevanza penale della detenzione a scopo commerciale di qualsiasi «*mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori*».

concreta ad essere utilizzati per scopi criminosi (nozione oggettiva)[89]. Non esiste dunque alcuna definizione che permetta di individuare in modo generalizzato e *a priori* quali programmi informatici debbano ritenersi intrinsecamente illeciti; si dovrà al contrario fare riferimento ai fini perseguiti dall'utente o dal programmatore ovvero alla attitudine del programma ad agevolare la commissione di determinati reati.

Ciò rende estremamente complesso stabilire a che condizioni la programmazione o la diffusione di uno *smart contract* sia un fatto dotato di autonomo disvalore penale. La questione non riguarda quelle condotte che trovano già in una disposizione di legge espressa tipizzazione[90], ma quei fatti che appaiono atipici e assumerebbero rilevanza soltanto entro gli schemi del tentativo o del concorso di persone.

A tal riguardo possiamo richiamare il caso, sopra esemplificato, del servizio di *mixing* di transazioni[91]. La condotta del programmatore dello *smart contract* consiste nel mettere a disposizione del pubblico un mezzo astrattamente idoneo ad agevolare il riciclaggio di capitali di provenienza illecita, ipotesi non riconducibile ad alcuna delle fattispecie che sanzionano la creazione o la divulgazione del *software*.

---

[89] A questa categoria appartengono diverse nozioni di *dual-use software*, che fanno leva su criteri di tipo oggettivo. Ad esempio l'art. 3, par. 1, lett. d) della Direttiva 2014/62/UE impone l'adozione di sanzioni penali per punire la fabbricazione fraudolenta, la ricettazione, il procacciamento o il possesso di programmi informatici che *«per loro natura sono particolarmente atti alla contraffazione o all'alterazione di monete»*. È giusto il caso di osservare che la norma nazionale che punisce una simile condotta si basa invece su un criterio soggettivo della destinazione (cfr. art. 461 c.p., fabbricazione e detenzione di programmi e dati informatici o strumenti destinati alla contraffazione). Delle altre fattispecie codicistiche l'art. 615-*quater* c.p. fa leva sul criterio dell'idoneità («*altri mezzi idonei all'accesso ad un sistema informatico o telematico*»), mentre il successivo art. 615-*quinquies*, il cui oggetto materiale era costituito dai programmi *«aventi per scopo o per effetto»* il danneggiamento di dati o sistemi informatici altrui, è stato modificato dalla legge 48/2008. Attualmente la selezione delle condotte penalmente rilevanti è affidata al dolo specifico di danneggiamento o di interruzione del funzionamento di un sistema informatico, che rende in linea di principio punibile anche la cessione o la consegna di programmi assolutamente innocui (es. un sistema operativo auto-avviante, se destinato ad essere utilizzato per forzare l'accesso a un sistema informatico protetto da misure di sicurezza). Al criterio oggettivo si affidano anche alcune fattispecie della legislazione penale speciale, ad esempio l'art. 171-*ter*, comma 1, lett. f), che punisce l'installazione di *«dispositivi o elementi di decodificazione che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto»*. In argomento, *amplius* v. SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale*, cit., 764.

[90] Si pensi a un contratto *smart* per regolare la cessione di credenziali di accesso a un sistema informatico così congegnato: il soggetto interessato all'acquisto trasmette il prezzo da pagare all'indirizzo dell'agente contrattuale autonomo il quale, dopo aver ricevuto in *input* dal venditore le credenziali, ne verifica automaticamente il funzionamento. Nel caso in cui l'autenticazione abbia successo il prezzo è trasferito all'indirizzo del destinatario; laddove l'accesso sia rifiutato la somma viene restituita al mittente. Un programma di questo tipo sarebbe molto utile nelle contrattazioni illecite a distanza, poiché preverrebbe il rischio di inadempimento di una delle parti. L'autore del *software* risponderà tuttavia del reato previsto dall'art. 615-*quater* c.p. per aver messo a disposizione un mezzo idoneo all'accesso a un sistema informatico o telematico.

[91] Ipotizziamo che l'agente *software* sia programmato in base alle istruzioni seguenti: una volta raggiunto un determinato ammontare di valuta virtuale, ottenuto grazie alle rimesse di vari indirizzi, effettua un numero x di transazione intermedie, e poi restituisci ai destinatari una eguale percentuale di valuta virtuale, indipendentemente dal valore conferito da ciascuno. Un contratto *smart* di questo tipo sarebbe uno strumento formidabile per attribuire a ciascuno dei concorrenti una eguale frazione del capitale illecito, agevolando l'operazione di riciclaggio.

Né potrà affermarsi *sic et simpliciter* la responsabilità di quest'ultimo a titolo di concorso, *ex* artt. 110, 648-*bis* c.p., nel reato di riciclaggio commesso dalle parti che si servono del contratto. La natura *dual-use* del programma informatico rende piuttosto evidente l'assenza di una volontà diretta a fini criminosi. Il *software* potrebbe essere infatti utilizzato anche per scopi leciti, fungendo da strumento di ridistribuzione della ricchezza tra le parti con garanzia di una maggiore riservatezza[92] o di raccolta fondi per scopi benefici.

Più complessa è la questione circa la rilevanza del dolo eventuale di partecipazione, inteso quale accettazione del rischio che terzi utilizzino il programma *dual-use* in operazioni di riciclaggio. La giurisprudenza di legittimità[93] ha seguito un approccio particolarmente rigoroso nel valutare la compatibilità del dolo eventuale con la rappresentazione che il soggetto deve avere al fine di commettere alcuni reati contro il patrimonio[94]. In particolare, nel tracciare una linea distintiva tra il delitto di cui all'art. 648 c.p. e la contravvenzione di cui all'art. 712 c.p., le Suprema Corte ha stabilito che, per la configurabilità del primo, deve potersi affermare che il soggetto attivo non avrebbe desistito dall'acquisto anche nell'ipotesi in cui avesse avuto la certezza della provenienza illecita del bene acquistato, ricevuto o occultato.

Applicando *mutatis mutandis* l'insegnamento delle Sezioni Unite al caso della divulgazione del *software* multifunzionale, pare che per il relativo accertamento sarà necessario vincere la prova di resistenza della formula di Frank. Si dovrà quindi dimostrare che il programmatore avrebbe agito allo stesso modo pur rappresentandosi la certezza dell'utilizzo illecito del programma, *status* psicologico assimilabile alla volontà di contribuire alla condotta riciclativa commessa dagli utenti del servizio.

Come noto, si tratta di un giudizio fattuale rispetto al quale assumono rilevanza i vari "indicatori" fenomenici del dolo eventuale[95]; non è dunque possibile ricostruire in astratto le condizioni in presenza delle quali l'autore di un *criminal smart contract* risponderà a titolo di concorso nel reato commesso dalle parti che fruiscano del programma. L'indagine sulla componente volontaristica si muove su un terreno particolarmente scivoloso, dominato dall'ampia discrezionalità del giudice nella

[92] Il programma non potrebbe del resto essere inquadrato tra quelli "principalmente concepiti o adattati al fine di commettere un reato" (cfr. art. 6 della Convenzione di Budapest). Esso può essere impiegato come strumento di *equity* o di finanziamento all'interno di una organizzazione autonoma decentralizzata o come modalità di ripartizione degli utili in una società che offre servizi di portafoglio virtuale.

[93] Cfr. Cass., Sez. Un., 30 marzo 2010, n. 12433, Nocera, in *Diritto penale contemporaneo*, 20 dicembre 2010, con nota di ABBADESSA G., *Ricettazione e dolo eventuale.*

[94] Secondo la nota formula di Frank la deliberazione di agire nonostante la prospettazione dell'evento collaterale può essere assimilata al dolo soltanto quando è possibile affermare che l'agente avrebbe agito anche nella certezza di produrre il risultato. Tale impostazione presenta il vantaggio di creare un collegamento diretto, benché solo potenziale, tra azione ed evento lesivo. In seno alla giurisprudenza di legittimità si registra un *trend* favorevole all'estensione del principio – inizialmente affermato con riferimento alla rappresentazione della provenienza delittuosa del bene nella ricettazione – anche all'accertamento dell'accettazione del rischio dell'evento collaterale nei reati causalmente orientati. Si veda, sul punto, la celebre sentenza delle Sezioni Unite sul caso ThyssenKrupp (Cass. Pen., Sez. Un., 24 aprile 2014, n. 38343).

[95] Sugli indici fattuali alla stregua dei quali accertare la sussistenza dell'accettazione del rischio si veda la citata sentenza ThyssenKrupp, Cass. Pen., Sez. Un., 24 aprile 2014, n. 38343, 188.

valutazione dei singoli elementi indiziari[96]. Per questo motivo sarebbe forse preferibile prevedere una autonoma fattispecie di reato che punisca la produzione e la diffusione di programmi informatici aventi quale funzione principale il compimento di operazioni di riciclaggio, laddove il *software* sia concretamente ad ostacolare l'individuazione della provenienza delittuosa di beni o altre utilità[97].

4. L'evento in *blockchain* (rinvio)

Nei paragrafi che precedono si è dimostrato come il funzionamento della tecnologia a registro distribuito metta a dura prova il concetto penalistico di azione, che assume connotati ancor più evanescenti di quanto già non lo sia per il fatto di essere collocata nello spazio virtuale. La retroazione del blocco di transazioni e le regole del consenso da una parte[98], e gli agenti contrattuali autonomi dall'altra[99], rendono la condotta dell'uomo soltanto uno dei fattori determinanti l'attività giuridica compiuta sulla rete.

Ad ogni modo le criticità maggiori riguardano il concetto di evento che, nella dimensione virtuale, viene in rilievo come risultato logico-informatico della elaborazione di dati o di alterazione del funzionamento di uno o più sistemi informatici. In un sistema basato su registri distribuiti, in cui ciascun partecipante detiene una copia identica e aggiornata del *database*, l'evento "informatico" si produce simultaneamente in una pluralità luoghi; per quanto la convalida sia imputabile soltanto ai partecipanti che per primi abbiano risolto il dilemma crittografico, il sistema è configurato in modo da rendere unica la catena dei blocchi per tutti i nodi della rete. Ciò rende indubbiamente complesso stabilire quale sia il luogo fisico in cui si è prodotto il risultato della condotta che, per alcuni reati, individua anche il *locus commissi delicti* ai fini dell'applicazione delle norme in tema di competenza e giurisdizione.

Trattandosi di questioni parzialmente coincidenti ci sembra opportuno, oltre che in linea con le esigenze di continenza espositiva, esaminarle congiuntamente.

---

[96] Parte della dottrina ritiene che la tesi avallata dalla giurisprudenza rischi di sconfinare nel c.d. diritto penale d'autore poiché, laddove si tratti di un soggetto pluripregiudicato, la formula di Frank darà più facilmente esito positivo. In argomento, MANNA A., *Colpa cosciente e dolo eventuale: l'indistinto confine ed il principio di stretta legalità*, in *Indice penale*, 2010, 1-2, 9 ss.

[97] La fattispecie potrebbe essere strutturata come reato di pericolo concreto a dolo generico, la cui condotta esecutiva consiste, appunto, nella produzione o nella diffusione di programmi per elaboratore concretamente idonei ad agevolare il trasferimento, la sostituzione, o altre operazioni volte ad ostacolare l'identificazione della provenienza delittuosa di denaro, beni o altre utilità. Sarebbe invece da evitare la previsione di un dolo specifico secondo quanto previsto, ad, es., dall'art. 615-*quinquies* c.p. Se si punisse unicamente la produzione e la diffusione di programmi informatici commessa al fine di favorire il riciclaggio di capitali di provenienza illecita, l'area del penalmente rilevante risulterebbe eccessivamente ristretta, poiché, sul versante probatorio, non sarebbe affatto facile fornire la prova del dolo specifico.

[98] *Supra,* §§ 2.1.2 e seguenti.

[99] *Supra,* § 2.1.5 e § 2.1.6

5. Registri distribuiti e *locus commissi delicti*.

Alcuni autori hanno evidenziato come la rete sia uno straordinario strumento per delocalizzare le risorse e detemporalizzare le attività[100]. L'utente può infatti pianificare le operazioni e fare in modo di effettuarle da remoto, senza necessità di alcun contatto fisico fra persona e sistema informatico. Le attività compiute *online* si disperdono lungo la miriade di sistemi telematici interconnessi, potendo raggiungere in pochi istanti qualunque nodo della rete. Alla tendenziale evanescenza delle condotte criminose commesse nel cyberspazio si accompagna la enorme diffusività del mezzo che, essendo rivolto a un numero indeterminato di persone, può produrre effetti lesivi su larga scala. Un contenuto diffuso mediante Internet è accessibile simultaneamente da migliaia di persone, duplicabile *ad infinitum* e difficilmente eliminabile dalle *query* di ricerca; sono note le esigenze di tutela che scaturiscono da questa nuova realtà panoptica, condensate nel riconoscimento di un personalissimo diritto all'oblio[101].

Del resto, sono ormai note le problematiche connesse alla realizzazione *online* di un fatto costituente reato. Dall'impossibilità di individuare un preciso *locus commissi delicti* deriva una profonda incertezza tanto sulla legge penale applicabile, quanto sulla attribuzione della *potestas iudicandi* all'autorità giudiziaria di uno o di un altro Stato. La dimensione transnazionale del *cybercrime* rende un simile problema tutt'altro che trascurabile, mettendo al contrario in evidenza l'importanza di una adeguata soluzione che garantisca l'effettiva giustiziabilità dei reati informatici[102].

Se si volesse individuare in astratto la causa di questo "disorientamento", lo si potrebbe facilmente ricondurre all'incapacità del principio di territorialità[103] a disciplinare la legge applicabile alle condotte commesse mediate le tecnologie informatiche. Il criterio territoriale di applicazione della legge penale non è in grado di assicurare un legame sufficientemente stretto tra la lesione degli interessi dei cittadini

---

[100] Di quest'avviso, FLOR R., I *limiti del principio di territorialità nel cyberspace*, in *Dir. pen. proc.*, 2015, 10, 1296, secondo cui «*smaterializzazione, velocizzazione, deterritorializzazione, ubiquità e detemporalizzazione coinvolgono le condotte concrete, che prescindono o si distanziano dalla fisicità dei comportamenti o dei fatti esteriori […] capaci di "incorporare" l'accadimento materiale (il danno o il pericolo concreto)*».

[101] FLOR R., *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de iure condendo?*, in *Diritto dell'informazione e dell'informatica*, 2014, 1-2, 775 ss; ID., *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in Diritto penale contemporaneo, 2014, 2, 178 ss.; ID., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention*, in *Ciberspazio e diritto*, 11, 2, 2010, 359 ss.

[102] In alcuni casi i criminali informatici agiscono da Paesi lontani, tecnologicamente arretrati e politicamente instabili, in modo da poter beneficiare dell'impunità; in altri casi i *server* su cui sono registrate le informazioni rilevanti per l'integrazione del reato si trovano *off-shore*, rendendo problematica l'individuazione dei colpevoli e l'acquisizione della *digital evidence*. *Amplius*, in questo capitolo, § 1.1 e nel capitolo V, § 2.

[103] Si veda in tal senso la posizione espressa da FLOR, I *limiti del principio di territorialità nel cyberspace*, cit., 1309

e la perseguibilità nello Stato delle condotte commesse mediante Internet. Un fatto commesso "a distanza" – realizzato interamente all'estero, sia dal punto di vista della condotta, sia dell'evento "informatico" – concretizza spesso una lesione degli interessi del singolo che lo Stato ha interesse a perseguire penalmente.

L'individuazione del luogo di commissione del reato informatico rappresenta la questione in assoluto più delicata dell'intero diritto penale dell'informatica; la giurisprudenza ha affrontato il tema in modo episodico e disorganico, pronunciandosi a più riprese in materia di accesso abusivo a sistema informatico. Prima di passare all'analisi delle criticità più strettamente connesse all'utilizzo della *blockchain* e alla "dispersione" del luogo di commissione del reato in più registri distribuiti, è opportuno rivolgere lo sguardo agli approdi giurisprudenziali più significativi.

5.1. Principio di territorialità, reati informatici e luogo di commissione del reato.

La rete Internet mette in comunicazione utenti collocati in ogni parte del globo. Essa non conosce confini territoriali, mentre gli ordinamenti nazionali necessitano di uno spazio ben delimitato sul quale esercitare la propria sovranità esclusiva.

Il principio di territorialità, sia pur con alcuni temperamenti, è stato recepito all'interno del codice penale per regolare l'applicazione spaziale della legge penale[104]. In base al criterio c.d. dell'ubiquità, il reato si considera commesso nel territorio dello Stato quando l'azione o l'omissione che lo costituisce è ivi avvenuta in tutto o in parte, oppure in esso si è verificato l'evento[105].

Stante la dimensione transnazionale degli illeciti, si dovrà anzitutto stabilire a che condizioni un reato informatico possa considerarsi commesso in Italia. La questione – come si vedrà – risulta quanto mai problematica specialmente in relazione ai reati di

[104] La sovranità territoriale è il criterio a cui si ispira l'art. 3 c.p. secondo cui la legge penale italiana obbliga tutti coloro che, cittadini o stranieri, si trovano nel territorio dello Stato, salve le eccezioni stabilite dal diritto pubblico interno o dal diritto internazionale. Il secondo comma della disposizione introduce un temperamento a tale principio, prevedendo l'applicabilità *ultra fines* della legge penale anche a tutti coloro che, cittadini o stranieri, si trovano all'estero, ma soltanto nei casi stabiliti dalla legge medesima o dal diritto internazionale. Le disposizioni successive disciplinano le eccezioni al principio di territorialità nei casi di reati che offendono interessi primari dello Stato (art. 7, delitti contro la personalità dello Stato, delitti di contraffazione del sigillo e di falsità di monete, delitti commessi da pubblici ufficiali con abuso di poteri o violazione di doveri), di delitti politici commessi all'estero (art. 8), delitti comuni commessi dal cittadino all'estero (art. 9).

[105] La *ratio* di questo criterio è da ravvisarsi nell'interesse dello Stato ad attrarre nella sfera di efficacia della legge penale italiana anche i *reati di transito,* in cui soltanto una mera frazione intermedia della condotta si realizza nel territorio nazionale. In dottrina vi è una disparità di vedute circa l'esatta individuazione del *quantum actionis* sufficiente a radicare nel territorio italiano il luogo di commissione del reato. Secondo una prima linea di pensiero, il riferimento all'azione commessa "in parte" ricomprenderebbe tutti gli atti di esternazione dell'*iter criminis,* anche quelli meramente preparatori; una tesi più restrittiva ritiene che debba essere compiuto almeno un atto esecutivo; altri ancora sostengono che sia necessario il compimento *ex* art. 56 c.p. di atti idonei e diretti in modo non equivoco a commettere il reato. Sul tema si veda MANTOVANI F., *Principi di diritto penale*, Padova, 2002, 441; ANTOLISEI, *Manuale di diritto penale – Parte generale*, cit., 140; PAGLIARO A., (voce) *Legge penale nello spazio,* in *Enc. Dir*., 1973, 1055; GALLO M., *La legge penale (Appunti di diritto penale)*, Torino, 1965, 74.

pura condotta e a quelli in cui l'evento rappresenta il risultato di una elaborazione automatica di dati in forma digitale. A tal riguardo occorre ribadire che, in assenza di una regola specifica, non si potrà che fare riferimento al criterio dell'ubiquità. Ci si dovrà dunque domandare quale sia il luogo fisico in cui si è realizzata, almeno in parte, la condotta o quello in cui si è prodotto l'evento. Si tratta di un interrogativo che chiama in causa non soltanto la questione relativa ai limiti spaziali di applicazione della legge penale (e dunque la *giurisdizione*, tecnicamente intesa) ma anche l'individuazione del giudice nazionale competente. Le disposizioni del codice di procedura penale sulla competenza per territorio operano infatti un coordinamento tra la regola generale del *locus commissi delicti*[106] e le ipotesi particolari, in cui il reato è commesso soltanto in parte in Italia ovvero totalmente all'estero[107].

Ebbene, tanto per la determinazione della giurisdizione quanto per la competenza, si pone il problema di stabilire in modo preciso il *locus commissi delicti*. La peculiarità della rete sta nel fatto che essa è ovunque, ma, al contempo da nessuna parte. L'accesso alle informazioni in essa contenute è possibile da ogni terminale/nodo di accesso, sebbene i dati siano 'fisicamente' registrati su *server* collocati in luoghi diversi (talvolta molto lontani). Si pone quindi il problema di stabilire quale sia il momento rilevante ai fini della individuazione del luogo di commissione del reato (accesso alla rete, accesso al *client server*, accesso allo *storage server*).

È bene precisare fin da ora che la questione non riguarda i reati di evento quali la truffa via *web* (art. 640 c.p.), la frode informatica (art. 640-*ter* c.p.), lo *stalking* (art. 612-*bis*), la diffamazione (art. 595 c.p.) rispetto ai quali la consumazione è legata alla realizzazione del risultato naturalistico della condotta[108]. Parimenti, non sorgono particolari dubbi nei casi in cui il reato informatico sia commesso *offline* (es. accesso

[106] Il primo comma dell'art. 8 del codice di rito dispone che la competenza per territorio sia determinata dal luogo in cui il reato è stato consumato. I vari capoversi della disposizione individuano precisano che, se si tratta di fatto dal quale è derivata la morte di una o più persone, è competente il giudice del luogo in cui è avvenuta l'azione o l'omissione; se si tratta di reato permanente, è competente il giudice del luogo in cui ha avuto inizio la consumazione; se si tratta di delitto tentato, è competente il giudice del luogo in cui è stato compiuto l'ultimo atto diretto a commettere il delitto.

[107] Nel caso in cui il reato sia commesso solo in parte in Italia, ma si è consumato all'estero, il successivo art. 9, comma 1, prevede che la competenza spetti al giudice dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione. I capoversi successivi dettano delle ulteriori regole suppletive nel caso in cui non sia noto l'ultimo luogo in cui è avvenuta una parte dell'azione. Sarà in questo caso competente, successivamente, il giudice della residenza, della dimora o del domicilio dell'imputato. Se nemmeno in tale modo è possibile determinare la competenza, questa appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'articolo 335. Qualora il reato sia commesso interamente all'estero, la competenza è determinata successivamente dal luogo della residenza, della dimora, del domicilio, dell'arresto o della consegna dell'imputato.
In tutti gli altri casi […] la competenza, questa appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'articolo 335. Se il reato è stato commesso in parte all'estero, la competenza è determinata a norma degli articoli 8 e 9.

[108] Che si tratti di reato necessariamente informatico (art. 640-*ter* c.p.) o eventualmente informatico (artt. 640, 612-*bis* c.p.) la realizzazione dell'evento naturalistico di profitto o *lato sensu* di danno segnerà la consumazione del reato e dunque il *locus commissi delicti*.

abusivo a sistema informatico commesso *in loco*), oppure quando la condotta consista in una pura omissione (es. art. 169 D. Lgs. 196/2003 abr.)[109].

Le incertezze maggiori riguardano i reati a evento c.d. informatico, come ad esempio il danneggiamento di dati e programmi informatici (art. 635-*bis* c.p.) o il danneggiamento di sistemi informatici o telematici (art. 635-*quater c*.p.). Talvolta neppure il titolare dei dati o dei sistemi informatici conosce la precisa collocazione geografica delle informazioni o del *server* che le ospita; la diffusione della tecnologia del *cloud computing*[110] e del *software-as-a-service*[111] complica ulteriormente il quadro, rendendo assai complessa l'individuazione del luogo di effettiva verificazione del danno.

La questione riguarda anche i reati di mera condotta commessi *online*, quali l'accesso abusivo a sistema informatico a distanza (art. 615-*ter* c.p.), la diffusione di codici di accesso o di programmi informatici (artt. 615-*quater* e art. 615-*quinquies* c.p.), intercettazione di comunicazioni telematiche (art. 617-*quater* c.p.), nonché le ipotesi di tentativo di commettere un reato di evento realizzato *online* (es. tentativo di truffa o di frode informatica, artt. 56, 640 o 640-*ter* c.p.)[112].

In breve, la questione si pone per quelle fattispecie appartenenti alla categoria dei *cybercrime*[113] che siano prive di evento naturalistico, rispetto ai quali l'utilizzo della rete Internet e la dispersione di informazioni non consente di stabilire quale sia il luogo esatto di consumazione del reato.

5.1.1. Il punto delle Sezioni Unite sul luogo di commissione dell'accesso abusivo a sistema informatico.

[109] Nel primo caso è pacifico che il reato si consuma nel luogo di commissione dell'azione delittuosa, che è lo stesso in cui si trova il sistema informatico. Qualora il reato consista in una pura omissione, il *locus commissi delicti* coinciderà con quello dove si trova il destinatario del precetto alla scadenza del termine per l'adempimento, stante la connotazione personale del dovere di ottemperare all'obbligo imposto dalla legge penale.

[110] Il *cloud computing* è quella tecnologia che consente di usufruire, tramite un *server* remoto, di risorse *software* e *hardware*, gestite, offerte e organizzate da un *provider* remoto, quasi sempre in abbonamento. In sostanza, esso consiste nell'offerta di servizi di calcolo – come *server*, risorse di archiviazione, database, rete, *software*, analisi e altro – tramite la rete Internet.

[111] Il *Software-as-a-Service* (SaaS) è un modello di distribuzione in cui l'applicativo e gli eventuali servizi collegati sono eseguiti in un *server* centrale a cui gli utenti accedono da remoto attraverso la rete Internet, usando un *browser* come interfaccia. Essa offre all'utente il vantaggio di non dover affrontare una spesa impegnativa per l'acquisto del *software*, la sua implementazione e la sua manutenzione. Il *software* in SaaS si utilizza in abbonamento e comporta una spesa inferiore e certa, anche se ricorrente, e la manutenzione è eseguita direttamente dal fornitore del servizio.

[112] Per approfondimenti sulla struttura e sulle tecniche di incriminazione utilizzate per i reati informatici si rinvia al volume di PECORELLA C., *Diritto penale dell'informatica,* cit., 37 ss.

[113] Sulla distinzione tra *computer crime* e *cybercrime,* v. FLOR, *Cyber-criminality: Finding a Balance between Freedom and Security*, cit., 14; CLOUGH J., *Principles of cybercrime*, Cambridge, 2015, 10 ss.

La giurisprudenza nazionale si è occupata del tema in modo episodico[114], soffermandosi in particolare sul luogo di commissione del reato di accesso abusivo a sistema informatico, oggetto di un recente intervento delle Sezioni Unite[115]. L'importanza del *decisum* è dovuto alla latitudine dei principi affermati, che sembrano andare oltre la questione di diritto sottoposta al vaglio della Suprema Corte. Ci sembra dunque opportuno ripercorrere in sintesi l'*iter* argomentativo, prima di passare all'esame dei profili più strettamente connessi alla commissione di un reato in *blockchain*.

Il reato informatico, nella maggior parte dei casi, si realizza a distanza in presenza di un collegamento telematico tra più sistemi informatici con l'introduzione illecita di un soggetto all'interno di un elaboratore, o con l'alterazione del funzionamento dello stesso[116]. Gli approdi ermeneutici più significativi hanno messo in luce due opposte soluzioni che si differenziano nel modo di intendere la spazialità nei reati informatici: per alcune, competente per territorio è il tribunale del luogo nel quale il soggetto si è connesso alla rete effettuando il collegamento abusivo[117]; per altre, il tribunale del luogo ove è fisicamente allocata la banca-dati che costituisce l'oggetto della intrusione[118]. La ordinanza di rimessione alle Sezioni Unite – dopo avere evidenziato

[114] Il tema che ci occupa sembra sfuggire all'attenzione della giurisprudenza e della dottrina, che lo hanno affrontato in modo soltanto parziale, limitatamente ad alcune ipotesi di reato (quali ad esempio la diffamazione telematica e l'accesso abusivo). A nostro modo di vedere, vi sarebbe spazio per una elaborazione coerente e sistematica, che analizzi la questione del luogo di commissione del reato informatico a partire dalla struttura delle singole fattispecie di reato.

[115] Cass. Pen., Sez. Un., 24 aprile 2015, n. 17325, in *Diritto penale contemporaneo*, 11 maggio 2015 con nota di DE MARTINO P., *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico*; in *Diritto penale e processo*, 2015, 10, 1291, con nota di FLOR. R., *I limiti del principio di territorialità nel cyberspace*, cit.; in *Cass. Pen.*, 2015, 10, 3507, con nota di SCIUBA M. L., *Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico*. In dottrina v. anche BELLACOSA M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *Diritto Penale Contemporaneo*, 2 febbraio 2015. La vicenda trae origine dal rinvio a giudizio di una impiegata della Motorizzazione Civile di Napoli e di un amministratore di una agenzia automobilistica imputati *ex* artt. 81, 110, 615-*ter*, commi 2 e 3, c.p per essersi introdotti abusivamente nel sistema informatico del Ministero dei Trasporti, avvalendosi delle credenziali d'accesso dell'imputata, per effettuare visure elettroniche che esulavano dalle mansioni assegnate a quest'ultima. Il G.U.P. del Tribunale di Napoli aveva dichiarato la propria incompetenza per territorio ritenendo competente il Giudice del Tribunale di Roma, in ragione della ubicazione della banca dati della Motorizzazione civile presso il Ministero delle Infrastrutture e dei Trasporti con sede in Roma. Il G.U.P. del Tribunale di Roma aveva sollevato conflitto negativo di competenza per territorio ritenendo che il luogo di consumazione del reato di accesso abusivo ad un sistema informatico dovesse invece radicarsi nel luogo in cui l'operatore aveva agito, ossia a Napoli. La Prima Sezione penale, rilevando un potenziale contrasto di giurisprudenza, ha rimesso gli atti alle Sezioni Unite perché si pronuncino sulla seguente questione: *«Se, ai fini della determinazione della competenza per territorio, il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter c.p., sia quello in cui si trova il soggetto che si introduce nel sistema o, invece, quello nel quale è collocato il server che elabora e controlla le credenziali di autenticazione fornite dall'agente».*

[116] Lo stesso problema si pone per tutti quei reati in cui la condotta del reo si esaurisce nel commettere un'azione online che di per sé costituisce reato (es. diffusione di virus, art. 615-*quinquies* c.p.).

[117] In questo senso era l'orientamento maggioritario, *ex plurimis* Cass. Pen., Sez. III, 15 giugno 2014, n. 34165.

[118] Cfr. Cass. Pen., Sez. I, 27 maggio 2013, n. 40303, Martini, in *Giurisprudenza penale*, 8 novembre 2013, secondo cui il luogo di commissione del reato di cui all'art. 615-*ter* c.p. coincide con quello in cui

che il *client* ed il *server* sono componenti di un unico sistema telematico – osserva che l'accesso penalmente rilevante inizia dalla postazione remota ed il perfezionamento del reato avviene nel luogo ove si trova l'utente, diverso da quello in cui è ubicato il *server*[119]. Secondo l'opinione largamente prevalente il delitto previsto dall'art. 615-*ter* c.p., è di mera condotta e si perfeziona con la semplice violazione del domicilio informatico[120].

In ambito informatico – osservano le Sezioni Unite – deve attribuirsi rilevanza, più che al luogo in cui materialmente si trova il sistema informatico, a quello da cui parte il dialogo elettronico tra i sistemi interconnessi e dove le informazioni vengono trattate dall'utente[121]. Infatti, da un punto di vista tecnico, il sistema telematico deve considerarsi unitario, essendo coordinato da un *software* di gestione che presiede al funzionamento della rete, alla condivisione della banca dati, alla archiviazione delle informazioni, nonché alla distribuzione e all'invio dei dati ai singoli terminali interconnessi. Sarebbe pertanto irragionevole scomporre i singoli componenti dell'architettura di rete, separando i terminali periferici dal *server* centrale, dovendo tutto il sistema essere inteso come *«un 'complesso inscindibile' nel quale le postazioni remote non costituiscono soltanto strumenti passivi di accesso o di interrogazione, ma essi stessi formano parte integrante di un complesso meccanismo, che è strutturato in modo da esaltare la funzione di immissione e di estrazione dei dati da parte del client»*[122]. Ne consegue che il *locus commissi delicti* si identifica con quello in cui è collocata la postazione remota da cui l'agente digita le credenziali di autenticazione e

è allocato il *server*. Ciò che rileverebbe ai fini della integrazione del delitto è il momento in cui si l'agente, interagendo con il sistema informatico o telematico altrui, si introduce in esso contro la volontà di chi ha il diritto di estromettere l'estraneo. Ne deriva che l'accesso si determina nel luogo ove viene effettivamente superata la protezione informatica e si verifica la introduzione nel sistema e, quindi, dove è materialmente situato il server violato, l'elaboratore che controlla le credenziali di autenticazione del client. Già in precedenza la S.C. aveva affermato un principio simile con riferimento al reato di frode informatica. Si veda, Cass. Pen., sez. III, 24 maggio 2012, n. 23798, Casalini, in *Diritto penale contemporaneo*, 2 luglio 2013 con nota di TRIPODI A.F., *La Cassazione alla prova dello spamming, tra presunzione e torsioni*, secondo cui la competenza territoriale deve essere individuata nel luogo in cui si trova il *server* all'interno del quale sono archiviati i dati oggetto di abusivo trattamento.

[119] Il terminale mediante il quale l'operatore materialmente inserisce *username* e *password* è ricompreso, quale elemento strutturale ed essenziale, nell'intera rete di trattamento e di elaborazione dei dati, assumendo rilevanza il luogo di ubicazione della postazione con cui l'utente accede o si introduce nel sistema che contiene l'archivio informatico.

[120] Non si pone dunque il problema di individuare il luogo di realizzazione dell'evento, che avrebbe verosimilmente condotto a conclusioni differenti in punto di luogo di consumazione del reato. In argomento FLOR, *I limiti del principio di territorialità nel cyberspace*, cit., 1300.

[121] Cass. Pen., Sez. Un., 24 aprile 2015, n. 17325, cit., § 4. Se si articolasse la competenza secondo i comuni criteri fisico-spaziali, non si terrebbe conto del fatto che la nozione di collocazione materiale è essenzialmente estranea alla circolazione dei dati in una rete di comunicazione telematica e alla loro contemporanea consultazione da più utenti spazialmente diffusi sul territorio. Sarebbe dunque erroneo ritenere che i dati si trovino soltanto nel *server*, dal momento che la banca-dati è contestualmente compresente e consultabile in condizioni di parità presso tutte le postazioni remote autorizzate all'accesso. A dimostrazione della unicità del sistema telematico, l'estensore rileva che la traccia delle operazioni compiute all'interno della rete e le informazioni relative agli accessi sono reperibili, in tutto o in parte, sia presso il *server* che presso il *client*.

[122] In questi termini si esprimono le Sezioni Unite, § 4.2 del considerato in diritto.

preme il testo di avvio[123], ponendo così in essere l'unica azione materiale e volontaria che lo pone in condizione di entrare nel dominio delle informazioni che vengono visionate direttamente all'interno della postazione periferica.

5.1.2. Rilievi critici. Le questioni irrisolte sul luogo di commissione del reato informatico.

La sentenza delle Sezioni Unite lascia molti punti insoluti, che avrebbero forse meritato un esame più approfondito. L'esito decisorio sembra motivato da comprensibili esigenze di carattere pratico, tra cui quella di evitare l'accentramento della competenza nei luoghi in cui sono collocati i *server* centrali, ma non pare risolutivo delle questioni più spinose che si pongono con riferimento al luogo di commissione del reato informatico. Le argomentazioni sembrano basarsi sul recepimento di una *fictio giuridica*; l'individuazione del luogo di accesso nella postazione della persona fisica che agisce da remoto non pare infatti conciliabile con il funzionamento tecnico-informatico del protocollo di comunicazione *client-server.* Un tale protocollo si basa su una infrastruttura centralizzata – e non già unitaria o decentralizzata come ritiene la Corte. A stretto rigore l'accesso si realizza nel luogo in cui le informazioni o il domicilio virtuale si trovano, e non in quello di partenza della richiesta di 'interrogazione' del *database*.

Desta peraltro stupore l'affermazione secondo cui, qualora sia impossibile individuare il luogo in cui è collocato il *client*, la competenza sarà fissata in base alle regole suppletive dettate dal codice di procedura penale[124]. Non si può infatti escludere che il nodo periferico della rete dal quale il soggetto ha agito si trovi all'estero, circostanza che, a seconda del titolo di reato considerato, renderebbe il fatto non punibile in Italia, ovvero procedibile soltanto a richiesta del ministro della Giustizia[125].

Appaiono del resto evidenti i possibili "effetti collaterali" del *dictum* delle Sezioni Unite in una materia caratterizzata dalla transnazionalità degli illeciti. L'autore dell'attacco informatico potrebbe infatti strumentalizzare il regime attenuato di procedibilità[126] per scegliere il Paese da cui far partire l'attacco. Si incentiverebbe così

[123] In caso di mantenimento abusivo nel sistema (condotta di tipo omissivo) non assume rilevanza, ai fini della commissione del reato, l'azione con la quale l'agente accede al sistema digitando le credenziali, condotta da ritenersi inizialmente lecita. Si dovrà pertanto considerare l'inizio della condotta omissiva che coincide con un uso illecito dello elaboratore. Varranno dunque gli stessi principi affermati con riferimento alla condotta commissiva, poiché l'operatore remoto, anche in questo caso, si relaziona, con impulsi elettronici e colloquia con il sistema dalla sua postazione periferica.

[124] La possibilità di individuare il luogo preciso dell'accesso (terminale o postazione periferica) non è la regola, bensì l'eccezione, specialmente quando il soggetto abbia commesso il fatto mediante l'uso di dispositivi mobili o di *browser* anonimi. In buona sostanza, c'è il rischio che le regole suppletive di determinazione della competenza diventino il criterio principale, anziché quello sussidiario.

[125] La disciplina è in parte differente a seconda che si tratti di delitto comune commesso dal cittadino o dallo straniero all'estero (Cfr. artt. 9 e 10 c.p.).

[126] Il delitto comune commesso all'estero, diversamente da quanto è previsto per i delitti politamente orientati, è punibile in Italia a condizione che il colpevole si trovi nel territorio dello Stato.

la prassi, peraltro già diffusa, di lanciare attacchi da Paesi tecnologicamente arretrati e politicamente deboli (c.d. paradisi cibernetici)[127].

Il ragionamento giuridico facente leva sul concetto "unitario" di rete telematica sembrerebbe, a prima vista, estensibile a tutte le ipotesi di reato informatico commesse *online*; il *locus* di consumazione dei reati di mera condotta andrebbe così individuato nella postazione remota da cui il colpevole ha agito[128]. Occorre tuttavia tenere distinte alcune ipotesi particolari, che fuoriescono dallo schema delineato dalla Corte.

Anzitutto, quelle in cui la commissione di un reato *online* prescinde dall'accesso ad un sistema informatico e presuppone una relazione tra utenti (e non tra sistemi informatici)[129]. Qui il principio di diritto delineato dalle Sezioni Unite non può operare perché la comunicazione, consistendo in un transito intersoggettivo di informazioni, non si esaurisce nella sola attività posta in essere dal terminale di partenza, ma richiede piuttosto che il messaggio giunga al destinatario (diversamente ricorrerebbero soltanto gli estremi del tentativo)[130].

A voler essere coerenti con le statuizioni della Corte, si dovrebbe valorizzare il luogo in cui il destinatario ha preso conoscenza del messaggio. L'affermata unitarietà della rete consente infatti di affermare che la conoscenza si ha nel luogo in cui il ricevente digita la *password* di accesso alla propria casella di posta, e non già nel luogo in cui si trova il *server* del gestore di posta elettronica.

Vi sono poi quelle fattispecie caratterizzate da un intervento senza diritto su dati e informazioni che provocano una alterazione del *software* (art. 635-*bis* c.p.)[131] o un

---

[127] Sul tema v. FLOR, *I limiti del principio di territorialità nel cyberspace,* cit., 1308

[128] Nel reato di interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater*) l'utente viene a contatto con il sistema informatico, poiché ne altera il funzionamento in modo da impedire la comunicazione con l'esterno. Si potrebbe dedurre, in linea con le argomentazioni delle Sezioni Unite, che il luogo di commissione del reato è quello in cui si trova il *client* che, da remoto, interrompe la comunicazione (si pensi a un attacco c.d. di DNS *poisoning*).

[129] Si pensi al caso in cui un utente comunichi o consegni via mail il codice di accesso a un sistema informatico altrui, fatto riconducibile al reato di cui all'art. 615-*quater* c.p.

[130] Vi sono poi quei casi in cui l'*iter criminis* è frazionabile in più momenti successivi, in cui l'informazione 'viaggia' sui *server* gestiti dai *provider*. L'invio per posta elettronica di un codice di accesso a sistema informatico (art. 615-*quater* c.p.) lascia intravedere almeno quattro 'aspiranti' luoghi di commissione del reato: quello in cui si trova la postazione dell'agente che fa partire la comunicazione abusiva; quello in cui si trova il *server* del gestore del servizio di posta elettronica del reo, atteso che prima che ciò accada l'azione criminosa non potrebbe dirsi compiuta; il luogo in cui si trova il *server* del *provider* del destinatario del messaggio di posta elettronica, poiché è soltanto con la ricezione del messaggio che il reato potrebbe dirsi perfetto (recettizietà della comunicazione); luogo in cui si trova la persona fisica destinataria del messaggio, atteso che la recettizietà non deve intendersi in astratto come conoscenza legale, ma come conoscenza effettiva. In questi casi *borderline* l'individuazione del luogo di commissione del reato dipenderà dalla struttura della fattispecie di reato e, in particolare, dal momento consumativo individuato. In ogni caso, la tesi delle Sezioni Unite del sistema informatico 'unitario', che abbraccia anche le articolazioni periferiche della rete, non pare suscettibile di applicazione con riferimento alla condotta dell'agente. Sarebbe infatti arduo (oltre che tecnicamente errato) sostenere che il mittente di un messaggio di posta elettronica si connette al sistema informatico del (*provider* di posta del) destinatario direttamente dalla postazione fisica in cui si trova.

[131] Sul danneggiamento informatico, per la formulazione della norma precedente all'entrata in vigore della legge n. 48/2008 v. PECORELLA, *Diritto penale dell'informatica*, cit., 179 ss; più di recente, all'indomani della riforma, SALVADORI I., *Il microsistema normativo concernente i danneggiamenti*

ostacolo al funzionamento dell'*hardware* (art. 635-*quater* c.p.). La presenza di un evento di tipo logico-informatico fa venir meno la possibilità di individuare il *locus* di commissione del reato nella postazione remota dell'agente, radicando la competenza là dove i dati o i sistemi sono allocati. Tenuto conto che, nella maggioranza dei casi, questi ultimi si trovano in territorio straniero[132], si ripropongono le perplessità sul regime di procedibilità attenuata degli illeciti, condizionata alla presenza del colpevole sul territorio italiano e alla richiesta del ministro della Giustizia.

5.2. L'ubiquità nell'infrastruttura. Problematiche relative all'individuazione del luogo di commissione del reato in *blockchain*.

Nel prendere posizione a favore dell'orientamento maggioritario, le Sezioni Unite tratteggiano un concetto unitario di rete che permette di superare – quantomeno ai fini della individuazione del *locus commissi delicti* – la distinzione di natura informatica tra *client* e *server*. Ma *quid iuris* nel caso in cui l'illecito sia commesso su una infrastruttura che utilizza un differente protocollo di comunicazione? Ci si domanda, in particolare, se l'utilizzo di una rete *peer-to-peer* possa assumere una qualche rilevanza ai fini della individuazione del luogo del commesso reato. La questione andrà esaminata con riferimento ad alcune condotte illecite commesse mediante la DLT, in cui la tenuta distribuita del registro non permette, a differenza dei comuni sistemi centralizzati, di individuare un luogo preciso di allocazione delle risorse e delle informazioni. Per dare maggiore concretezza alle riflessioni di seguito svolte, ci sembra utile ricorrere a due esempi pratici: da un lato l'invio di una somma di denaro di provenienza illecita da un mittente a un destinatario, operazione che integra gli estremi del delitto di riciclaggio (art. 648-*bis* c.p.); dall'altro la cancellazione dei dati registrati nella catena dei blocchi, fatto sussumibile nel reato di cui all'art. 635-*bis* c.p.

Nel primo caso si tratta di un reato di mera condotta[133], che si consuma con il compimento dell'operazione, purché questa sia idonea ad ostacolare l'individuazione della provenienza delittuosa dei valori trasferiti[134]. Il luogo del commesso reato potrebbe coincidere con quello da cui il mittente, utilizzando le chiavi private di criptazione, invia l'*input* di transazione alla rete decentralizzata. In questa fase l'*iter*

informatici. Un bilancio molto poco esaltante, in *Rivista italiana di diritto e procedura penale*, 2012, 1, 204 ss.

[132] Per approfondimenti sulla collocazione dei *server* nel mondo, in mancanza di statistiche precise, si rinvia alle notizie di cronaca, v. COSIMI S., *I data center nel mondo*, in Repubblica.it, 06 ottobre 2015.

[133] Non è infatti necessario che l'ostacolo all'identificazione della provenienza delittuosa delle utilità sia effettivo o che la condotta cagioni un evento tale da crearlo. Il riciclaggio non è reato di evento, bensì di mera condotta, più precisamente di "condotta pericolosa". In argomento, ZANCHETTI, *Il riciclaggio di denaro proveniente da reato*, cit., 365; MANGIONE A., *Mercati finanziari e criminalità organizzata: spunti problematici sui recenti interventi normativi di contrasto al riciclaggio*, in *Rivista italiana di diritto e procedura penale*, 2000, 3, 1136.

[134] Cionondimeno, l'accertamento della idoneità della condotta a provocare il pericolo è reso piuttosto complesso dalla possibilità di omessa convalida e caducazione del blocco. Per approfondimenti v. *supra*, § 2.1.2.

criminis non può tuttavia dirsi compiuto, almeno fintanto che la richiesta non viene validata e inserita nel blocco. Come noto, la verifica della transazione avviene in modo casuale ad opera del *miner* che primo sia riuscito a risolvere una equazione matematica predefinita. Il destinatario dell'accredito viene immesso nel possesso dei valori virtuali non appena si chiude la fase di validazione, ma per poter "spendere" la provvista ricevuta è necessario attendere un certo numero di conferme. Si delineano così una pluralità di possibili luoghi di commissione del reato[135], dal quale discendono, sul versante giudiziale, non poche incertezze sulla competenza territoriale.

A nostro modo di vedere, il *locus commissi delicti* dovrebbe coincidere con quello in cui si trova il mittente al momento di inoltro dell'ordine di pagamento. Il riciclaggio è un reato istantaneo e di mera condotta, che si consuma nel luogo in cui è compiuta l'operazione. Vero è che, da un punto di vista tecnico-informatico, il processo di validazione della transazione si articola lungo i nodi dell'infrastruttura decentralizzata, ma si tratta di attività automatiche che sfuggono al *dominium* dell'uomo[136]. La soluzione ci sembra peraltro in linea con la concezione "unitaria" della rete elaborata dalle Sezioni Unite[137]. Se si attribuisce rilevanza centrale alla condotta dell'uomo, non vi è alcuna differenza nel fatto che il dialogo informatico sia instaurato con una infrastruttura decentralizzata anziché con un *server* centrale. In entrambi i casi l'utente si collega al sistema dalla propria postazione, ponendo in essere la condotta 'umana' penalmente rilevante attraverso il proprio elaboratore.

In risposta al quesito formulato in apertura del paragrafo possiamo pertanto concludere che il protocollo di comunicazione utilizzato per accedere alle risorse informatiche – sia esso basato sul modello *client-server* (C2S) ovvero *peer-to-peer*

[135] Ragionando per ipotesi, potrebbero alternativamente individuarsi almeno quattro luoghi di commissione del reato a seconda di dove si trova: (i) la postazione remota del mittente, poiché secondo la concezione "unitaria" dalla diramazione periferica della rete egli si connette direttamente all'infrastruttura decentralizzata; (ii) il computer (*mining rig*) che per primo ha validato la transazione, tenuto conto che, prima della verifica, la condotta rimane allo stadio del tentativo; (iii) la postazione remota del destinatario delle somme, dal momento che il requisito dell'idoneità dell'ostacolo all'individuazione della provenienza illecita potrebbe sussistere unicamente nella misura in cui il denaro sporco sia immesso nella disponibilità di terzi; (iv) il nodo della rete che ha inviato l'ultima conferma necessaria a "svincolare" la somma e renderla spendibile per il destinatario, non essendovi, fino a quel momento, alcun pericolo di ulteriore dispersione delle somme.

[136] Non sarebbe del resto possibile ritenere che il reato sia consumato nel luogo in cui si trova il destinatario delle somme, poiché, per consolidata giurisprudenza, costituisce condotta idonea alla integrazione della fattispecie criminosa anche la sola disponibilità del soggetto a ricevere sul proprio conto beni di origine illecita, anche se i valori non sono poi stati ricevuti o utilizzati (Cass. Pen., Sez. VI, 6 aprile 2011, n. 26746). Saranno quindi attratti alla giurisdizione italiana tutti i fatti di *cyberlaundering* commessi da soggetti che agiscono dall'Italia. Si potrebbe invece discutere sull'applicabilità della legge penale italiana al riciclaggio commesso all'estero, laddove i fondi siano stati ricevuti da un soggetto presente sul territorio dello Stato. In tal caso non sarebbe corretto ritenere che il reato è commesso anche solo 'in parte' in Italia, poiché, se si avvalora la tesi della consumazione istantanea del delitto, la ricezione dei valori virtuali da parte del destinatario dovrebbe essere considerata un *post factum* non rilevante ai fini della individuazione del *locus commissi delicti.* Sarà pertanto necessaria la richiesta del ministro della Giustizia (artt. 9 e 10 c.p.), condizione sufficiente a rendere punibile il reato in Italia se il soggetto si trova nel territorio dello Stato.

[137] Cass. Pen., Sez. Un., 24 aprile 2015, n. 17325, *amplius* § 2.2.2.

(P2P) – non assume alcuna rilevanza ai fini della individuazione del luogo di commissione di reati di mera condotta[138].

La questione diviene indubbiamente più complessa in relazione ai reati di evento. Laddove la fattispecie sia costruita attorno alla verificazione di un *exitus* di carattere tecnico-informatico, per determinare il foro competente si dovrebbe aver riguardo al luogo di produzione del danno. In questo caso la delocalizzazione delle risorse sulla *blockchain* è un fattore di evidente complicazione. Nel caso addotto come esempio il soggetto riesce a cancellare i dati iscritti sul registro pubblico sfruttando una falla nel sistema di sicurezza; la cancellazione di dati informatici[139] figura tra le condotte esecutive del delitto di danneggiamento di cui all'art. 635-*bis* c.p., comunemente ritenuto un reato di evento. Benché l'azione delittuosa sia commessa a danno di un singolo insieme di dati[140], l'aggiornamento simultaneo dei registri distribuiti propagherà l'effetto lungo tutti i nodi del sistema; si avranno pertanto tanti "eventi", quanti sono gli elaboratori che compongono l'infrastruttura. In tal caso per l'individuazione del luogo del commesso reato possono delinearsi due alternative: da una parte quella di accettare la natura ubiquitaria del danneggiamento commesso a danno di dati inseriti in un sistema telematico di registri distribuiti, considerando un evento autonomo l'alterazione di ogni singolo registro; dall'altra quella di ritenere evento in senso tecnico giuridico soltanto l'alterazione dei dati registrati sul *computer* bersaglio dell'attacco. Aderendo alla prima soluzione si determinerebbe una pluralità di *loci commissi delicti*, che, sul piano giudiziale, darebbe luogo a una significativa estensione della competenza per territorio[141]; se si propendesse per la seconda, si opererebbe una *reductio ad unitatem* del luogo del commesso reato, con difficoltà notevoli circa la sua precisa individuazione[142].

5.3. Registri distribuiti e disciplina della continuazione *ex* art. 81 c.p.

Per un corretto inquadramento del problema si deve anzitutto chiarire se la cancellazione o l'alterazione di dati informatici registrati in *blockchain* integri un fatto di reato unico ovvero una pluralità di reati uniti dal vincolo del concorso formale

[138] Parimenti, il tentativo di commettere un reato di evento – ad esempio un danneggiamento informatico – si intenderà realizzato nel luogo in cui si trova il soggetto che, da remoto, fruisce delle risorse di rete per commettere un fatto penalmente rilevante (v. *infra*).

[139] SALVADORI, *Il microsistema normativo concernente i danneggiamenti informatici,* cit., 210

[140] Il soggetto agente potrebbe prendere di mira una specifica articolazione periferica della rete, sfruttando il protocollo di aggiornamento simultaneo per amplificare gli effetti lesivi dell'alterazione del registro.

[141] Se due o più nodi della rete si trovano all'interno del territorio dello Stato, si determinerebbe una pluralità di fori competenti e dunque la necessità di un coordinamento nell'esercizio dell'azione penale da parte delle divisioni distrettuali della Procura della Repubblica specializzate nei reati informatici. Anche nei rapporti tra le giurisdizioni di più Stati sarebbe necessario un coordinamento delle iniziativ3

[142] Il simultaneo aggiornamento dei registri rende piuttosto complesso stabilire quale sia il database alterato per primo; anche laddove ciò sia possibile, l'accertamento presupporrà il necessario passaggio per una indagine tecnico-informatica.

omogeneo (art. 81, comma 1, c.p.). La propagazione degli effetti dannosi non dipende da una azione ulteriore dell'agente, ma piuttosto dalla particolare conformazione della infrastruttura. Il protocollo di base è infatti impostato in modo tale da garantire la decentralizzazione su basi crittografiche e il simultaneo aggiornamento[143] del registro detenuto da ciascun partecipante. Se, da una parte, ciò farebbe propendere per la tesi dell'unicità del reato, dall'altra non si può non considerare come l'evento di danno riguardi più sistemi informatici tra loro collegati.

A ben vedere, la "perdita" dei dati si realizza presso ciascuna articolazione periferica della rete nel momento stesso in cui l'elaboratore colpito dall'attacco fornisce una copia "alterata" del registro[144]. Dal punto di vista oggettivo si realizzano dunque tanti eventi di danno quanti sono gli elaboratori che compongono l'infrastruttura. È del resto assai verosimile che la produzione di un effetto "a catena" trovi pieno riscontro nelle intenzioni del soggetto, che agisce nella consapevolezza dell'interconnessione tra i registri e della estensione "sistemica" degli effetti dannosi.

Tali rilievi portano a ritenere preferibile la tesi del concorso formale omogeneo; l'autore dell'attacco informatico risponderà dunque della pena prevista dall'art. 635-*bis* c.p. aumentata fino al triplo[145].

Sul versante processuale ricorrerà una ipotesi di connessione *ex* art. 12, comma 1, lett. b)[146] che renderà applicabile la disposizione sulla competenza per territorio determinata dalla connessione (art. 16 c.p.p.). I criteri dettati per l'individuazione del giudice territorialmente competente[147] non paiono tuttavia risolutivi nel caso in esame. Trattandosi di violazioni della medesima disposizione di legge, non è possibile individuare un reato più grave; la simultaneità nella verificazione degli eventi dannosi rende tendenzialmente inapplicabile anche il criterio di priorità temporale, che potrà essere invocato soltanto nel caso in cui sia nota la sorgente dei dati oggetto di alterazione. Diversamente si dovrà ricorrere alle regole suppletive, che attribuiscono la competenza al giudice dell'ultimo luogo in cui è avvenuta una parte dell'azione o

[143] Si veda al riguardo la definizione fornita dalla recente novella legislativa (art. 8-*ter*, D.L. 14 dicembre 2018 n. 135), sulla quale *amplius*, Cap. I, § 3.1.

[144] Per esemplificare abbiamo dato per assunto che la cancellazione di un dato nei registri periferici sia in grado di modificare il *public ledger* e le copie detenute dagli altri partecipanti della rete. Si tratta naturalmente di una ipotesi che potrebbe sortire eccezioni in base alle istruzioni di codifica di ciascuna infrastruttura.

[145] Resta comunque fermo il limite posto dal terzo comma dell'art. 81, per cui la pena non potrà essere superiore a quella che sarebbe applicabile sulla base del regime ordinario del concorso materiale. Si applicherà il cumulo giuridico delle pene anche nel caso in cui il fatto sia stato commesso con più azioni, anche in tempi diversi, unite dal vincolo della continuazione.

[146] Segnatamente, il caso in cui una persona è imputata di più reati commessi con una sola azione od omissione ovvero con più azioni od omissioni esecutive di un medesimo disegno criminoso.

[147] Ai sensi del primo comma dell'art. 16 del codice di rito penale la competenza per territorio per i procedimenti connessi rispetto ai quali più giudici sono ugualmente competenti appartiene al giudice competente per il reato più grave e, in caso di pari gravità, al giudice competente per il primo reato.

dell'omissione ovvero, successivamente, al giudice della residenza, della dimora o del domicilio dell'imputato[148].

5.4. Registri distribuiti e *tempus commissi delicti*.

Nel trattare in generale delle peculiarità legate alla commissione di un reato in un ambiente virtuale disintermediato, non potremmo non considerare la questione del *tempus commissi delicti*. Come noto, la registrazione di un dato sulla *blockchain* assicura la certezza della data (c.d. marca temporale) e, a determinate condizioni, la immodificabilità della stessa. Si tratta di una delle caratteristiche di maggior pregio della tecnologia a registro distribuito, tanto che il legislatore vi ha fatti espresso riferimento nella recente legge di conversione del "decreto semplificazioni"[149].

Occorre fin da subito precisare che il tema della validazione temporale elettronica di determinati atti e documenti è tutt'altro che nuovo nella scienza giuridica italiana[150]. Prima dell'entrata in vigore del decreto di riforma[151], il Codice dell'Amministrazione Digitale definiva la validazione temporale come «il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi»[152]. La materia è oggi disciplinata dal Regolamento 910/2014/UE che, in un'ottica di armonizzazione delle legislazioni nazionali, individua i requisiti e gli effetti giuridici della validazione temporale elettronica[153]. A corredo

[148] Se nemmeno in tale modo è possibile determinare la competenza, questa appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'articolo 335 (cfr. art. 9, comma 3, c.p.p.).

[149] In particolare gli ultimi due commi dell'art. 8-*ter* del D.L. 14 dicembre 2018 n. 135, convertito con emendamenti dalla legge 11 febbraio 2019 n. 12 secondo cui «*la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica»*, purché siano rispettati standard tecnici dettati dall'Agenzia per l'Italia Digitale.

[150] In argomento, senza pretese di esaustività, SIGNORELLI A., *Il valore giuridico del documento informatico*, in *Il processo telematico*, 15 marzo 2019; RODRIGUEZ AYUSO J. F., *Verso il raggiungimento di un mercato unico interno in materia di transazioni elettroniche. Il nuovo regolamento europeo 910/2014*, in federalismi.it, 2017, 24, 25 ss.; CONTALDO A., GORGA M., *Le novità della disciplina del Processo Civile Telematico (PTC) anche con riguardo alla recente disciplina del Codice dell'Amministrazione Digitale (CAD)*, in *Rassegna dell'Avvocatura dello Stato*, 2016, 4, 166 ss.; CHIBBARO S. BECHINI U., *Dal documento all'evento: bollo e documento informatico*, in *Rivista del notariato*, 2013, 2, 273 ss.; NAVONE G., *La data del documento informatico: osservazioni in materia di validazione temporale*, in *Obbligazioni e contratti*, 2009, 4, 364 ss.

[151] Si richiama la riforma da ultimo operata con D. Lgs. 26 agosto 2016, n. 179, recante «modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche».

[152] Art. 1, comma 1, lett. bb), D. Lgs. 7 marzo 2005, n. 82, abrogata dall'art. 1, comma 1, lett. h) del D. Lgs. 26 agosto 2016, n. 179. Il successivo art. 20, comma 3, specificava il valore legale della marcatura temporale, sancendo l'opponibilità a terzi della data e dell'ora di formazione del documento informatico redatto in conformità alle regole tecniche sulla validazione temporale (periodo oggi abrogato dal D. Lgs.13 dicembre 2017, n. 217).

[153] Circa gli effetti giuridici della validazione temporale il Regolamento prevede che ad essa «non possano essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali». Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora,

della normativa civilistica, il legislatore ha avvertito l'esigenza di tutelare penalmente l'efficacia probatoria del documento informatico, introducendo alcune disposizioni a tutela del patrimonio[154] e della fede pubblica informatica[155].

Del tutto estranea alla logica penalistica è invece la presunzione di certezza della data e del contenuto del documento informatico, che le leggi civili ricollegano alla validazione elettronica. Se si volesse esaminare la questione dalla prospettiva dell'accertamento giudiziale, ci si renderebbe immediatamente conto delle profonde differenze che intercorrono tra il processo civile e quello penale. L'adozione del modello accusatorio ha reso il processo penale assolutamente impermeabile a qualunque forma di presunzione legale, di talché ogni prova, salvo eccezioni, dovrà essere formata nel contradditorio delle parti. Risulta pertanto evidente come la registrazione di una transazione sui registri distribuiti costituirà – laddove acquisita nelle forme rituali[156] – alla stregua di ogni altro documento, una prova liberamente valutabile da parte del giudice.

Mettendo ora da parte le questioni più strettamente processuali, ci chiediamo se la registrazione in *blockchain* di una transazione illecita possa valere ad individuare in modo certo il *tempus commissi delicti*[157]. Dottrina[158] e giurisprudenza[159] concordano

---

e di integrità dei dati ai quali tale data e ora sono associate. A tal fine è necessario che il dispositivo o la procedura informatica assicurino il rispetto di alcuni requisiti tra cui: il collegamento della data al contenuto del documento in modo da escludere la possibilità di modifiche non rilevabili dei dati; l'utilizzo di una unità di misura del tempo UTC; l'apposizione mediante firma elettronica avanzata con un sigillo elettronico avanzato del prestatore di servizi fiduciari. Cfr. artt. 41 e 42 Regolamento 910/2014/UE.

[154] Si veda l'art. 640-*quinquies* c.p. che punisce la condotta del prestatore di servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. In dottrina sul tema v. MINICUCCI G. *Le frodi informatiche*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 827 ss.; SCOLETTA M, *Il nuovo regime penale delle falsità informatiche*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, 28; PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa – Profili sostanziali*, in *Dir. pen. proc.*, 2008, 6, 701.

[155] Sulla tutela penale delle falsità informatiche e, in particolare, sulla tutela apprestata dall'art. 491-*bis* c.p. si vedano SALCUNI G., *Le falsità informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA, *Cybercrime*, cit., 273 ss.; RESTA F., *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, in *Giur. merito*, 2008, 2147 ss.; CAUTERUCCIO R., *I nuovi reati contro la fede pubblica: il falso in documento informatico pubblico o privato*, in *Rivista penale*, 2007, 965; CORVINO G., La tutela penale del documento informatico, in PLANTAMURA V., MANNA A., *Diritto penale e informatica*, Bari, 2007, 26; GROTTO M., *Regime giuridico del falso informatico dubbi sulla funzione interpretativa dell'art. 491 bis c.p.*, in *Dir. Inf.*, 2006, 589.

[156] Cfr. artt. 234 e 234-*bis* c.p.p., che disciplinano, rispettivamente, la prova documentale e l'acquisizione di dati e documenti informatici.

[157] Ci si riferisce in particolare a quei casi in cui il trasferimento di dati integri di per sé reato (c.d. reato-transazione).

[158] Sul tema di recente v. FIORELLA A., *Le strutture del diritto penale*, Torino, 2018, 156 ss.; MANTOVANI F., *Diritto penale – Parte generale*, Padova, 2017, 93 ss.

[159] Da ultimo, Cass. Pen. Sez. Un., 19 luglio 2018 n. 40896, in *Diritto penale contemporaneo*, 4 ottobre 2018, con nota di ZIRULIA S., *Le Sezioni Unite sul tempus commissi delicti nei reati c.d. ad evento differito*. Le Sezioni Unite non rinvengono nel codice penale alcuna disposizione che funga da guida all'interprete nel ritrovare una definizione unitaria del *tempus*. Tale non potrebbe essere l'art. 6, comma 2, c.p. che – come si è visto – fa coincidere la commissione del reato con il verificarsi nel territorio

nell'affermare che il tempo di commissione del reato non possa essere declinato in termini generali, ma vada piuttosto riferito ai singoli istituti e ricostruito sulla base della *ratio* di ciascuno di essi e dei principi che li governano. In mancanza di una regola generale si tende a fornire una interpretazione che faccia prevalere, a seconda dei casi, il criterio della condotta o quello dell'evento[160]. Tanto premesso, appare evidente come l'efficacia di validazione temporale (*time-stamp*) tipica della tecnologia a registro distribuito non sia suscettibile di individuare in modo univoco il *tempus* di commissione del reato.

Si pensi al caso di una frode informatica (art. 640-*ter* c.p.) commessa mediante l'alterazione delle istruzioni di uno *smart contract*. Ipotizziamo che il soggetto riesca a modificare il funzionamento del programma inserendo il proprio indirizzo al posto di quello del creditore di una somma di valuta virtuale; il reato si perfezionerà con il conseguimento del profitto, nel momento in cui, avveratesi le condizioni, l'agente *software* eseguirà la prestazione in esso dedotta. Supponiamo che il fatto sia stato commesso con indebito utilizzo dell'identità digitale[161] (abuso delle credenziali di autenticazione) prima dell'entrata in vigore del D.L. 14 agosto 2013, n. 933, ma che le condizioni o il termine si avverino dopo alcuni anni; il reato si perfeziona con la realizzazione del profitto e del corrispettivo danno per effetto dell'atto di disposizione posto in essere dal programma informatico. Se si facesse coincidere il *tempus commissi delicti* con la data in cui fu eseguita la prestazione, facilmente ricavabile dalla lettura del registro delle transazioni, si dovrebbe concludere per l'applicabilità del più grave regime sanzionatorio previsto dal terzo comma dell'art. 640-*ter*. Sennonché, sulla scorta del recente insegnamento delle Sezioni Unite, per l'individuazione del tempo del commesso reato sembrerebbe doversi accordare prevalenza al criterio della condotta tutte le volte in cui da esso dipenda l'applicazione al caso concreto di una disciplina punitiva più favorevole al reo (art. 2, comma 4, c.p.)[162].

---

stesso, alternativamente, della condotta o dell'evento. L'equivalenza ai fini dell'art. 6 del criterio della condotta e del criterio dell'evento rende ragione dell'inidoneità di detta disciplina a fissare il *tempus commissi delicti*, posto che l'individuazione dovrebbe essere univoca.

[160] Così, ad esempio, ai fini della successione di leggi penali nel tempo o della sospensione condizionale della pena prevarrà il primo, ai fini della decorrenza del termine di prescrizione il secondo.

[161] L'art. 9, comma 1, lett. a), del D.L. 14 agosto 2013, n. 933, convertito, con modificazioni, dalla L. 15 ottobre 2013, n. 119, ha introdotto il terzo comma dell'art. 640-*ter* c.p. che prevede una circostanza aggravante a effetto speciale *«se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti»*.

[162] Cass. Pen. Sez. Un., 19 luglio 2018 n. 40896, cit., § 6. Nel caso sottoposto al vaglio delle Sezioni Unite, il Procuratore generale aveva chiesto che fosse sollevata questione di legittimità costituzionale dell'art. 2, quarto comma, c.p., per contrasto con l'art. 25, comma 2, Cost., nella parte in cui fa riferimento alla commissione del "reato" e non del "fatto" anche con riguardo ai reati di evento, qualora quest'ultimo sia differito nel tempo e, dopo la realizzazione della condotta, sopravvenga una disciplina punitiva meno favorevole. La tesi del Procuratore generale si basa su argomenti di tipo testuale (utilizzo del sostantivo "reato" e non "fatto") e logico (non sarebbe consentito in via interpretativa la scissione degli elementi costitutivi del reato a seconda delle esigenze applicative). La Corte ritiene infondata la questione, osservando come l'individuazione del *tempus commissi delicti* non possa essere delineata in termini generalizzanti, ma vada riferita ai singoli istituti e ai princìpi costituzionali che li governano.

Lo stesso con potrebbe dirsi avuto riguardo all'operatività di altri istituti, quali ad esempio la prescrizione; in tal caso il tempo di commissione del reato, rilevante per il *dies a quo* di decorrenza del termine, può essere individuato facendo riferimento al criterio dell'evento. Le risultanze della *blockchain* potranno pertanto garantire un referente temporale preciso e affidabile, ferma restando la possibilità di fornire una prova contraria.

Volendo in estrema sintesi ricapitolare gli esiti dell'indagine compiuta sul *tempus* di commissione del reato in *blockchain*, è possibile affermare che: non esiste nell'attuale ordinamento penale una definizione univoca di *tempus commissi delicti*, dovendo l'interprete far riferimento, a seconda dell'istituto di riferimento, al criterio della condotta o a quello dell'evento; in entrambi i casi è possibile trarre dai registri distribuiti un referente temporale assai preciso per collocare temporalmente l'azione delittuosa o l'evento da esso prodotto; ad ogni modo il requisito della validazione temporale, previsto dagli ultimi due commi dell'art. 8-*ter* del D.L. 135/2018, non produce alcuna presunzione di certezza della data e del contenuto del documento informatico ai fini dell'accertamento processuale penale; la particolare procedura informatica che assicura certezza e immutabilità alle risultanze del pubblico registro verrà in rilievo quale prova scientifica nel processo penale, come tale sottoposta alle regole della acquisizione nel contraddittorio delle parti.

5.5. *Locus commissi delicti* e natura ubiquitaria dell'infrastruttura. Alcune considerazioni conclusive.

Numerose sono dunque le questioni meritevoli di approfondimento. Le reti basate su registri distribuiti, delocalizzate, simultaneamente accessibili e in continuo aggiornamento, introducono un ulteriore fattore di complicazione nell'individuare il luogo di commissione del reato informatico.

Si tratta di un tema assai delicato che meriterebbe certamente maggiore attenzione da parte degli studiosi. La dottrina più attenta[163] ha ormai da tempo messo in luce le problematiche legate al rapido sviluppo delle tecnologie dell'informazione e della comunicazione, evidenziando la necessità di far leva su criteri più flessibili di individuazione del *locus commissi delicti* nel cyberspazio. Con la creazione della tecnologia a registro distribuito si è avuta una ulteriore conferma della difficoltà di trovare una soluzione soddisfacente ricorrendo ai criteri tradizionali dettati dal codice penale.

Nel ricercare una soluzione alternativa, la stessa dottrina propone di valorizzare il luogo di produzione del danno, riflettendo sul bene giuridico protetto dalle fattispecie

[163] Si richiama l'opinione espressa da FLOR, *I limiti del principio di territorialità nel cyberspace*, cit., 1305 il quale aveva fatto notare come la diffusione della tecnologia *mobile* e quella del *cloud computing* avrebbero inevitabilmente condotto a criticità in punto di luogo di commissione del reato informatico.

di reato in concreto considerate. È questo un criterio al quale la Corte di Giustizia[164] ha fatto riferimento in alcune pronunce in tema di lesione di diritti della personalità mediante Internet[165]. Il legislatore potrebbe sperimentare anche in ambito penale un criterio simile, prendendo le distanze dall'impostazione fondata sul principio di territorialità[166]. L'accentramento della competenza giudiziaria diventerebbe così un fattore di armonizzazione verso l'alto delle legislazioni nazionali, spingendo gli attori economici a collocare il proprio centro di interessi in quei Paesi che offrono un più alto standard di *cybersecurity* e dispongono di un apparato investigativo più efficiente.

Si tratta di una teoria sicuramente innovativa, che permetterebbe di superare, in un'ottica di efficientamento della giustizia, alcune delle problematiche che derivano dalla natura ubiquitaria delle infrastrutture decentralizzate[167]. Quando il sistema è controllato da uno o più titolari o sviluppatori (*blockchain* private o ibride) vi è un centro di imputazione degli effetti giuridici[168]; sarà dunque possibile applicare il criterio del luogo di concretizzazione del danno. Nelle *blockchain* pubbliche non esiste invece alcuna figura in posizione sovraordinata: l'infrastruttura si autogoverna sulla base delle regole impartite dall'algoritmo e dal protocollo informatico. Ne deriva una totale rarefazione della soggettività giuridica e l'impossibilità di rinvenire un centro d'imputazione unitario, diverso e autonomo rispetto all'organizzazione decentralizzata in sé, con evidenti ricadute sul piano della responsabilità. A questo tema dedicheremo ampio spazio nel prosieguo della trattazione; basti qui osservare come, in un quadro

[164] Corte di Giustizia dell'Unione Europea, Grande Sezione, 25 ottobre 2011, cause riunite C-509/09, C-161-10, eDate Advertising GmbH c. Société MGN ltd, in http://curia.europa.eu, richiamata anche da FLOR, *I limiti del principio di territorialità nel cyberspace*, cit., 1306.

[165] Nella specie la Corte ha statuito che la competenza del giudice civile deve essere parametrata luogo di concretizzazione del danno, *«poiché l'impatto, sui diritti della personalità di un soggetto, di un'informazione messa in rete può essere valutata meglio dal giudice del luogo in cui la vittima possiede il proprio centro di interessi, l'attribuzione di competenza a tale giudice corrisponde all'obiettivo di una buona amministrazione della giustizia»* (§ 48).

[166] La teoria è stata elaborata come criterio alternativo per individuare il luogo di commissione del reato di accesso abusivo a sistema informatico. A tal proposito, è ricorrente il riferimento al «centro di interessi» e al «domicilio informatico», che permettono di attribuire rilevanza non già alle informazioni registrate su un *server* (che ben potrebbero essere collocati in più sedi), bensì al diritto della personalità leso. Questo approccio consente di evitare le innumerevoli difficoltà tecniche di localizzazione dei dati e, in ogni caso, di individuazione della "sorgente" dell'attacco.

[167] Supponiamo che un attacco di *denial-of-service* colpisca una *blockchain* privata i cui nodi sono localizzati in diverse parti del mondo; il reato di cui all'art. 617-*quater* c.p. (interruzione di comunicazioni informatiche o telematiche) si realizza nel luogo in cui si trova il sistema informatico o telematico. I criteri comuni di cui all'art. 6 c.p. consentono di individuare una pluralità di luoghi di commissione del reato che, a ben vedere, potrebbero anche tutti trovarsi in territorio estero. Al contrario, l'accentramento della competenza giudiziaria nel luogo di produzione del danno alla libertà e segretezza delle comunicazioni informatiche – che corrisponde con la sede effettiva di esercizio dell'attività da parte del titolare della *blockchain* privata – sortirà l'effetto positivo non solo di avvicinare il foro competente alla vittima del reato, ma anche di risolvere a monte l'ambiguità circa il luogo di commissione del reato.

[168] *Amplius*, Cap. I, § 2.2.

dominato dall'ubiquità e dall'incertezza sul luogo di commissione del reato, la ricerca di un criterio puntuale e univoco pare destinata all'insuccesso[169].

6. Obblighi di controllo e omesso impedimento di reati. La posizione di garanzia in *blockchain*.

Le infrastrutture basate su registri distribuiti permettono ai partecipanti del *network* di compiere attività giuridiche di vario tipo, tra cui lo scambio di *token*, la registrazione di informazioni digitali, la conclusione di accordi auto-eseguibili. Nei paragrafi che precedono sono stati illustrati i vantaggi che la tecnologia DLT offre per gli utenti della rete[170]: rapidità ed efficienza delle transazioni, costi ridotti, fiducia nell'infrastruttura, anonimato, disintermediazione. Si è tuttavia messo in luce anche il "volto oscuro" delle applicazioni economico-finanziarie della *blockchain*, rappresentato dalla accentuata propensione ad essere strumentalizzata per finalità illecite[171].

Guardando al fenomeno dalla prospettiva del diritto penale, appare piuttosto evidente l'esigenza di contenere al minimo le elevate potenzialità criminogene del nuovo ritrovato tecnologico. Una questione spinosa, se solo si considera che la rete e la tecnologia, in sé considerate, sono sempre neutrali. La rilevanza penale delle condotte non dipende certo dalle caratteristiche proprie del mezzo, ma dai presupposti giuridico-fattuali dell'agire umano. E dunque a quest'ultimo che si dovrà rivolgere lo sguardo, per valutare se un soggetto sia rimproverabile per aver commesso o omesso di impedire un fatto costituente reato.

Rinviando al prosieguo della trattazione l'analisi delle fattispecie di reato più rilevanti, ci interroghiamo ora sulla possibilità di configurare obblighi di garanzia in capo ai soggetti che, a vario titolo, gestiscono o utilizzano l'infrastruttura decentralizzata. L'attenzione andrà rivolta, in particolare, alla possibilità di muovere un rimprovero per omesso impedimento di reati *ex* art. 40, comma 2, c.p., da parte di alcune figure soggettive in posizione "qualificata" rispetto ai semplici utenti del servizio. Secondo una autorevole opinione dottrinale[172], l'equiparazione della causalità omissiva a quella commissiva è la rappresentazione più evidente, al contempo, della logica prevenzionistica e materialistica che anima il diritto penale moderno. Il presupposto della nostra indagine si lega dunque alla necessità di individuare una o più

[169] L'interprete dovrà pertanto rassegnarsi a una applicazione quasi fisiologica delle regole suppletive per individuare il giudice competente.
[170] *Supra*, §§ 1.1 e seguenti.
[171] L'assenza di una autorità centrale e la pseudonimizzazione delle transazioni sono sfruttate dai criminali informatici, rispettivamente, per ostacolare le investigazioni e mantenere nascosta la propria identità.
[172] BLAIOTTA R., *Causalità giuridica*, Torino, 2010, 249 secondo cui nei reati omissivi impropri è stata tratteggiata l'equiparazione tra l'omissione e la causazione dell'evento ad alcune condizioni. Anzitutto che il reato commissivo sia configurato come reato d'offesa e che l'obbligo di garanzia sia concepito in termini solidaristici e cioè limitato alla protezione di beni bisognosi della tutela rafforzata, essendo i titolari incapaci di proteggerli adeguatamente. In secondo luogo che sia posto a carico di soggetti muniti di effettivi poteri impeditivi e che la condotta sia idonea ad impedire l'effetto offensivo.

figure di garanti che si trovino in posizione tale da potersi attivare per impedire la lesione di un bene giuridico. È una premessa coerente con l'esigenza di evitare che la disintermediazione degli scambi e l'assenza di una autorità centrale diventino un fattore di rischio per beni giuridici penalmente protetti.

Procedendo con ordine, si tratterà anzitutto di comprendere da quali fonti può derivare la posizione di garanzia e quali sono i soggetti destinatari dell'obbligo impeditivo. Nel far ciò, ripercorreremo in breve lo stato dell'arte, soffermandoci in particolare sul tema – per molti versi simile a quello che ci occupa – della responsabilità penale dell'*Internet Service Provider*. La questione andrà esaminata distinguendo a seconda della tipologia di infrastruttura: se nelle *blockchain* private l'individuazione di un soggetto garante non desta particolari problemi, in quelle pubbliche potrebbe non risultare agevole. Alcune riflessioni conclusive saranno dedicate alle prospettive *de lege ferenda* e ai possibili ambiti di intervento da parte del legislatore.

6.1. La causalità omissiva e la posizione di garanzia nel diritto penale.

La rilevanza dell'omissione nei reati di evento rappresenta uno dei temi più spinosi e controversi del diritto penale. La figura del reato commissivo mediante omissione tende a fuoriuscire dallo schema del *diritto penale del fatto*: l'accertamento della responsabilità del reo si sposta su un piano eminentemente teorico-normativo[173].

La genesi di questa peculiare categoria di reati è legata alla presenza, invalsa in molti ordinamenti giuridici moderni[174], di clausole estensive della punibilità, vale a dire di norme che stabiliscono un rapporto di equivalenza, sul piano eziologico, tra il commettere un reato e il non impedirlo, in violazione di un determinato obbligo giuridico. L'incriminazione dell'omissione antidoverosa è una scelta assai delicata, che, implicando un bilanciamento tra libertà fondamentali[175], crea numerosi punti di tensione.

---

[173] In dottrina l'opinione più accreditata sostiene che la causalità omissiva, diversamente da quella commissiva, abbia carattere normativo. Nella seconda c'è un rapporto tra due entità reali, nella prima non si riscontra alcuna connessione tra l'evento e una condizione di carattere reale. Dal punto di vista naturalistico si è di fronte a un *non facere* e l'evento è attribuibile alle forze della natura, alla serie causale in atto, non influenzata dal possibile intervento dell'uomo. Per approfondimenti, senza pretese di esaustività si veda STELLA F., *Leggi scientifiche e spiegazione causale nel diritto penale*, Milano, 1975, 2 ss. ID., *La nozione penalmente rilevante di causa*, in *Riv. It. dir. proc. pen*, 1988, 1217 ss; GRASSO G., *Il reato omissivo improprio*, Milano, 1983, 12 ss.; FIANDACA G., *Il reato commissivo mediante omissione*, Milano, 1979, 12 ss.; PALIERO C.E., *La causalita dell'omissione: formule concettuali e paradigmi prasseologici*, in *Rivista Italiana di medicina legale*, 1992, 4, 828; GIUNTA F., *La posizione di garanzia nel contesto della fattispecie omissiva impropria*, in *Diritto penale e processo.*, 1999, 169 ss.; LEONCINI I., *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Torino, 1999, 42; CENTONZE F., *Causalità attiva e causalità omissiva: tre rivoluzionarie sentenze della giurisprudenza di legittimità*, in *Riv. It. dir. proc. pen*, 2001, 1, 289; MANTOVANI F., *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, di solidarietà, di libertà e di responsabilità personale*, in *Riv. It. dir. proc. pen*, 2001, 2, 337; BARTOLI R., *Il problema della causalità penale*, Torino, 2010, 85.

[174] Per alcuni spunti comparatistici si veda SERENI A., *Causalità e responsabilità penale*, Torino, 2008.

[175] Secondo la concezione liberista, lo Stato deve limitarsi a vietare le condotte costituenti indebita limitazione della libertà altrui. Lo Stato autoritario, invece, si esprime attraverso comandi finalizzati ad

Una prima criticità è legata al rispetto del fondamentale principio di legalità. In tanto è possibile rimproverare al soggetto per non aver agito, in quanto questi era tenuto giuridicamente ad attivarsi per impedire la realizzazione dell'evento. Diversamente ragionando si rischierebbe di eludere il principio *nullum crimen sine lege poenali*. È bene quindi che le suddette clausole normative di equivalenza elenchino in modo specifico le fonti dalle quali discende, per il soggetto, un dovere di agire penalmente sanzionato in caso di omissione.

Da altro punto di vista, per il tramite di questa categoria di reati il diritto penale riesce a estendere la portata incriminatrice delle fattispecie commissive, superando il paradigma eziologico della *causalità naturalistica* in favore di una *causalità ipotetica*[176]. È noto come l'accertamento del legame causale nei reati omissivi impropri abbia rappresentato un vero e proprio banco di prova per la teoria e la prassi, impegnate su un duplice fronte di lavoro: da una parte l'individuazione dell'*iter* logico da seguire per l'accertamento della causalità omissiva; dall'altra la ricerca di un coefficiente statistico che sia sufficiente a dimostrare l'esistenza del rapporto eziologico[177]. Ambedue le questioni meriterebbero un esame approfondito, dal quale dovremo però prescindere per evidenti ragioni di continenza espositiva. L'attenzione andrà piuttosto rivolta alla categoria della posizione di garanzia, anch'essa al centro di un acceso dibattito in dottrina. Una breve disamina dello stato dell'arte si consentirà di fissare le coordinate essenziali per valutare l'esistenza di obblighi di impedimento di reati a carico dei soggetti che operano in *blockchain*.

6.1.1. Le fonti dell'obbligo giuridico impeditivo. Sintesi dello stato dell'arte.

Si è detto che la causalità omissiva non è fondata su un obiettivo rapporto eziologico tra fatti, non potendo la condotta omissiva causare materialmente l'evento nel quale si concretizza l'offesa del reato. Essa ha, dunque, un carattere normativo, nel

orientare la vita dei cittadini verso gli interessi collettivi e gli scopi del regime; esso tende, di conseguenza, ad accrescere il numero dei reati omissivi. Nel mezzo si colloca lo Stato sociale che, pur imponendo alcuni obblighi volti a conseguire fini solidaristici, non dimentica i diritti fondamentali del consociato, tra cui le libertà negative (libertà dallo Stato, *melius* dalla sfera degli obblighi che sono imposti dallo stesso). In argomento, MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 337; BLAIOTTA, *Causalità giuridica*, cit., 250.

[176] La causalità omissiva non è fondata su un obiettivo rapporto eziologico tra fatti non potendo la condotta omissiva causare materialmente l'evento nel quale si concretizza l'offesa del reato. Essa ha, dunque, un carattere normativo, nel senso che si basa sul rapporto di equivalenza tra il causare e il non impedire l'evento di reato. La causalità naturalistica e quella ipotetica presentano profonde differenze in punto di accertamento: nel primo caso si può ragionare su fatti, cioè dati concreti; nel secondo caso si tratta piuttosto di un'astrazione, di congetture ipotetiche. In argomento, BLAIOTTA, *Causalità giuridica*, cit., 255 al quale si rinvia per gli opportuni riferimenti bibliografici.

[177] La verifica non ha ad oggetto un accadimento del passato, ma la previsione di un evento del futuro. Un ragionamento di questo tipo fa leva fu un giudizio puramente ipotetico secondo la formula della *condicio sine qua non*; l'azione è idealizzata, supposta, e ciò non può che illuminare sull'incertezza e astrattezza di tale ragionamento.

senso che si basa sul rapporto di equivalenza tra il causare e il non impedire l'evento stabilito dall'art. 40, capoverso, c.p.[178]; per queste ragioni la dottrina parla anche di "equivalente normativo della causalità". Il presupposto essenziale della causalità omissiva è, dunque, la sussistenza di un obbligo giuridico di impedire l'evento; al fine di stabilire quando ricorra una tale circostanza sono state elaborate in dottrina diverse teorie.

Come noto, secondo una prima *teoria* c.d. *formale*[179] la fonte dell'obbligo giuridico va ricercata nella legge (penale o extrapenale, ivi compresa la consuetudine), o nel contratto. La posizione di garanzia avrebbe dunque un ancoraggio giuridico, che garantisce il rispetto del principio di legalità. La tesi presta tuttavia il fianco a una duplice critica: da un lato non sarebbe in grado di selezionare, tra le norme di legge, quelle aventi una reale funzione di garanzia; dall'altra, si affida eccessivamente alle conseguenze sul piano giuridico, trascurando l'andamento della realtà fattuale[180]. In altre parole viene contestato un eccessivo rigore formale, che rischia di collidere con alcuni principi fondamentali[181].

Secondo la opposta *concezione funzionale*[182] l'obbligo di garanzia va parametrato alle specifiche funzioni in concreto svolte dall'agente, titolare di un potere di signoria sulle condizioni essenziali per il verificarsi dell'evento. La posizione del garante si caratterizza per uno speciale vincolo di tutela, che sorge in virtù della concreta assunzione di un ruolo di protezione del bene esposto a pericolo o per effetto di una precedente attività pericolosa. Benché questa teoria detti un criterio razionale di delimitazione del reato omissivo improprio, appaiono evidenti i punti di frizione con il principio di legalità[183]. Invero, l'ancoraggio a criteri di tipo sostanziale non permette di

---

[178] La causalità si reputa esistente allorché, ipotizzando come posta in essere la condotta possibile e doverosa omessa, l'evento costitutivo del reato non si sarebbe verificato, o si sarebbe verificato più avanti nel tempo, secondo quanto desumibile dalla migliore scienza del momento.

[179] Tale è la teoria seguita dalla dottrina e dalla giurisprudenza italiana tradizionale, espressione del liberalismo giuridico. Cfr. MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 338

[180] Così, nel caso in cui un contratto sia affetto da *invalidità*, la posizione di garanzia dovrebbe venire meno indipendentemente dalla presa in carico il bene giuridico o dall'affidamento dello stesso da parte del garante originario. Allo stesso modo, si dovrebbe affermare l'esistenza dell'obbligo di garanzia per il solo fatto della *validità* del contratto, anche in assenza di effettiva presa in carico del bene. Sul tema v. anche LEONCINI I., *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Torino, 1999

[181] In un ordinamento fondato sul principio della colpevolezza e di offensività, la responsabilità penale non può basarsi su dati puramente formali. Perché un evento possa essere posto a carico di chi aveva il dovere di attivarsi è necessario, da un lato, che questi si fosse trovato nella condizione di espletare l'attività giuridica che aveva il dovere di compiere, dall'altro, che, nel caso in cui la fonte normativa sia cessata per fatti sopravvenuti, il soggetto sia chiamato comunque a rispondere degli eventi che concretamente aveva il potere di impedire.

[182] Tale concezione è stata elaborata dalla dottrina tedesca nella metà del secolo scorso e ha presto preso piede nella scienza penalistica italiana. Cfr. ROXIN C., *Strafrecht, Allgemeiner Teil*, Vol. II, *Besondere Erscheinungsformen der Straftat,* Monaco, 2003, 671; FIANDACA, *Il reato commissivo mediante omissione*, cit., 21 ss.; GRASSO, *Il reato omissivo improprio*, cit., 192 ss.; GIUNTA, *La posizione di garanzia nel contesto della fattispecie omissiva impropria*, cit., 620.

[183] Secondo alcuni la "copertura" normativa sarebbe garantita da norme di contenuto generale, quali l'art. 2 Cost. (doveri di solidarietà sociale) o l'art. 32 Cost. (tutela della salute). Alla tesi è stato obiettato che tali norme non appaiono suscettibili di orientare la condotta del singolo, essendo piuttosto rivolte a regolare l'azione del legislatore e dello Stato nel suo complesso. Sulla eccessiva dilatazione della

circoscrivere l'area del penalmente rilevante entro limiti definiti, lasciando alla discrezionalità dell'interprete l'individuazione e la delimitazione della posizione di garanzia.

È stata pertanto elaborata una terza *teoria mista* (o formale-sostanziale) oggi prevalente, che, integrando le due precedenti, sostiene che la fonte dell'obbligo debba essere legislativamente predeterminata, ma che la posizione di garanzia sorga soltanto nel caso di corrispondenza con la funzione e il ruolo in concreto ricoperti dal garante[184]. Alla tesi si obietta di non aver affatto risolto la questione più controversa relativa alle ipotesi in cui il dovere "funzionale" di agire non trova riscontro in norme giuridiche dal contenuto sufficientemente determinato.

La giurisprudenza non ha sempre seguito un indirizzo univoco[185], talvolta affermando che la posizione di garanzia deve avere una fonte normativa, anche di natura privatistica, altre volte attribuendo rilevanza alle situazioni di mero fatto, come la volontaria assunzione di compiti di tutela o la precedente condotta illecita[186]. Non è raro imbattersi in pronunce di legittimità che effettuano una commistione tra criteri sostanziali e formali, lasciando presupporre una sorta di tacita adesione alla concezione mista[187].

Non potendosi dare qui conto delle diverse opinioni espresse dalla dottrina, dovremo limitarci a sottolineare l'importanza di una ricostruzione dell'istituto sulla base dei principi cardine della materia penalistica[188]. *In primis* del principio di legalità, *sub specie* di riserva di legge e tassatività, da cui deriva la necessaria giuridicità dell'obbligo di garanzia. Esso trae fondamento solo da fonti giuridiche formali[189], ivi

posizione di garanzia ricostruita sulla base della concezione funzionale v. SGUBBI F., *Responsabilità penale per omesso impedimento dell'evento*, Padova, 1975, 127 ss.

184 I sostenitori di questa teoria riconoscono efficacia precettiva anche a norme dal contenuto estremamente ampio, al fine di evitare che cadano al di fuori dell'area del penalmente rilevante l'omissione di doveri sociali non puntualmente codificati. In sostanza si cerca di superare la critica mossa all'impostazione funzionale di trascurare i limiti derivanti dal principio di tassatività attraverso il riconoscimento che soltanto in alcuni casi eccezionali la protezione di determinati beni da fonti di pericolo è idonea a fondare una posizione di garanzia 'generalizzata e solidaristica', come avviene, ad. esempio, per i genitori.

185 Cfr. tra le più recenti, Cass. Pen., Sez. IV, 10 giugno 2010 n. 38991; Cass. Pen., Sez. IV, 3 maggio 2010, n. 16761; Cass Pen, Sez. IV, 6 febbraio 2004, n. 4981.

186 In questo senso, v. Cass. Pen., Sez. IV, 22 ottobre 2008, n. 45698; Cass. Pen., Sez. IV, 22 maggio 2007 n. 25527.

187 Sulla opportunità di una reciproca integrazione fra la concezione formale e funzionale v. ROMANO, M., *Commentario sistematico del codice penale*, I, Milano, 2004, 391 ss.

188 Le considerazioni che seguono costituiscono una sintesi della autorevole posizione di MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 340, più volte richiamata.

189 Non vi è uniformità di opinioni sulle fonti dell'obbligo di garanzia. Da una parte vi è chi sostiene (MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 344) che fonte primaria sia la sola legge extrapenale, con esclusione delle fonti sublegislative, alle quali va riconosciuta una efficacia meramente integrativa entro i limiti stabiliti dalla legge); dall'altra chi ammette la possibilità di derivare l'obbligo di garanzia direttamente dalle fattispecie incriminatrici (ANTOLISEI, *Manuale di diritto penale – Parte generale*, cit., 260), dimostrando una apertura maggiore verso l'eterointegrazione del precetto da parte di fonti di rango secondario (a proposito della legislazione settoriale a tutela della salute e della sicurezza sul lavoro v. LEONCINI I., *L'obbligo di impedire l'infortunio*, in GIUNTA F., MICHELETTI D., *Il nuovo diritto penale della sicurezza nei luoghi di lavoro*, Milano, 2010, 112 ss.); altri ancora

compreso il contratto[190], con esclusione tanto delle situazioni meramente fattuali[191], quanto degli obblighi del tutto indeterminati[192].

Nondimeno, occorre considerare il principio di libertà/frammentarietà, che impone al legislatore di individuare in modo specifico i soggetti titolari della posizione di garanzia, selezionando coloro che si trovano in un particolare rapporto giuridico con il bene da proteggere[193]. Infine, il principio di personalità della responsabilità penale che, inteso nella sua più lata eccezione di rimproverabilità per fatto proprio colpevole, rende inevitabile l'ancoraggio dell'obbligo di garanzia a un effettivo potere impeditivo[194].

---

attribuiscono rilevanza a ogni norma giuridica, ivi compresa la consuetudine (Cfr. PAGLIARO A., *Principi di diritto penale - Parte generale*, Milano, 1998, 363).

[190] L'idoneità del regolamento contrattuale a fondare posizioni di garanzia deriva dalla disposizione che attribuisce forza di legge all'autonomia negoziale dei privati (cfr. art. 1372 c.c.). Secondo la lettura proposta dal Mantovani (*op. ult. cit.),* gli obblighi di garanzia di origine contrattuale comprendono sia quelli trasferiti dal garante originario a quello derivato, sia gli obblighi creati *ex novo* a carico del soggetto garante. In ogni caso sarà necessario, in virtù del principio di personalità del rimprovero penale, l'effettivo trasferimento al garante derivato o l'insorgenza in capo al nuovo garante di concreti poteri impeditivi (cumulo tra poteri giuridici e poteri fattuali), che non coincide necessariamente né con il momento della perfezione del contratto, né con la mera presa in carico fattuale del bene. Ne consegue che anche la controversa questione circa l'insorgenza o meno dell'obbligo di garanzia in caso di negozio invalido andrebbe risolta in termini relativistici, valutando l'idoneità della singola causa d'invalidità a incidere sui requisiti penalistici dell'obbligo di garanzia.

[191] Vi è divergenza di opinioni sulla rilevanza l'assunzione volontaria dell'obbligo, che avviene nella forma della *negotiorum gestio* ai sensi dell'art. 2028 c.c. Cfr. GIUNTA, *La posizione di garanzia nel contesto della fattispecie omissiva impropria*, cit. 621; *contra* MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 350. Per quel che concerne la precedente attività pericolosa, alcuni la considerano fonte della posizione di garanzia tutte le volte in cui essa dia luogo a una situazione di pericolo per i terzi, a fronte della quale il soggetto deve attivarsi per impedire che si concretizzi nella lesione di beni altrui. La precedente attività pericolosa è uno dei petali che compongono il c.d. *trifoglio*, che metaforicamente esprime la teoria, in base alla concezione formale, secondo cui le fonti dell'obbligo di attivarsi possono essere la legge, il contratto e la precedente attività pericolosa (v. FIANDACA G., MUSCO E., *Diritto penale - Parte Generale*, Bologna 2019, 541; ANTOLISEI, *Manuale di diritto penale – Parte generale*, cit., 260). Al riguardo, ci sembrano insuperabili le obiezioni mosse dalla dottrina secondo cui non vi è alcuna norma giuridica che prescrive di impedire le offese derivanti dalla propria attività pericolosa. Tale non potrebbe essere l'obbligo generale di diligenza che informa l'agire dei consociati poiché, a stretto rigore, un evento che si realizzasse come conseguenza di una azione negligente sarebbe addebitato al soggetto, ricorrendone i presupposti, come fatto commissivo colposo. Inoltre, il criterio della precedente attività pericolosa si pone in tensione con il principio della riserva di legge, dato che l'art. 40 comma 2 c.p. non fa alcun riferimento, né esplicito né implicito, a tale criterio. In argomento v. GIUNTA, *La posizione di garanzia nel contesto della fattispecie omissiva impropria*, cit., 624; MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 349.

[192] Una ricostruzione dell'istituto in conformità con il principio di determinatezza porta a ritenere che requisito essenziale dell'obbligo di garanzia sia la sua *specificità*. Tale principio verrebbe eluso se si attribuisse rilevanza a norme di principio o clausole costituzionali quali l'art. 2 Cost.

[193] Secondo Mantovani (*op.ult.cit*.) il reato commissivo mediante omissione dovrebbe essere classificato come un *reato proprio* di specifiche categorie di soggetti.

[194] La presenza di un potere giuridico impeditivo distingue l'*obbligo di garanzia* dall'*obbligo di sorveglianza*, gravante su soggetti titolari di poteri di vigilanza e di informazione. Il principio di personalità della responsabilità penale impedisce che l'inosservanza del secondo possa dar luogo a un rimprovero per omesso impedimento dell'evento: il soggetto sarebbe infatti chiamato a rispondere per fatto altrui, dal momento che non dispone dei poteri idonei a prevenire la realizzazione del fatto. Per approfondimenti, LEONCINI, *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, cit., 12 ss.; MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 343; MICHELETTI D., *La posizione di garanzia nel diritto penale del lavoro*, in *Riv. trim. dir. pen. econ*., 1 - 2, 2011, 155 ss.

Più precisamente dovrà trattarsi di un dovere preesistente[195] rispetto alla situazione di pericolo, cosicché il garante sia in condizione di attivarsi per prevenire l'*eventus damni*, e di un dovere esigibile, nel senso che quest'ultimo deve trovarsi nella materiale possibilità di compiere l'azione impeditiva idonea.

6.1.2. Obbligo di garanzia e teoria del rischio. Brevi cenni.

Per concludere l'analisi del quadro teorico, si ritiene utile ai fini dell'indagine una breve disamina delle tesi che, partendo dalla concezione funzionale dell'obbligo di garanzia, hanno ricostruito la causalità omissiva a partire dal concetto di "rischio".

La teoria dell'imputazione oggettiva dell'evento, anche detta teoria del rischio, è sorta in Germania negli anni '30 del secolo scorso con lo scopo di offrire un correttivo al principio della causalità condizionalistica. Essa permette di esaminare da una prospettiva dinamica il riparto di ruoli e di responsabilità nello svolgimento di attività pericolose, ancorando il concetto penalistico di causa a quello di concretizzazione del c.d. rapporto di rischio; il *quid pluris* rispetto agli altri correttivi consiste infatti nell'individuazione del rischio quale chiave di volta nella lettura degli intrecci causali. Sebbene sia stata del tutto ignorata dalla dottrina per più di mezzo secolo, negli ultimi anni la teoria ha avuto crescente seguito in Italia[196].

Volendo delineare in estrema sintesi i postulati dell'imputazione obiettiva dell'evento[197], si sostiene che la constatazione dell'esistenza di un nesso di condizionamento non è sufficiente, sul piano oggettivo, all'attribuzione del fatto, essendo invece necessario che la condotta abbia determinato o incrementato un pericolo giuridicamente riprovato e che tale pericolo si sia effettivamente realizzato nell'evento in concreto prodotto: creazione del pericolo e realizzazione del rischio diventano i due elementi fondanti l' imputazione oggettiva[198]; il nesso di imputazione diventa perciò un nesso di rischio[199]. Per quanto l'ordinamento si sforzi di orientare il comportamento degli individui in modo da evitare situazioni di pericolo, esistono

[195] Il requisito della preesistenza differenzia l'obbligo di garanzia dal mero obbligo di attivarsi, che insorge al verificarsi di uno o più presupposti di fatto descritti da una norma di legge (ad. es. il ritrovamento della persona in pericolo nell'omissione di soccorso, art. 593 c.p.).

[196] DONINI M., *Lettura sistematica delle teorie dell'imputazione obiettiva dell'evento,* in *Riv. It. dir. pen proc.*, 1989, 1115 ss.; CASTALDO A., *Linee politico criminali e imputazione oggettiva del delitto colposo di evento,* in *Riv. It. dir. pen. proc*., 1987, 881.

[197] Sul tema fondamentale DONINI M., *Imputazione oggettiva dell'evento. "Nesso di rischio" e responsabilità per fatto proprio*, Torino, 2007.

[198] La teoria del rischio riesce a punire condotte che, altrimenti, dovrebbero andare esenti da pena per difetto del nesso di causalità: si fa l'esempio di chi monta in modo inappropriato un parafulmine sul tetto di un'abitazione, evidentemente, al verificarsi di un evento di morte o lesioni, per costui non varrebbe alcun argomento sulla eccezionalità statistica di verificazione dell'evento. Cfr. BLAIOTTA, *Causalità giuridica,* cit., 150.

[199] Alla teoria in commento è stata mossa l'obiezione di anticipare impropriamente sul piano della causalità un giudizio che riguarda l'imputazione soggettiva, vale a dire la prevedibilità dell'evento nella colpa. Il rilievo non pare però risolutivo, atteso che anche altre teorie (ad. es. quella della causalità umana o causalità adeguata) si affidano a parametri di tipo soggettivo (eccezionalità e assoluta imprevedibilità del fattore causale da solo sufficiente a determinare l'evento).

alcuni rischi che, in un bilanciamento razionale di interessi, è necessario correre. Il diritto penale non può pertanto punire la produzione di eventi che costituiscano concretizzazione di un rischio accettato come lecito, perché minimale o ineliminabile.

Gli elementi strutturali del ragionamento fondato sulla teoria in commento prendono storicamente il nome di 'radici' mutuando il termine dalla dogmatica tedesca[200].

La *prima radice* è quella della natura del rischio, attraverso il quale è possibile escludere l'imputazione quando la condotta non ha determinato un pericolo obiettivamente riprovato dall'ordinamento, oppure quando l'azione ha pur influito sulla produzione dell'evento ma rimane entro i limiti di un rischio non giuridicamente apprezzabile o comunque consentito dall'ordinamento. All'area di rischio consentito viene ricondotta anche la questione relativa all'affidamento sulla liceità del comportamento altrui[201].

La *seconda radice* è quella della realizzazione del rischio. Affinché l'evento possa essere imputato all'agente occorre che si sia prodotto come risultato di un decorso causale tipico, nel senso che l'evento finale costituisce concretizzazione di quel rischio che la regola di diligenza violata mirava a prevenire[202]. L'imputazione, dunque, trova il suo fulcro in una valutazione finalistica, cioè nello scopo di protezione della norma. Questo secondo canale opera *ex post* e richiede che il pericolo giuridicamente riprovato, creato o aumentato dalla condotta dell'agente si sia effettivamente realizzato nel concreto prodursi dell'evento.

La teoria del rischio contribuisce a spiegare in modo razionale i limiti di rilevanza causale dell'omissione; sarà pertanto opportuno richiamare alcuni suoi corollari con riferimento alla responsabilità dei soggetti che operano sul mercato delle valute virtuali.

6.2. *Internet Service Provider* e libertà della rete.

Il tema della responsabilità del fornitore di servizi è senza dubbio tra quelli più hanno messo in luce la tendenziale inconciliabilità delle categorie del diritto penale con le sfide lanciate dal progresso tecnologico. Benché la dottrina più attenta abbia iniziato

200 BLAIOTTA, Causalità giuridica, cit., 159.

201 Sebbene l'esperienza insegni che gli uomini delinquono e commettono errori rimane in larga misura lecito confidare che essi agiranno in modo corretto. Ne consegue che il rischio che ne deriva è lecito, salvi casi particolari in cui l'agente, in virtù della posizione rivestita, aveva un obbligo di prevenire anche il comportamento illecito altrui (c.d. rischio rinforzato), come avviene, ad esempio, per i destinatari della disciplina preventiva del riciclaggio. Ad esso faremo riferimento nell'affrontare il tema della responsabilità omissiva del titolare della *blockchain* e del programmatore di *smart contract* per i reati commessi dagli utenti della piattaforma (v. *infra*, § 6.3.).

202 Così, ad esempio, il concorso omissivo dell'*exchange provider* nel reato di riciclaggio commesso dall'utente sarà possibile a condizione che l'omissione degli obblighi imposti dalla normativa antiriciclaggio (identificazione della clientela e segnalazione delle operazioni sospette) abbia reso possibile la commissione del reato (*amplius*, Cap. III, § 3.5.1.).

ad approfondirlo fin dagli ultimi anni del secolo scorso[203], esso è ancora al centro del dibattito tra gli studiosi[204]. Le ragioni della mai sopita attenzione per il tema appaiono piuttosto evidenti. Se da un lato, nella moderna società dell'informazione, si avverte in modo sempre più pressante l'esigenza di responsabilizzare i soggetti che operano sulla rete, dall'altra l'inerzia del legislatore nel disciplinare in modo autonomo la responsabilità dei *provider* ha talvolta indotto la giurisprudenza a "forzare" gli schemi tradizionali di imputazione.

Una trattazione che voglia esaminare *funditus* la responsabilità dei soggetti qualificati che operano in *blockchain* deve necessariamente partire dall'indagine – prospettica e più generale – della responsabilità dei *provider* di Internet, al fine di cogliere eventuali similitudini e differenze.

Alla base del dibattito vi è la contrapposizione tra due opposte tesi sulla libertà di Internet: quella secondo cui essa non sarebbe suscettibile di ostacoli o limitazioni di alcun tipo; quella secondo cui, all'opposto, si dovrebbe assicurare – nello spazio virtuale come in quello fisico – la protezione da fonti di rischio potenzialmente lesive di interessi meritevoli di tutela. Il difficile bilanciamento tra garanzie di libertà ed esigenze di controllo[205] è una *vexata questio* che, dalla prospettiva penalistica, si compendia nella opportunità di considerare il fornitore di servizi come il titolare di una posizione di garanzia volta ad impedire la commissione di reati sulla piattaforma virtuale.

Chi fa prevalere la prima tesi sostiene che, se l'ordinamento pretendesse dai *provider* di attivarsi per impedire la commissione di reati, ciò varrebbe ad introdurre meccanismi di censura preventiva tali da minare alle fondamenta la libertà di

---

[203] SIEBER U., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer*, in *Riv. trim. dir. pen. ecom.*, 1997, 756 ss.; SEMINARA S., *La responsabilità penale degli operatori su internet*, in *Dir. Inf.*, 1998, 3, 745 ss.; ID., *La pirateria su* internet *e il diritto penale*, in *Riv. trim. dir. pen. ecom.*, 1997, 1, 71 ss.; PICOTTI L., *Fondamento e limiti della responsabilità penale dei* service-providers *in* internet, in *Dir. pen. proc*., 1999, 1, 379 ss.; ID., *La responsabilità penale dei* service-providers *in* internet, in *Dir. pen. proc*., 1999, 2, 501 ss.; ZENO ZENCOVICH V., *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su* internet *(riflessioni preliminari)*, in *Dir. Inf*., 1999, 6, 1049 ss.

[204] Più di recente sul tema, MANNA A., *I soggetti in posizione di garanzia*, in *Dir. Inf.*, 2010, 6, 786; RESTA F., *La responsabilità penale del provider: tra* laissez faire *ed obblighi di controllo*, in *Giur. mer*., 2010, 9, 1715 ss.; PEZZELLA V., *Google Italia, diffamazione e riservatezza: il difficile compito del* provider *(e del giudice)*, in *Giur. mer*., 2010, 2232 ss.; LOTIERZO R., *Il caso* Google-Vivi Down *quale emblema del difficile rapporto degli* internet providers *con il codice della* privacy, in *Cass. Pen*., 2010, 11, 4003 ss..; DE NATALE D., *Responsabilità penale dell'internet service provider per omesso impedimento e per concorso nel reato di pedopornografia*, in GRASSO G., PICOTTI L., SICURELLA R., *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, 295 ss.; INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?* in LUPARIA L. (a cura di), Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, 15 ss; ACCINNI G.P., *Profili di responsabilità penale dell'*hosting provider *"attivo"*, in Archivio penale, 2017, 2, 1 ss.; MANNA A, DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 892;

[205]Cfr. INGRASSIA, *Il ruolo dell'ISP nel* ciberspazio, cit., 18

Internet[206]. Il legislatore dovrebbe pertanto astenersi dal dettare regole *ad hoc* per prevenire la commissione di reati, poiché tale eventualità non giustifica aprioristicamente la possibilità di adottare meccanismi di limitazione preventiva[207].

A questa lettura si contrappone quella che considera la presenza di controllori nel cyberspazio funzionale alla tutela dei diritti dei singoli e, di riflesso, della effettiva libertà della rete. Il legislatore non potrebbe dimostrarsi indifferente di fronte a un fattore di rischio così allarmante, dovendo piuttosto predisporre delle misure di carattere preventivo[208].

Tra i due estremi si colloca una tesi intermedia, secondo cui a determinate condizioni ed entro certi limiti è necessario che i 'garanti' della rete si attivino per evitare che la libertà nella rete sconfini nell'anarchia[209]. Adottando un approccio più realista, essa si propone andare alla ricerca di un equo bilanciamento tra l'esigenza della libertà *della rete* e la necessità di libertà *nella rete*[210]. Per contemperare le contrapposte esigenze occorre individuare i soggetti che, rivestendo una posizione qualificata rispetto al *quivis de populo*, possano attivarsi al ricorrere di determinate situazioni di rischio. La legge dovrebbe dunque disciplinare in modo preciso e puntuale le condizioni che legittimano la limitazione delle libertà in Internet, per evitare che la sicurezza cibernetica si trasformi in uno strumento generalizzato di censura[211]. Questa tesi risulta indubbiamente più in linea con le esigenze della moderna società: il controllo esercitato dai 'garanti' non deve essere generalizzato, ma mirato a fronteggiare determinate situazioni di rischio; un controllo preventivo 'a tappeto' comprimerebbe in modo eccessivo non soltanto la libertà dei singoli utenti, ma anche

[206] Sul tema della libertà di Internet fondamentale RODOTÀ S., *Una Costituzione per Internet*, in *Politica del diritto*, 2010, 3, 339 ss.

[207] La tesi si fonda sul rilievo di Internet come strumento di libera manifestazione del pensiero, in grado di riunire una comunità meritevole di tutela come 'formazione sociale' (artt. 2, 21 Cost.). Non vi sarebbe alcuna necessità di controllori o garanti, essendo sufficiente il presidio apprestato dalla legge penale per punire il singolo che abbia abusato della propria libertà.

[208] La progressiva informatizzazione dei processi produttivi, informativi e decisionali renderebbe ormai evidente la necessità di controlli e di centri di imputazione di obblighi di filtraggio o rimozione. Si argomenta che il ruolo del diritto penale non è soltanto quello di punire le condotte antigiuridiche e colpevoli, ma altresì quello di prevenire la commissione di reati. Quando vi è una fonte di rischio che trovi causa in un rapporto qualificato tra un soggetto e l'attività da questi esercitata, l'attribuzione di una posizione di garanzia è funzionale a una tutela effettiva dell'interesse, giuridicamente rilevante, esposto a pericolo. La garanzia dei diritti nel cyberspazio può pertanto essere assicurata soltanto attraverso l'individuazione di soggetti chiamati a 'sorvegliare' l'operato degli utenti. In tal senso, ai controllori spetta l'obbligo di attivarsi per prevenire la commissione di reati, laddove ciò risulti tecnicamente e 'umanamente' possibile.

[209] Questa è la tesi che meglio descrive la posizione espressa dal legislatore europeo nel disciplinare la materia (v. *infra*).

[210] Nella moderna società, il pluralismo democratico passa *in primis* per la libera fruizione degli strumenti informatici e telematici, che consentono al cittadino un effettivo esercizio dei propri diritti (manifestazione del pensiero, istruzione, associazionismo politico e sindacale etc.). D'altro canto, sarebbe impossibile non considerare come dette libertà possano irrimediabilmente essere compromesse in uno spazio virtuale privo di regole e di tutori dell'ordine.

[211] Il legislatore dovrebbe dunque valorizzare modelli di *compliance* e di controllo successivo (obbligo di rimozione, vigilanza prudenziale di soggetti pericolosi), anziché meccanismi di controllo preventivo.

del titolare del fornitore del servizio (o di altro soggetto qualificato), che sarebbe tenuto *ad impossibilia* a dotarsi di apparati e strumenti preventivi[212].

Ciò posto, si pone il problema di definire a quali condizioni il *provider* dovrà attivarsi e, a monte, individuare chi sono i soggetti chiamati a far fronte alle situazioni di pericolo ingenerate dalla commissione di un reato *online;* si dovrà inoltre stabilire quale siano le conseguenze penali per l'inosservanza dell'obbligo imposto dalla legge. A tal fine, l'indagine sulla responsabilità penale del *provider* dovrà essere calata nel peculiare contesto spazio-temporale del ciberspazio che, come più volte accennato[213], fa perdere all'azione e all'evento ogni connotazione naturalistica[214].

L'*Internet Service Provider* svolge un ruolo fondamentale per il funzionamento della rete, fornendo agli utenti servizi di connessione, messaggistica (posta elettronica, *chat line*) memorizzazione (*hosting* di siti web o *blog*), e indicizzazione (motori di ricerca)[215]. Come noto gli art. 14 ss. del D. Lgs. 70/2003 (c.d. Codice del commercio elettronico) individuano tre tipologie di *provider* in base all'attività di memorizzazione svolta e al tempo di *retention* dei dati[216], prevedendo che il prestatore del servizio non sia responsabile delle informazioni trasmesse o registrate a condizione che non le selezioni né le modifichi, e che agisca prontamente per rimuoverle non appena venga effettivamente a conoscenza del fatto che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione[217].

---

[212] Del resto, la previsione di un regime di responsabilità per omesso controllo troppo rigoroso sarebbe d'ostacolo al libero esercizio dell'attività d'iniziativa economia privata (art. 41 Cost.).

[213] *Supra*, §§ 2.1. e 2.2.

[214] INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 17

[215] Il provider non si identifica in una persona in carne ed ossa, quanto piuttosto in un'organizzazione che svolge tale attività professionalmente e all'interno della quale si dovrà rinvenire un soggetto penalmente responsabile.

[216] Il *mere conduit* provider, anche detto *access provider*, svolge una attività di mero trasporto di dati, occupandosi di gestire un flusso di informazioni intercorrente tra terzi al fine di consentire l'accesso alla rete e alle risorse digitali. Le attività di trasmissione includono la memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, a condizione che questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario a tale scopo (art. 14); il *caching provider* presta un servizio di memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta (art. 15); l'*hosting provider*/*content provider* è quello più di frequente chiamata a rispondere per gli illeciti commessi sulla piattaforma di *host,* specie nei casi in cui nella prestazione del servizio, il fornitore compia attività di indicizzazione sul contenuto dei file ospitati. Il servizio di *hosting* consiste nella memorizzazione delle informazioni fornite da un destinatario del servizio, vale a dire di archiviazione di dati in transito (*storage* di informazioni), al fine di renderle reperibili a utenti remoti (art. 16). L'attività di hosting è detta passiva allorché il fornitore del servizio si limiti a mettere a disposizione la piattaforma digitale a richiesta del destinatario, senza compiere alcuna attività sui file oggetto di archiviazione. Diversamente, si parla di *host* attivo quando il fornitore del servizio si interessa, a vario titolo, del contenuto dei file ospitati, al fine di catalogarli, indicizzarli, ordinarli, selezionarli etc. In argomento, ACCINNI, *Profili di responsabilità penale dell'*hosting provider *"attivo*", cit., 2 ss.; PANATTONI B., *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di* notice and take down, in *Diritto penale contemporaneo – Rivista trimestrale*, 2018, 5, 249 ss.

[217] Con riferimento a ciascuna delle tre tipologie di *provider* il Codice del commercio elettronico prevede (artt. 14, comma 3, 15, comma 2, 16, comma 3) che *«L'autorità giudiziaria o quella amministrativa*

La normativa sul commercio elettronico prevede espressamente l'assenza di un obbligo generale di sorveglianza[218] temperato da un dovere di collaborazione con la pubblica autorità. Qualora sia a conoscenza di presunte attività illecite compiute da un utente, il *provider* è tenuto ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, e a fornire, a richiesta delle stesse, le informazioni in suo possesso che consentano l'identificazione del destinatario del servizio. Dalla lettura congiunta delle disposizioni emerge che il legislatore delegato, in linea con le indicazioni espresse nella Direttiva 2000/31/CE sui servizi della società dell'informazione, ha sposato la tesi intermedia della libertà "condizionata" della rete[219].

Il legislatore fa riferimento, in modo generico, alla 'responsabilità' senza specificare l'ambito di operatività dell'esenzione. Ci si domanda se la clausola possa assumere rilievo come esimente di responsabilità penale. Per fornire una risposta esaustiva occorre inserire le previsioni in esame nel complesso quadro della posizione di garanzia penalistica, alla stregua della quale valutare l'esistenza di un obbligo giuridico impeditivo in capo al *provider* donde stabile se, ed entro che limiti, questi debba rispondere per i reati commessi dagli utenti del servizio.

6.2.1. I modelli di responsabilità dell'ISP.

Una parte della dottrina[220] distingue tre diversi ruoli sociali da attribuire al *provider*, ai quali associa altrettanti modelli di responsabilità penale.

Il primo paradigma idealtipico è quello del fornitore di servizi come *quivis de populo*, posto sullo stesso piano degli altri utenti di Internet, senza doveri di controllo rispetto a condotte altrui o obblighi di denuncia dei reati da altri commessi o oneri di collaborazione con le autorità nella repressione degli illeciti. Egli sarà penalmente responsabile nelle ipotesi di autoria e di concorso commissivo doloso nell'altrui condotta criminosa; risponderà, in altre parole, solo dei reati di cui è autore o alla cui commissione ha partecipato.

All'estremo opposto si colloca la figura dell'ISP come *controllore* e garante della tutela dei diritti nel cyberspazio; un tale modello si caratterizza per le penetranti limitazioni alla libertà di comunicazione, realizzate attraverso una censura preventiva del materiale caricato sulla piattaforma. In questa veste egli potrà essere ritenuto

competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività impedisca o ponga fine alle violazioni commesse».

[218] L'art. 17, comma 1, prevede che nella fornitura dei servizi di cui agli articoli 14, 15 e 16, *«il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite».*

[219] A ben vedere, le disposizioni non escludono *tout court* che il *provider* possa essere chiamato a rispondere; l'esenzione di responsabilità opera infatti soltanto alle condizioni stabilite dalla legge (regime c.d. di responsabilità limitata).

[220] Per approfondimenti di rinvia a INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 20 alla cui ricostruzione faremo riferimento nell'illustrare i modelli di responsabilità del *provider*.

responsabile per non aver impedito un fatto di reato commesso da altri *ex* art. 40, capoverso, c.p.

La figura del *provider* come *tutore dell'ordine* nello spazio virtuale si pone a metà strada tra le precedenti. In questa veste egli ha l'obbligo di denuncia degli illeciti di cui viene a conoscenza e di collaborazione con l'Autorità al fine di agevolare l'individuazione degli autori e attenuare le conseguenze dei reati commessi dagli utenti della piattaforma. Non ha alcun obbligo di verifica preventiva del materiale presente in rete, dovendo attivarsi unicamente *ex post* per ripristinare l'ordine violato. La violazione dei suddetti obblighi sarà sanzionata secondo il modello del reato omissivo proprio: il *provider* incorrerà in responsabilità penale laddove ometta di collaborare con gli inquirenti, ferma l'eventuale responsabilità per fatto proprio o per concorso attivo nell'altrui reato. Questo terzo paradigma ascrittivo è quello che sembra meglio descrivere il regime di responsabilità del *provider* delineato nel Codice del commercio elettronico.

Quale che sia il ruolo riconosciuto al *provider*, nessuno dubita che questi debba rispondere dei reati dallo stesso realizzati o commessi in concorso con gli utenti della piattaforma. Non è tuttavia agevole – tanto in relazione a specifiche fattispecie delittuose, quanto alla descrizione del contributo atipico – delimitare l'area di responsabilità[221]. A tal riguardo, ci si è chiesti in cosa debba sostanziarsi il contributo atipico di partecipazione dell'ISP e se la responsabilità a titolo di concorso commissivo soggiaccia alle regole comuni ovvero debba essere ricondotta a uno statuto autonomo. Secondo alcuni[222] il contributo atipico del fornitore del servizio soggiace alla ordinaria disciplina sul concorso di persone nel reato: è dunque sufficiente, da un punto di vista oggettivo che venga realizzato un illecito e che l'azione del *provider*, si traduca in una agevolazione, senza la quale il reato sarebbe stato ugualmente commesso, ma con maggiori incertezze o difficoltà; sul piano soggettivo si richiede un duplice proiezione volontaristica, consistente nella rappresentazione e nella volizione che sia realizzato un reato e di contribuire con la propria condotta al fatto dell'utente.

Altri ritengono che il *provider* debba beneficiare di uno statuto più garantista di responsabilità concorsuale, tale che lo si potrebbe ritenere colpevole soltanto quando il

[221] È pacifico che l'ISP possa rendersi responsabile di un reato informatico in senso stretto. A determinate condizioni potrà assumere la qualifica di operatore di sistema e commettere il reato in forma aggravata (*amplius*, con riferimento alla posizione del proprietario della *blockchain* privata, si veda il paragrafo seguente). La realizzazione monosoggettiva di reati non necessariamente informatici dipende invece dalla descrizione del fatto tipico. In molti casi è il contenuto intrinsecamente illecito (es. diffusione di materiale pedopornografico o coperto da copyright) o eventualmente illecito (delitti contro l'onore, istigazione a delinquere, procurato allarme etc.) del materiale diffuso a integrare gli estremi di un reato; laddove la fattispecie sia formulata in termini ampi non si pongono problemi di particolare rilievo, poiché il *provider* sarà responsabile in via autonoma qualora siano ravvisabili nella sua condotta attiva gli estremi del dolo.
In altri casi l'estensione della fattispecie incriminatrice ha sollevato alcuni dubbi sul rispetto del principio di tassatività, come ad es. per il delitto di favoreggiamento della prostituzione (art. 3, comma 1, n. 8 legge 20 febbraio 1958 n. 75). Cfr. INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 27.

[222] Cfr. PICOTTI, *La responsabilità penale dei service-providers in internet,* cit., 504 ss., DE NATALE, *Responsabilità penale dell'*internet service provider, cit., 323 ss.

fatto concretamente posto in essere sia assistito da un dolo di partecipazione particolarmente intenso e da un'oggettiva possibilità di impedire la commissione del reato[223].

Ci si è anche domandati se le esimenti di responsabilità contenute nel Codice del commercio elettronico possano in qualche modo incidere sull'accertamento responsabilità penale del *provider* per concorso (attivo) nel fatto illecito commesso dall'utente. Secondo una parte della dottrina le disposizioni testé richiamate escluderebbero la rilevanza penale dei contributi atipici dell'ISP alla realizzazione del fatto tipico qualora non siano almeno accompagnati, al momento della trasmissione o della memorizzazione dei dati, da una effettiva conoscenza del contenuto illecito degli stessi[224]. In tempi recenti è sempre più frequente imbattersi in fornitori di servizi che intervengono attivamente sulle informazioni in transito o archiviate sui propri *server,* al fine di trarre profitto. Non è chiaro se ciò sia sufficiente a integrare l'elemento della effettiva conoscenza e, di conseguenza, a far venir meno il regime di responsabilità limitata[225].

In giurisprudenza si rinviene un certo disorientamento nel delimitare i «servizi aggiuntivi» che valgono a mutare la natura dell'*hosting* provider da passivo ad attivo, facendo venir meno l'esimente di responsabilità[226].

---

[223] In tal senso, il concorso commissivo sarebbe integrato solo quando i dati vengano inseriti nel circuito di pubblico accesso dopo una positiva attività di vaglio sulle informazioni. Cfr. SEMINARA S., *La pirateria su internet e il diritto penale*, in *Riv. trim. dir. pen. ecom*., 1997, 1, 71 ss.

[224] Egli non sarà dunque responsabile per fatti commessi con colpa o imputati a titolo di colpa o di dolo eventuale. Nel dolo indiretto manca infatti nell'agente la rappresentazione certa (l'effettiva conoscenza) della realizzazione del reato. Non a caso nella versione inglese della Direttiva 2000/31/CE è utilizzato il termine «*actual knowledge*» che descrive un coefficiente psicologico assimilabile al 'nostro' dolo diretto.

[225] La Corte di Giustizia dell'Unione Europea nell'affermare che le deroghe alla responsabilità previste dalla direttiva sul commercio elettronico riguardano esclusivamente i casi in cui l'attività di prestatore di servizi della società dell'informazione sia di ordine «*meramente tecnico, automatico o passivo*», ha rimesso la valutazione di "neutralità" dell'*hoster* ai giudici nazionali. Cfr. CGUE, Cause riunite C-236/08 to C-238/08 *Google France*; C-324/09 *L'Oréal and Others* secondo cui «*in order to establish whether the liability of a referencing service provider could be limited under Article 14 of Directive 2000/31/EC, it was necessary to examine whether the role played by that service provider was neutral […] Article 14(1) of Directive 2000/31/EC was to be interpreted as applying to the operator of an online marketplace where that operator had not played an active role allowing it to have knowledge of or control over the data stored*».

[226] Secondo una tesi estensiva (maggioritaria in seno alla giurisprudenza civile) per qualificare l'*hoster* come attivo è sufficiente l'indicizzazione dei contenuti multimediali immessi dagli utenti o l'inserimento di messaggi pubblicitari personalizzati. Ad essa si contrappone una tesi restrittiva che esclude la natura di *hosting* provider "attivo", laddove il prestatore del servizio non intervenga in alcun modo sul contenuto caricato dall'utente, ma si limiti a sfruttarne commercialmente la presenza sul proprio sito. Il limite letterale all'esenzione da responsabilità è infatti la conoscenza dell'illiceità dei contenuti, non integrata in alcun modo da meccanismi automatici di filtraggio, indicizzazione, selezione o organizzazione dei contenuti. Sul tema, di recente, ACCINNI, *Profili di responsabilità penale dell'hosting provider "attivo",* cit., 9 ss, al quale si rinvia per gli opportuni approfondimenti bibliografici e giurisprudenziali.

6.2.2. In particolare: la responsabilità *per omissionem*.

La dottrina e la giurisprudenza dominante hanno apertamente rifiutato l'idea che l'ISP sia titolare di una posizione di garanzia penalmente rilevante. Si è parlato addirittura di un fuoco di sbarramento[227], finalizzato ad escludere l'esistenza di obblighi di garanzia per evitare che il *provider* divenisse una sorta di censore della rete. La questione è stata esaminata a partire dagli elementi strutturali del reato commissivo mediante omissione. Senza entrare ulteriormente nel merito della ricostruzione dogmatica, basti qui ricordare che l'esistenza di una posizione di garanzia postula, oltre alla individuazione di un obbligo di garanzia *ex* art. 40, comma 2, c.p., che si possa pretendere dal garante una determinata condotta (esigibilità) e che questi disponga del potere impeditivo specifico.

La dottrina dominante[228] ritiene che tali requisiti non siano soddisfatti con riferimento alla posizione del *provider* poiché manca una norma che fondi un generale obbligo di sorveglianza degli utenti della rete o dal quale possa ricavarsi la responsabilità per la protezione dei beni esposti a pericolo nel cyberspazio[229]. Un obbligo generale di sorveglianza non sarebbe del resto esigibile, dal momento che sui *server* di ciascun fornitore di servizi digitali transitano ogni secondo un'enorme quantità di dati, che rende materialmente impossibile esperire un controllo sul relativo contenuto.

Mancherebbe inoltre un potere impeditivo specifico, sia dal punto di vista giuridico che da quello fattuale. Dalla lettura congiunta degli artt. 14 ss. del D. Lgs. 70/2003 si ricava che i *provider* sono tenuti a impedire l'accesso ai dati (o altrimenti a rimuoverli) solo a seguito di richiesta della pubblica autorità; in tutti gli altri casi, la rimozione di materiale potrebbe dar luogo a un obbligo risarcitorio nei confronti dell'utente ingiustamente censurato. Dal punto di vista fattuale, si sottolinea come l'intervento del *provider* si colloca in un momento successivo rispetto alla commissione del reato, tale per cui egli – pur volendo – non potrebbe in alcun modo impedirne la consumazione.

Nell'attuale quadro normativo sembra dunque doversi concludere nel senso dell'insussistenza di obblighi di garanzia a carico del fornire di servizi[230]. L'assenza di obblighi generali di controllo è il frutto della accurata e consapevole ponderazione di interessi che il legislatore ha compiuto tra libertà ed efficienza della comunicazione e garanzia dei diritti individuali. Il precario equilibrio sarebbe compromesso se il fornitore di servizi indossasse le vesti del controllore e avesse la possibilità (*rectius*, il dovere) di censurare talune informazioni. L'ordinamento giuridico è tuttavia in continua evoluzione e la normativa di settore – come vedremo a proposito della

[227] L'espressione è di INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 47

[228] Si veda, tra i primi, il contributo di SEMINARA, *La responsabilità penale degli operatori su internet*, cit., 745 ss.

[229] È opportuno ribadire che l'art. 17 del Codice del commercio elettronico sancisce il principio, diametralmente opposto, dell'assenza di un obbligo generale di sorveglianza.

[230] Nella giurisprudenza più recente si veda Cass. Pen., Sez. V, 27 dicembre 2016, n. 54946; Cass. Pen., Sez. V, 8 novembre 2018, n. 12546;.

disciplina antiriciclaggio – potrebbe attribuire rilevanza penale, *ex* art. 40, cpv., all'omissione di determinati doveri giuridici[231].

L'aura di 'neutralità' che avvolge il *provider* svanisce non appena abbia conoscenza della commissione di reati o gli venga richiesto di attivarsi per impedire l'aggravamento delle conseguenze del reato. Il dovere di collaborazione è spesso presidiato da sanzioni di carattere amministrativo[232]; rimane tuttavia aperta la questione circa la rilevanza penale dell'eventuale inosservanza degli obblighi[233] e il rapporto tra il reato e gli illeciti amministrativi[234].

6.3. *Blockchain* private e ibride.

In apertura del paragrafo si è detto che la posizione di garanzia in *blockchain* è un tema reso particolarmente delicato dalle potenzialità criminogene della nuova tecnologia, in particolare per quel che riguarda le applicazioni nel settore economico-finanziario. In quella sede avevamo formulato una riserva sull'individuazione delle figure titolari di eventuali obblighi di garanzia, che è giunto il momento di sciogliere. L'ampia premessa teorica sulla posizione di garanzia penalistica e, più nel dettaglio, sugli obblighi del *provider* ci permette di approfondire ora il tema della responsabilità omissiva dei soggetti che professionalmente gestiscono l'infrastruttura DLT o operano su di essa.

---

[231] Una parte della dottrina (PICOTTI L., *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet*, in *Studium iuris*, 2007, 1207) ha individuato delle ipotesi residuali in cui sarebbe ipotizzabile una responsabilità del *provider* per omesso impedimento di reati, facendo leva sulla particolare incisività dei doveri imposti dalla disciplina di settore, ad es., gli artt. 14-*ter* e *quater* della legge 269/1998, che impongono all'ISP una stringente collaborazione con il Centro nazionale per il contrasto della pedopornografia in Internet (obbligo di immediata denuncia dei reati, obblighi di rimozione/inibitoria). Si tende tuttavia ad escludere anche in questo particolare ambito l'esistenza di una posizione di garanzia, poiché l'intervento dell'ISP avviene successivamente alla consumazione dell'illecito. L'assolvimento degli obblighi di segnalazione e collaborazione non potrebbe impedire il reato, ma soltanto di attenuarne le conseguenze: si è dunque fuori dal perimetro del reato omissivo improprio.

[232] Il legislatore sembra preferire il ricorso allo strumento della sanzione amministrativa per punire l'inosservanza degli obblighi facenti capo al fornitore di servizi digitali (art. 14-*ter*, comma 3, l. 269/1998; art. 21, D. Lgs. 65/2018). La *ratio* della scelta è da ravvisarsi nella maggiore opportunità di configurare come illecito amministrativo condotte di mera inosservanza, limitando l'intervento del diritto penale ai soli casi di lesione o concreto pericolo per il bene giuridico protetto.

[233] La responsabilità penale per omissione degli obblighi di denuncia/rimozione è affidata alle disposizioni di comuni. In caso di omessa denuncia potrebbero ricorrere gli estremi del favoreggiamento personale (art. 378 c.p.), che la giurisprudenza ritiene configurabile anche mediante un *non facere* antidoveroso.

La violazione dell'obbligo di rimozione del materiale illecito o di inibizione all'accesso su richiesta dell'autorità competente può integrare il delitto di mancata esecuzione dolosa di un provvedimento del giudice (art. 388 c.p.) soltanto se il fornitore del servizio compia atti fraudolenti diretti ad eludere i predetti obblighi e si tratti di un provvedimento giurisdizionale. Diversamente, il fatto sarà inquadrato nella contravvenzione di cui all'art. 650 c.p. che punisce (anche a titolo di colpa), l'inosservanza di provvedimenti dell'autorità emessi, come nel caso di specie, per ragioni di giustizia.

[234] Una parte della dottrina (INGRASSIA, *Il ruolo dell'ISP nel ciberspazio*, cit., 63) ritiene che, laddove l'inosservanza costituisca illecito amministrativo, il principio di specialità previsto dall'art. 9 della legge 689/1981 farebbe venir meno la possibilità di applicare l'art. 650 c.p.

Occorre fin da subito precisare come vi sia un parallelismo tra la responsabilità dei gestori delle infrastrutture decentralizzate e quella del *provider*, dal momento che, tanto nel primo quanto nell'altro caso, l'attività consiste nel mette a disposizione di un certo numero di utenti – che sia o meno determinato – servizi consistenti nella registrazione e della trasmissione di dati informatici. Medesime sono dunque le esigenze connesse alla individuazione di un destinatario dei doveri di collaborazione con l'Autorità per impedire la commissione di reati o attenuarne le conseguenze lesive.

Si tratterà anzitutto di precisare quali sono le figure in posizione "qualificata" che operano nel settore considerato, donde stabilire se gravi in capo ad essi un obbligo di garanzia ai sensi dell'art. 40, comma 2, c.p. Si dovrà poi stabilire se a detti soggetti si applichi il particolare regime di responsabilità previsto dalla normativa sul commercio elettronico e quali siano i doveri di collaborazione posti a loro carico. Per affrontare il tema in modo analitico è opportuno ricorrere a una *summa divisio* in base alla struttura e alla titolarità del sistema decentralizzato, distinguendo tra *blockchain* pubbliche e private che, come si vedrà, presentano profonde differenze in punto di imputazione degli effetti giuridici. Concentreremo ora l'attenzione su queste ultime, rinviando al prosieguo della trattazione l'esame delle problematiche connesse alla titolarità dei sistemi pubblici *permissionless*[235].

Le *blockchain permissioned* sono controllate un'autorità centrale che determina le condizioni di accesso, la posizione che ciascun utente può ricoprire all'interno della stessa, e le regole sulla visibilità dei dati registrati. Si rende così possibile una *governance* dell'infrastruttura, attraverso il recupero dell'idea di centralizzazione in una rete che nasce come decentralizzata e distribuita. Si è già detto che le caratteristiche delle *blockchain permissioned* le rendono più interessanti agli occhi delle grandi imprese e degli attori istituzionali, che hanno iniziato a impiegarle in numerosi progetti[236]. La fiducia degli utenti o di coloro che vi operano non è tanto (o soltanto) nell'infrastruttura in sé, ma nell'organizzazione che ne ha il controllo, ritenuta altamente affidabile e imparziale[237]. Il gestore della rete inoltre, ha inoltre il potere di modificare le regole di funzionamento e il protocollo di formazione del consenso.

È bene precisare che la natura *permissioned* del sistema non vale da sé a qualificare la *blockchain* come privata, essendovi alcuni esempi – anche degni di nota – di sistemi pubblici sottoposti ad autorizzazione[238]. Queste infrastrutture sono anche dette ibride poiché nascono dalla commistione di requisiti di pubblicità con meccanismi del consenso piuttosto restrittivi: alcuni nodi hanno una influenza maggiore rispetto agli

[235] *Infra*, § 6.5.
[236] Le *blockchain permissioned* vengono ritenute più scalabili, anche se meno sicure di quelle pubbliche. Esse permettono infatti di controllare i dati registrati, ma anche di apportare modifiche alla catena dei blocchi (*supra*, Cap. I, § 2.2.).
[237] Si pensi, ad esempio, alla tenuta di un database distribuito tra più società per la registrazione di fatture e/o documenti contabili che sia controllata da un ente esterno o dal dipartimento IT di una di esse. Il protocollo informatico per la gestione degli accessi o per la formazione del consenso potrebbe essere modificato dal titolare dell'infrastruttura in ogni momento.
[238] Si pensi all'infrastruttura di Ripple, in cui l'accesso al ruolo di *miner* è limitato ad un numero esiguo di individui considerati fidati.

altri e possono decidere quali transazioni convalidare; il sistema è accessibile al pubblico a determinate condizioni ma non tutti i *contributors* sono posti sullo stesso piano[239].

Si può dunque notare come la vera differenza tra sistemi *permissioned* e *permissionless* è nel numero degli attori che, all'interno della rete, ha il potere di assumere determinate decisioni; l'infrastruttura sarà tanto più centralizzata quanto minore è il numero di partecipanti o di soggetti che su autorizzazione possono prendervi parte. La concentrazione di "potere" raggiunge l'apice nelle *fully private blockchain* nelle quali vi è una organizzazione che ha il controllo esclusivo sulla convalida delle transazioni e sulla tenuta dei registri[240]. Una piattaforma di questo tipo non presenta differenze significative rispetto ai tradizionali database centralizzati, dai quali si distingue soltanto per l'utilizzo della crittografia come strumento di sicurezza e verifica.

Posto dunque che nei sistemi *permissioned* – indipendentemente dalla possibilità di un ingresso di altri partecipanti – esiste sempre un *board* decisionale facente capo a uno o più soggetti, si dovrà stabilire quale siano le conseguenze in termini penalistici della particolare posizione rivestita in seno all'organizzazione decentralizzata.

6.3.1. *Blockchain permissioned* e titolarità del sistema.

Un primo nodo da sciogliere è quello relativo alla assunzione della qualifica di "operatore di sistema" da parte degli apicali dell'organizzazione che sovrintende alla tenuta dei registri (*validator*) e dei singoli partecipanti dotati del potere di voto.

Il legislatore codicistico attribuisce rilevanza alla figura del *Sysop* nel prevedere un aumento di pena per i principali reati informatici. Più precisamente, fu per la prima volta la legge 23 dicembre 1993, n. 547 a introdurre due circostanze aggravanti a effetto speciale collegate al possesso della qualifica di operatore di sistema per i delitti di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche (art. 617-*quater*, comma 2) e di frode informatica (art. 640-*ter*, comma 2); la legge 18 marzo 2008 n. 48 di ratifica della Convenzione di Budapest ha esteso dette aggravanti anche ai reati di reato di accesso abusivo a sistema informatico (art. 615-*ter*, comma 2) e di danneggiamento di dati e sistemi informatici (artt. 365-*bis* e seguenti). L'aumento di pena per l'abuso della qualità di operatore del sistema si giustifica a causa della

[239] Secondo SARZANA DI S. IPPOLITO F., NICOTRA M., *Diritto della blockchain, Intelligenza artificiale e Iot*, Milano, 2018, 21 le *blockchain* ibride possono utilmente essere impiegate nei casi in cui il registro delle transazioni deve rimanere pubblico, ma, al contempo, occorre garantire che soltanto alcuni nodi abbiano il potere di registrare le transazioni. Si pensi a un sistema per la registrazione di documenti nell'ambito di un procedimento amministrativo che vede coinvolte più pubbliche amministrazioni, in cui ciascuna di esse può esprimere una propria posizione e registrarla in modo trasparente e pubblicamente verificabile.

[240] In una *blockchain* totalmente privata non è necessario stabilire incentivi economici che garantiscano il buon funzionamento del sistema. La possibilità di scaricare il *software* è solitamente ristretta a pochi soggetti che per la fruizione del registro o l'accesso al *database* dovranno pagare un corrispettivo.

maggiore facilità di intervento che tale mansione offre al soggetto agente[241], da cui deriva una maggiore particolare pericolosità sociale in considerazione del suo rapporto privilegiato con il sistema[242].

La dottrina si è a lungo interrogata sui presupposti per individuare l'operatore di sistema, essendo questa una espressione normativamente vaga e indefinita. Alcuni hanno sostenuto che rivesta una tale qualifica qualsiasi tecnico legittimato ad operare sul computer[243]; altri, in senso opposto, la ravvisano soltanto in capo ai tecnici che controllano le varie fasi di elaborazione dei dati, escludendo l'operatore addetto a funzioni meramente esecutive[244]. Si è pure prospettata una tesi intermedia secondo cui la qualifica *de qua* è propria di tutti i soggetti che possono legittimamente operare sul sistema e che godono delle qualifiche professionali o di conoscenze specifiche rispetto a quelle di un qualsiasi altro utente del sistema[245].

A nostro avviso, il punto di partenza è dato dalla *ratio* della norma, da ravvisarsi nella necessità di punire più incisivamente coloro che, approfittando delle autorizzazioni all'accesso e del particolare rapporto con il sistema informatico o telematico, ne abbiano alterato o compromesso il funzionamento. A tal fine, non pare necessario che il *system operator* abbia il controllo del sistema informatico o telematico o che rivesta una posizione di vertice all'interno dell'ufficio IT, dovendo al contrario attribuirsi rilevanza anche a compiti ordinari di verifica, aggiornamento e manutenzione del sistema. Ne consegue che anche il semplice tecnico autorizzato al rilascio dei certificati di accesso, l'incaricato alla gestione delle *password* o l'addetto all'aggiornamento dell'*antivirus* dovranno rispondere dei delitti in forma aggravata.

La posizione rivestita in seno all'impresa e i poteri propri della funzione non concorrono quindi a riempire di contenuto la qualifica di operatore di sistema, che spetterà indifferentemente tanto all'apicale, quanto al subordinato, che dispongano delle autorizzazioni necessarie ad intervenire sull'*hardware* e sul *software*. Ne consegue che anche il titolare del sistema[246] che gestisca in proprio determinate risorse

---

[241] In questo senso Cass. Pen., Sez. II, 11 novembre 2009 n. 44720 ha affermato che l'operatore di sistema, abusando della propria posizione, viola un dovere di fedeltà cui è tenuto sia nei confronti del titolare del sistema informatico da lui delegato, sia delle persone i cui interessi economici sono presi in carico da quel sistema (vicenda in cui l'imputato, dopo essersi appropriato della *password* rilasciata ad un terzo, responsabile di zona di una compagnia assicurativa, manipolava i dati del sistema, predisponendo false attestazioni di risarcimento dei danni).

[242] Cfr. D'AIETTI G., *La frode informatica*, in BORRUSO R., BUONOMO G., CORASANTI G., D'AIETTI G., *Profili penali dell'informatica*, Milano, 1994, 39; PECORELLA, *Diritto penale dell'informatica,* cit., 115.

[243] D'AIETTI, *La frode informatica*, cit., 27

[244] POMANTE G., *Internet e criminalità*, Torino, 1999, 31

[245] Tesi autorevolmente sostenuta da MUCCIARELLI F., *Commento all'art.10 della legge 547 del 1993*, in *Legislazione Penale*, 1996, 136.

[246] Per titolare del sistema si intende il soggetto proprietario dell'infrastruttura. Nelle organizzazioni complesse la titolarità del sistema va verosimilmente riferita al vertice della *governance*, in grado di determinare le modalità e le finalità dell'utilizzo del sistema stesso. A tale figura fanno riferimento le Sezioni Unite che, nel dirimere il contrasto interpretativo sulla configurabilità del delitto di cui all'art. 615-*ter* c.p. da parte del soggetto astrattamente legittimato all'accesso, hanno affermato che il giudizio sull'abusività della condotta deve essere parametrato alla violazione delle condizioni e dei limiti imposti dal titolare del sistema (Cass. Pen., Sez. Un., 27 ottobre 2011, n. 4694, *Casani*).

o funzionalità[247] potrà essere ritenuto, per quel segmento di attività, un operatore di sistema[248].

Venendo ora all'oggetto della nostra indagine, risulta abbastanza evidente che il proprietario della *blockchain* totalmente privata possiede la qualifica penalistica di operatore di sistema[249]. Egli è invero l'operatore per eccellenza, l'unico in grado di intervenire sulle informazioni registrate in *blockchain* e di modificare la catena dei *record*. Ben si giustifica a carico di costui la previsione di un trattamento sanzionatorio più aspro, stante il maggior disvalore di azione che caratterizza il reato informatico eventualmente posto in essere. A differenza delle *blockchain* pubbliche (*trustless network*), nelle reti private gli utenti ripongono fiducia in coloro che promuovono e sovrintendono al progetto (*trusted network*); si comprende pertanto come l'abuso della posizione dia luogo a una violazione del rapporto fiduciario alla base della decisione di investimento o di utilizzo dell'infrastruttura[250].

La posizione dei partecipanti nelle *blockchain permissioned* pubbliche o private è sicuramente più complessa. Se da una parte essi non dispongono, *uti singuli*, del potere di intervenire sui dati registrati, ma soltanto di validare le transazioni, di verificare le informazioni in *input* o di esprimere un voto; dall'altra il protocollo del consenso permette a un qualificato numero di nodi di assumere decisioni rilevanti e di modificare dati e impostazioni altrimenti immutabili.

---

[247] Supponiamo che un sistema informatico permetta l'accesso all'anagrafica storica aziendale soltanto dall'*account* dell'amministratore delegato. Se questi decidesse di cancellare tutti i dati informatici, difficilmente si potrà negare la configurabilità del reato di cui all'art. 635-*bis* c.p. in forma aggravata dall'abuso della qualità di operatore di sistema; nessun'altro soggetto potrebbe infatti accedere o modificare quelle informazioni, rispetto alle quali egli è di fatto l'unico "operatore" di sistema.

[248] La definizione è dunque più ampia rispetto a quella di "amministratore di sistema" che individua, in ambito informatico, le figure professionali incaricate della gestione e della manutenzione di un impianto di elaborazione o delle sue componenti. Il Provvedimento del Garante Privacy del 27 novembre 2008 (*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*) considera tali anche altre figure, equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi *software* complessi. Gli amministratori di sistema pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo nelle loro consuete attività sono – secondo l'Autorità – in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati. La normativa di settore precedente al riordino del 2003 definiva l'amministratore di sistema come il «*soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione*» (art. 1, comma 1, lett. c) d.P.R. 318/1999). Rinviando al citato provvedimento dell'Autorità per gli opportuni approfondimenti, basti qui rilevare come la figura dell'amministratore di sistema possa essere descritta come un cerchio concentrico di minori dimensioni rispetto a quella dell'operatore di sistema, che ricomprende anche ruoli di carattere meramente operativo.

[249] Anche in questo caso la qualifica andrà riferita tanto al titolare del sistema (*idest,* il vertice della società), quanto a coloro che gestiscono il sistema su delega di questi (gli esperti informatici addetti alla manutenzione dei registri distribuiti).

[250] Ci si riferisce tanto a coloro che, confidando nella buona riuscita del progetto, hanno acquistato *token* (in una ICO o presso un *exchange*), quanto agli utilizzatori della piattaforma che se ne servono per effettuare scambi o compiere altro tipo di attività giuridica, riponendo fiducia nella immodificabilità del registro delle transazioni.

Risulta evidente che il solo fatto di contribuire alla tenuta dei registri o alla conferma delle transazioni non è sufficiente a rendere costoro "operatori di sistema"; ci si chiede piuttosto se possano assumere una tale qualifica al momento in cui – a maggioranza, secondo i meccanismi del consenso – intervengono sui dati registrati nel sistema. A nostro avviso il possesso della qualifica dovrà essere esaminato non in astratto, in relazione al ruolo e ai compiti attribuiti a ciascun partecipante, bensì in concreto tenuto conto della specifica operazione *hic et nunc* compiuta[251]. In tal senso, le regole sulla formazione del consenso permetteranno a soggetti privi di poteri di intervento attivo di instaurare un rapporto "qualificato" con il sistema informatico, tale da renderli *system operator* sul piano penalistico. L'eccesso di potere da parte della maggioranza[252] dovrà pertanto essere considerato un abuso della qualità di operatore di sistema, atteso che la manipolazione dei dati non sarebbe stata altrimenti possibile; i partecipanti che, abusando delle regole del consenso, abbiamo commesso un reato, dovranno dunque risponderne in forma aggravata[253].

In conclusione, riteniamo che nelle infrastrutture *blockchain* la figura dell'operatore di sistema non possa essere individuata in modo statico o sulla base di rigido rapporto con il sistema decentralizzato, dovendo al contrario essere valutata in relazione ai meccanismi del consenso che regolano la validazione dei dati e l'intervento sulle informazioni registrate.

6.3.2. *Blockchain permissioned* e posizione di garanzia.

L'analisi svolta nel paragrafo precedente ha condotto all'individuazione di alcune categorie di soggetti – nella specie il titolare del sistema e la maggioranza dei partecipanti – che possiedono (o possono possedere) la qualifica di operatore di sistema. Questo primo approdo ci consente di passare ora all'esame della questione

[251] A tal riguardo sia consentito richiamare il dibattito, ormai superato, sull'attribuzione qualifica di pubblico ufficiale o incaricato di pubblico servizio (artt. 357 e 358 c.p.) che, com'è noto, ha visto contrapporsi due criteri. Con la riforma del 1990 si ebbe il passaggio dal criterio soggettivo a quello oggettivo-funzionale, che condusse a uno spostamento del baricentro verso un accertamento di tipo relativo; si affermò la tesi secondo cui la disciplina pubblicistica dell'attività andasse esaminata non in astratto, bensì con riferimento allo specifico segmento di attività. In dottrina, senza pretese di esaustività, FIORELLA A., *Ufficiale pubblico, incaricato di un pubblico servizio, o di un servizio di pubblica necessità*, in *Enc. dir.*, 1992, XLV, 563 ss.; PICOTTI L., *Le nuove definizioni penali di pubblico ufficiale e di incaricato di pubblico servizio nel sistema dei delitti contro la pubblica amministrazione*, in *Riv. trim. dir. pen. econom*, 1992, 264 ss.; SEVERINO P., *Pubblico ufficiale e incaricato di un pubblico servizio* voce, in *Dig. disc. pen.*, X, 508 ss.; ROMANO M., *I delitti contro la pubblica amministrazione. I delitti dei privati. Le qualifiche soggettive pubblicistiche*, in ID., *Commentario sistematico al codice penale*, Milano, 2013, 16 ss.; GAMBARDELLA M., *Art. 357*, in LATTANZI G., LUPO E. (a cura di), *I delitti contro la pubblica amministrazione*, Milano, 2010, 913 ss.

[252] Che, a seconda dei casi, potrà consistere nell'intervento senza diritti su dati e informazioni, nell'eliminazione di file o nella dolosa interruzione del funzionamento del sistema commessi in violazione del consenso o superando i limiti dello stesso.

[253] Il riferimento è ai reati per i quali è prevista l'aggravante dell'abuso della qualità di operatore di sistema (cfr., in questo stesso paragrafo, *supra*).

centrale, relativa alla configurabilità in capo alle figure qualificate di un obbligo giuridico di garanzia rilevante *ex* art. 40, comma 2, c.p.

L'attenzione andrà rivolta dapprima ai sistemi decentralizzati sottoposti ad autorizzazione, privati o ibridi, nei quali per definizione è possibile rinvenire uno o più soggetti in posizione sovraordinata. Successivamente l'analisi sarà estesa al contesto – decisamente più problematico – delle *blockchain* pubbliche, nelle quali manca *tout court* un centro di imputazione degli effetti giuridici.

Il titolare del sistema è indubbiamente il miglior "candidato" al ruolo di garante. In quanto proprietario dell'infrastruttura, egli ha piena disponibilità degli elaboratori interconnessi, potendo assumere ogni decisione relativa funzionamento e alla continuità operativa del servizio. Anche laddove si tratti di una rete parzialmente decentralizzata[254], il titolare conserva un pieno potere dispositivo sul protocollo informatico (*software*) di sistema mediante il quale potrà determinare l'*an* e il *quomodo* di funzionamento dell'infrastruttura.

A nostro modo di vedere, la figura del titolare del sistema presenta forti similitudini con quella del *provider*. Si è già detto come nei sistemi *permissioned* la decentralizzazione sia il più delle volte soltanto apparente[255]: l'accentramento del potere decisionale in capo a un soggetto fa venir meno il concetto di condivisione *peer-to-peer* in favore nel tradizionale modello *client-server*. Se il sistema è messo a disposizione di altri soggetti per il compimento di attività giuridica o la fruizione dei contenuti registrati in *blockchain,* il proprietario agisce come un *provider* di servizi.
Più precisamente, si tratterà di un servizio di *hosting* consistente nella memorizzazione delle informazioni e nell'archiviazione di dati in transito (*storage* di informazioni), al fine di renderli reperibili a utenti remoti[256]. Se il fornitore non compie alcuna indicizzazione o elaborazione dei *file* registrati troverà applicazione il regime di responsabilità limitata previsto per il c.d. *host* c.d. passivo[257]. L'impossibilità di configurare un obbligo penalistico di garanzia può ricavarsi in via immediata dalla disposizione, più volte citata, che sancisce l'assenza del dovere di sorveglianza (art. 17 D. Lgs. 70/2003). Né potrebbe ritenersi che la prestazione del servizio assuma rilevanza

[254] Il titolare di una *blockchain* privata potrebbe decidere di autorizzare altri soggetti (*contributors*) alla verifica delle transazioni e alla tenuta dei registri. In tal caso, pur non avendo la proprietà dell'intero sistema telematico, ma soltanto di una parte dei computer che lo compongono, sarà comunque in grado di esercitare un potere impositivo mediante l'aggiornamento del *software*.
[255] *Amplius,* Cap. I §, 2.2.
[256] Art. 16 D. Lgs. 70/2003 (v. *supra,* § 6.2.). Il titolare di una *blockchain* privata opera esattamente come un *content provider*. Previa validazione, le transazioni sono registrate sulla piattaforma e conservate in modo duraturo, senza alcun intervento sui dati e sulle informazioni.
[257] Il prestatore non sarà dunque responsabile delle informazioni memorizzate a condizione che: (i) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita; (ii) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. In argomento, ACCINNI, *Profili di responsabilità penale dell'*hosting provider *"attivo*", cit., 2 ss.; PANATTONI, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di* notice and take down, cit., 249 ss.

quale attività in sé pericolosa[258]; la necessaria giuridicità della posizione di garanzia tende infatti ad escludere da panorama delle fonti le situazioni meramente fattuali che concreterebbero il rischio di una violazione del principio di legalità[259].

Emerge parimenti l'assenza di un reale potere impeditivo nelle mani del titolare dell'infrastruttura. Al riguardo può notarsi – in linea con quanto si è detto a proposito della responsabilità *provider*[260] – come l'obbligo di azione sorga con effettiva conoscenza dell'attività illecita o per effetto della segnalazione dell'Autorità, in un tempo in cui il reato è stato ormai commesso[261]. Ciò dimostra che in nessun caso egli avrebbe il potere/dovere di prevenire il reato, poiché l'intervento si colloca in una fase in cui è materialmente impossibile il compimento dell'azione impeditiva idonea[262]. Si deve pertanto concludere che il proprietario della *blockchain* non è titolare di una posizione di garanzia volta ad impedire la commissione di reati da parte degli utenti del servizio.

L'assimilazione tra la figura di costui e quella dell'*hosting provider* fornisce un argomento ulteriore, di segno positivo, che porta ad escludere l'esistenza di un obbligo

---

[258] In tal senso v. RESTA, *La responsabilità penale del provider: tra laissez faire ed obblighi di controllo*, cit., 1725 secondo cui non è possibile ravvisare nell'attività del *provider «gli estremi di un'attività pericolosa suscettibile di imporre un obbligo di attivazione, dal momento che la mera fornitura di un accesso ad internet, […] rappresenta una condotta eccessivamente distante rispetto alla soglia del pericolo di realizzazione del fatto tipico […]».* Contra v. SGUBBI F., *Parere pro-veritate*, in *Dir. inf.*, 2009, 2, 746, che a margine della nota vicenda *Google vs Vividown* osserva che *«la gestione di un sito nel quale chiunque può caricare un proprio video con una semplice operazione di upload è senza dubbio esercizio di attività pericolosa per i beni altrui, considerata anche la potente diffusività dei messaggi diffusi a mezzo internet»*.

[259]Alcuni annoverano la precedente attività pericolosa tra le fonti della posizione di garanzia tutte le volte in cui essa dia luogo a una situazione di pericolo per i terzi, a fronte della quale il soggetto deve attivarsi per impedire che si concretizzi nella lesione di beni altrui (v. *supra*, § 6.2.2.). Per una critica, MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 350.

[260] La giurisprudenza è ferma nel ritenere che il *provider* non riveste una posizione di controllo penalmente rilevante. Tra le pronunce più rilevanti figura quella del Tribunale di Milano sul caso Google (Trib. Milano, 12 aprile 2010, n. 1972, 104 ss) nella quale l'estensore ha opportunamente precisato che: non esiste un obbligo di legge codificato che imponga agli ISP un controllo preventivo delle innumerevoli serie di dati che passano ogni secondo nelle maglie dei gestori o proprietari dei siti web; anche ammettendo, controfattualmente, un obbligo di impedire i reati in capo all'ISP, questo gli imporrebbe un controllo preventivo su tutto il materiale immesso in rete, cioè una condotta inesigibile data l'estrema difficoltà tecnica di controllare una miriade di dati; l'obbligo del *provider* di impedire l'evento diffamatorio, imporrebbe allo stesso un controllo o un filtro preventivo su tutti i dati immessi ogni secondo sulla rete, causandone l'immediata impossibilità di funzionamento. In dottrina v. INGRASSIA, *Il ruolo dell'ISP nel* ciberspazio, cit., 52; CORRIAS LUCENTE G., *La pretesa responsabilità penale degli intermediari di contenuti in internet*, in *Dir. inf..*, 2009, 1, 91 ss.; LOTIERZO R., *Il caso* Google-Vivi Down *quale emblema del difficile rapporto degli* internet providers *con il codice della* privacy, in *Cass. Pen*., 2010, 5, 4003 ss.; MANNA, DI FLORIO, *Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider*, cit., 892.

[261] Il dovere di collaborazione è imposto al fine di limitare le conseguenze dannose del reato e di agevolare la ricerca dei responsabili. La *ratio* delle norme pare dunque escludere già sul piano logico l'esistenza di un potere/dovere di carattere impeditivo.

[262] Secondo la dottrina più autorevole affinché la responsabilità omissiva impropria sia conforme al principio di personalità della responsabilità penale, occorre che l'obbligo giuridico impeditivo sia preesistente rispetto alla situazione di pericolo. Il garante deve non solo essere in condizione di attivarsi per prevenire l'*eventus damni,* ma anche di poter materialmente intervenire per compiere l'azione impeditiva idonea. Cfr. MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 343.

generale di sorveglianza sulle informazioni registrate sulla piattaforma, fermo restando che, in assenza di clausole espresse di limitazione della responsabilità, le conclusioni non sarebbero affatto diverse. Tra i doveri che la legge civile pone in capo al proprietario, non se ne riviene alcuno sufficientemente specifico da poter essere tratto a fondamento dell'obbligo di garanzia[263]. Allo stesso modo la normativa di settore non prevede alcun obbligo qualificato di attivazione a carico del gestore dell'infrastruttura digitale; la generica previsione di un dovere di assicurare la sicurezza della rete e dei sistemi informativi o del trattamento dei dati[264] non pare sufficiente a fondare un obbligo di garanzia penalmente rilevante. Le diposizioni settoriali sembrano rivolte al raggiungimento di un obiettivo – un alto livello di sicurezza informatica – piuttosto all'imposizione di doveri o misure di sicurezza. Si comprende quindi come esse siano inidonee a individuare un preciso comportamento idoneo a prevenire la commissione di un reato.

Esaminando la questione dalla prospettiva del potere impeditivo facente capo al *provider*, si deve porre in evidenza come il controllo preventivo sulle informazioni registrate in *blockchain* diviene tanto più inesigibile quanto maggiore è il numero di utenti che utilizza la piattaforma e/o "neutrale" l'informazione registrata. Si pensi ad esempio a una infrastruttura decentralizzata per la circolazione di *token* di pagamento, che, oltre a essere aperta a tutti i potenziali interessati/investitori, archivia dati che non rendono in sé manifesto il compimento di attività illecita[265]. In questi casi anche con l'ausilio della migliore scienza o delle tecniche più evolute la prevenzione dei fatti di reato tende a sfuggire al *dominium* dell'uomo.

Escluso che il proprietario/gestore di una *blockchain* privata o ibrida rivesta una posizione di garanzia volta ad impedire la commissione di reati – salvo quanto si dirà poco oltre a proposito della prevenzione del riciclaggio – ci si domanda se le medesime conclusioni possano valere anche per le altre figure soggettive. La risposta è chiaramente affermativa, sia pur con le precisazioni che seguono.

Le organizzazioni decentralizzate si caratterizzano per la presenza di una *governance* interna e di meccanismi del consenso che permettono alla maggioranza degli utenti di assumere determinate decisioni, intervenendo sui dati immessi nei

[263] Nelle materie in cui è più avvertita l'esigenza di individuare figure in posizione di garanzia (es. attività medico-chirurgica, sicurezza sul lavoro), la responsabilità *per omissionem* non viene ricostruita sulla base del rapporto giuridico tra il soggetto e la *res* (macchinario, impianto, struttura clinica), ma sui doveri specifici che derivano dal possesso dello *status* o da espresse previsioni di legge. Cfr. BLAIOTTA, *Causalità giuridica*, cit., 215.

[264] Si vedano, ad esempio, gli artt. 32 ss. del Regolamento 679/2016 UE sulla sicurezza del trattamento dei dati personali; gli artt, 14 ss. della Direttiva 1148/2016/UE (c.d. Direttiva NIS) e gli artt. 12 ss. D. Lgs. 18 maggio 2018 n. 65 relativamente agli obblighi di sicurezza gravanti sugli operatori dei servizi essenziali e sui fornitori di servizi digitali; gli artt. 51 ss. del D. Lgs. 7 marzo 2005, n. 82 e la normativa secondaria adottata dall'AgID per la sicurezza del trattamento effettuato dalle pubbliche amministrazioni.

[265] Basti pensare a fenomeni come il riciclaggio o il finanziamento del terrorismo, la cui esistenza non dipende dalla transazione in sé, ma da fattori esterni rispetto al trasferimento dei valori quali la destinazione delle risorse o la provenienza delittuosa del denaro o delle utilità (v. *infra*, Cap. III, § 3.1. ss.).

registri distribuiti. Le argomentazioni a favore dell'insussistenza di un obbligo di garanzia in capo al titolare del sistema varranno *a fortiori* anche per coloro che vi partecipano. Con l'ulteriore precisazione che sarebbe inconcepibile attribuire un dovere di azione – penalmente sanzionato – a una 'maggioranza' che non preesiste rispetto alla decisione da intraprendere e non ha, dunque, autonoma soggettività giuridica.

Si deve altresì escludere che un tale obbligo gravi sui singoli partecipanti (*miners, forgers* o *contributors*) impegnati nella validazione delle transazioni. Più volte abbiamo ribadito come l'attività di *mining* sia totalmente automatizzata e consista in una mera verifica formale sul rispetto delle regole[266] da parte degli utenti del servizio associata alla risoluzione di un enigma crittografico. I *miners* non processano informazioni in chiaro ma soltanto numeri in formato binario: ciò rende evidente come nessun controllo effettivo sulle informazioni possa essere esperito.

Su un piano diverso va affrontata la questione relativa alla responsabilità dei validatori che effettuano un vaglio preventivo del materiale immesso in rete. Ipotizziamo che il programmatore di uno *smart contract* avente come causa il finanziamento di una associazione terroristica decida di renderlo disponibile su un sistema di registri distribuiti[267]; che il sistema sia basato su una *blockchain* privata *permissioned* in cui i singoli nodi della rete, in modo casuale o alternato, siano chiamati validare la richiesta del programmatore previa verifica del funzionamento del *software*; che, pur emergendo in modo manifesto l'illiceità del programma, il validatore incaricato decida comunque di dare corso alla richiesta e di autorizzare la diffusione dello *smart contract*. Nel caso appena considerato il soggetto *miner* potrà certamente essere ritenuto responsabile per concorso nel reato di cui all'art. 270-*quinquies*.1. c.p. avendo questi agevolato la raccolta di denaro destinato a essere utilizzato per finanziare l'associazione terroristica. Si tratterà comunque di un concorso attivo, per aver materialmente contribuito alla diffusione del programma nella consapevolezza e volontà (anche in forma eventuale) della finalità dello stesso e della concomitante azione delittuosa altrui[268].

6.4. Organizzazioni autonome decentralizzate, *governance* interna, e controlli societari. Alcuni spunti di riflessione.

[266] Nella maggior parte dei casi l'oggetto dell'accertamento si limita al mero riscontro formale dell'appartenenza del potere (di spendita o di input) al soggetto che intende usufruire dell'applicativo.
[267] Si pensi a un contratto denominato "Islamic State found-raising" la cui illiceità emerge chiaramente, oltre che dalla denominazione, anche dall'indirizzo di destinazione delle somme, noto per essere pubblicato su numerosi forum di discussione del *dark web*.
[268] Un addebito per omesso impedimento del reato *ex* art. 40, comma 2, c.p. sarà configurabile soltanto nell'ipotesi in cui il validatore ometta *tout court* il controllo dovuto e sia previsto, alla scadenza del termine, il rilascio automatico dell'autorizzazione. In questo caso è possibile ritenere che il validatore rivesta una posizione di garanzia di origine contrattuale (accordo con il titolare del sistema sull'attività da svolgere per verificare il funzionamento degli *smart contract* che gli utenti intendono mettere a disposizione), che potrà essere assunta a fondamento della responsabilità per concorso omissivo nel reato altrui purché vi sia la prova del dolo di partecipazione.

Come noto, quello dei controlli intrasocietari è un tema caro alla dottrina penalistica, che vede in esso uno dei precipitati normativi della crisi di fiducia e del conflitto di interessi alla base del capitalismo moderno[269]. Sebbene la questione riguardi in modo soltanto marginale l'oggetto nella presente trattazione, emergono alcuni profili meritevoli di attenzione. Ci si potrebbe chiedere se nelle organizzazioni autonome decentralizzate ciascun partecipante sia investito del potere/dovere di prevenire una decisione illecita assunta dalla maggioranza.

La dottrina statunitense ha paragonato tali organizzazioni a vere e proprie società virtuali, partendo dall'ampia definizione di *general partnership*[270] contenuta nell'*uniform partnership act* e condivisa dalle corti americane[271]. In esse si realizza una sorta di commistione tra proprietà e controllo: gli acquirenti di *token* assumono le vesti di *stakeholder* e, in quanto soci, dispongono del diritto di voto; le scelte di *governance* sono regolate tramite *smart contract* e sottoposte ai meccanismi del consenso in *blockchain*[272]. Le organizzazioni autonome decentralizzate possono essere costituite con l'intento di esercitare una attività imprenditoriale[273], dando così luogo a una vera e propria impresa virtuale distribuita. Non essendo questa la sede opportuna per entrare nel merito nella qualificazione giuridica del fenomeno in base al diritto commerciale, possiamo qui limitarci a dare per assunto che una organizzazione di questo tipo possa essere considerata una società di fatto[274].

---

[269] Di quest'avviso CENTONZE F., *Controlli societari e responsabilità penale*, Milano, 2009, 73

[270] Il codice federale denominato *Uniform Partnership Act* (UPA), definisce la società (*partnership*) come *«the association of two or more persons to carry on as co-owners of a business for profit, whether or not the persons intended to form a partnership»*.

[271] DE FILIPPI P., WRIGHT A., *Blockchain and the Law*, Cambridge, 2018, 182 ss.; METJAHIC L., *Deconstructing the Dao: the Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations*, in *Cardozo Law Review*, 2018, vol. 39, 1550 secondo cui le organizzazioni autonome decentralizzate soddisfano appieno i requisiti di una società (o quanto meno di una *joint venture*).

[272] Si è sostenuto che la formazione del consenso in *blockchain* costituisca una sorta di trasposizione in codice delle regole di *governance* societaria. In tal senso il registro distribuito *«allows for the organization to code its entire set of business rules and record them permanently in the blockchain»* (METJAHIC, *Deconstructing the Dao*, cit., 1538).

[273] Basti pensare al celebre caso "The DAO" in cui l'organizzazione decentralizzata era finalizzata all'esercizio di un fondo d'investimento distribuito. Possiamo altresì immaginare una infrastruttura decentralizzata – finanziata mediante ICO – in cui ciascun nodo mette a disposizione una determinata potenza di calcolo per offrire un servizio della società dell'informazione (ad. es. la condivisione di documenti o la registrazione di file sulla *blockchain*) a fronte del pagamento di un corrispettivo.

[274] L'elemento comune a qualsiasi tipo di società è il c.d. *contratto sociale*. La giurisprudenza è concorde nel ritenere che alla base della società di fatto vi siano tre elementi: il fondo comune, l'alea nei guadagni e nelle perdite e, infine, il sentimento di affezione alla società (*affectio societatis*). Alcune sentenze recenti hanno affermato che poter considerare esistente una società di fatto occorre altresì la dimostrazione di un comportamento, da parte dei soci, tale da ingenerare nei terzi il convincimento giustificato ed incolpevole che i soggetti agissero come soci (Cass. Civ., Sez. Un., 6 febbraio 2015 n. 2243). La letteratura sul tema è davvero vasta. Per gli opportuni riferimenti bibliografici si rinvia alle monografie di VITRÒ V., *Le società di fatto: profili sostanziali ed effetti del fallimento,* Milano, 2009, 132 e di SPATAZZA G., *La società di fatto*, Milano, 1980.

Dal punto di vista penalistico è dato chiedersi quali siano le conseguenze in punto di responsabilità nel caso in cui venga commesso un reato nella gestione "societaria"[275]. Ipotizziamo che, dopo il lancio di una offerta pubblica di acquisto di valori virtuali (ICO), alcuni soggetti decidano di finanziare il progetto e ricevano in cambio *token* con diritto di voto. Essendo il capitale estremamente frammentato, su iniziativa di un certo numero di partecipanti viene messa ai voti la scelta di rimborsare coattivamente i detentori di *token* inferiori a un certo numero. Il fatto potrebbe integrare gli estremi del delitto di frode informatica (art. 640-*ter* c.p.) o di indebita restituzione dei conferimenti (art. 2626 c.c.)[276].

Ragionando secondo gli schemi tradizionali, dovremmo anzitutto individuare il vertice societario a cui imputare in via diretta la responsabilità, e poi valutare, eventualmente, l'ammissibilità di un concorso omissivo degli altri partecipanti ai sensi dell'art. 40, comma 2, c.p. per non aver impedito il reato. Nelle organizzazioni autonome decentralizzate un simile *modus procedendi* non è sempre praticabile, poiché potrebbe anche non esservi un organo gestorio distinto rispetto agli associati. Le DAO possono essere considerate come un fascio di contratti: un accordo complesso tra più utenti remoti istituzionalizzato per mezzo di *smart contract* e disciplinato dalle regole trascritte nel codice di programmazione[277]. Non esiste dunque un vertice né un organo decisionale: la *governance* è diretta emanazione del potere della maggioranza dei "consorziati" che, congiuntamente, la amministrano.

Se dunque è vero – come qui si sostiene – che tali organizzazioni devono essere qualificate come vere e proprie *società di fatto*[278], l'individuazione dei soggetti attivi del reato di impresa non potrà mai seguire l'approccio "presuntivo"[279] utilizzato dalla giurisprudenza per gli amministratori di diritto; si dovrà piuttosto accertare a quali soggetti sia *personalmente* imputabile una determinata decisione.

Ciò posto, resta da chiedersi se coloro che non abbiano preso parte alla decisione possano essere ritenuti penalmente responsabili a titolo di concorso (omissivo). Si potrebbe infatti ritenere che tutti i partecipanti, singolarmente considerati, siano titolari dell'obbligo prevenire gli illeciti nella gestione dell'organizzazione autonoma. A tale

[275] Di recente, sul tema della responsabilità dell'amministratore di fatto per i reati tributari v. CONSULICH F., *Poteri di fatto ed obblighi di diritto nella distribuzione delle responsabilità penali societarie*, in *Le società*, 2012, 5, 555 ss.

[276] È tuttavia bene precisare che la possibilità di ritenere integrato il reato societario sembra scontrarsi con il divieto di applicazione analogica *in malam partem*. Pur volendo aderire alla tesi della organizzazione autonoma decentralizzata come società di fatto, l'impiego nell'art. 2626 c.c. della locuzione "conferimenti" pare rinviare implicitamente alla relativa disciplina civilistica prevista per le società di capitali (artt. 2342, 2464 c.c.) la cui applicazione presuppone l'osservanza di determinate formalità (ad es. per la costituzione della società). È dunque piuttosto dubbio che il finanziamento dei partecipanti a una DAO sia qualificabile come "conferimento" in senso tecnico giuridico.

[277] Il potere di ciascun partecipante dipende, solitamente, dalla quota di partecipazione detenuta. L'influenza del singolo "socio" dipenderà dalla quota di capitale posseduta sottoforma di *token* oppure dalla potenza computazionale messa a disposizione della rete.

[278] Cfr. METJAHIC, *Deconstructing the Dao,* cit., 1538; DE FILIPPI, WRIGHT, *Blockchain and the Law*, cit., 124.

[279] Così lo definisce CONSULICH, *Poteri di fatto ed obblighi di diritto nella distribuzione delle responsabilità penali societarie,* cit., 556.

tesi viene facile obiettare che il consorziato non dispone *uti singulus* di alcun potere impeditivo, né di particolari strumenti per far valere il proprio dissenso[280]. L'assenza di una disciplina normativa[281] e l'inapplicabilità delle disposizioni del codice civile sulle società di capitali[282], portano ad escludere che i singoli "associati" siano titolari di obblighi giuridici di garanzia. Essi figurano piuttosto come vittime dell'illegalità nella gestione societaria e delle scelte effettuate dai "soci tiranni", dinanzi alle quali non hanno alcuno strumento – né tecnico, né giuridico – per poter reagire.

Nel caso esemplificato coloro che hanno deliberato il rimborso coattivo potranno essere ritenuti responsabili, di frode informatica e di indebita restituzione dei conferimenti, mentre i soci rimasti in minoranza oltre ad andare esenti da responsabilità penale potranno eventualmente agire per il risarcimento dell'eventuale danno.

Sarebbe infine interessante riflettere sui profili di *corporate social responsibility*. Si riscontrano obiettive difficoltà nel qualificare le organizzazioni autonome decentralizzate come enti destinatari della disciplina sulla responsabilità amministrativa da reato *ex* D. Lgs. 231/2001; sebbene l'ampiezza della formula normativa consenta di ricomprendere le più svariate forme giuridiche di esercizio collettivo dell'impresa, riteniamo che un atto di costituzione formale sia pur sempre necessario[283]. Si addiverrebbe altrimenti alla conseguenza, per certi versi paradossale, di irrogare una sanzione a un ente che, secondo il diritto civile, non è mai venuto ad esistenza e che, probabilmente, non verrà mai ad esistenza come ente regolarmente costituito.

---

[280] In assenza di regole giuridiche le procedure decisionali saranno disciplinate dal codice di programmazione: non sono dunque configurabili controlli "societari" interni, sulla falsariga di quanto avviene per le organizzazioni comuni.

[281] Sebbene il legislatore abbia di recente disciplinato gli *smart contract,* nessuna vigente disposizione di legge si occupa di definire le organizzazioni autonome decentralizzate.

[282] Secondo VITRÒ, *Le società di fatto: profili sostanziali ed effetti del fallimento,* cit., 15 ss. l'esistenza di una società di fatto viene in rilievo per lo più nei momenti patologici della vita dell'impresa, come ad esempio nel corso del fallimento. Il riconoscimento di un rapporto implicito di società è finalizzato all'applicazione delle procedure di liquidazione giudiziale o all'accertamento della responsabilità illimitata dei singoli partecipanti, con l'obiettivo di tutelare il legittimo affidamento dei terzi. Non sarà al contrario possibile applicare *sic et simpliciter* le norme che disciplinano i singoli tipi di società, che presupporrebbero la formale esistenza del vincolo societario. A differenza di quanto avviene per gli amministratori "di diritto" delle società rituali, il ruolo rivestito "di fatto" dai consorziati che amministrano una DAO non è riconducibile ad alcuna disciplina positiva; la posizione di garanzia dei gestori non potrà essere fondata sugli obblighi inerenti alla carica sociale (ad. es. l'art. 2392 c.c.), né sull'assunto di una investitura meramente fattuale che contravverrebbe al fondamentale principio di legalità (cfr. MANTOVANI, *L'obbligo di garanzia ricostruito alla luce dei principi*, cit., 349).

[283] La tesi prevalente in dottrina è quella opposta, secondo cui anche le società di fatto sarebbero destinatarie della disciplina sulla responsabilità degli enti. Si veda SCOLETTA M., *La responsabilità da reato delle società: principi generali e criteri imputativi nel d.lgs. n.231/2001, in* CANZIO G., CERQUA L.D., LUPÀRIA L. (a cura di), *Diritto penale delle società, I, I profili sostanziali*, Padova, 2014, 877; ROSSI A., *I soggetti persone giuridiche: su quali enti vigila il D.Lgs. 231*?, in *Le Società*, 2011, 1, 24; DI GIOVINE O., *Lineamenti sostanziali del nuovo illecito punitivo,* in LATTANZI G., (a cura di), *Reati e responsabilità degli enti*, Milano, 2010, 40.

6.5. *Blockchain* pubbliche. Alla ricerca di un garante?

La *blockchain* pubblica si caratterizza per l'assenza di titolari del sistema o di autorità di monopolio; il connotato essenziale è la decentralizzazione dell'infrastruttura in una pluralità di nodi gestiti da soggetti diversi. Il più delle volte il sistema è supervisionato da un team di sviluppo che, dopo aver programmato e diffuso il *software* di base, sovrintende al corretto funzionamento del protocollo e agli eventuali aggiornamenti. Come si è visto, l'accesso alla rete può essere *permissionless* o *permissioned* [284]: in questo secondo caso esiste una autorità che verifica il rispetto delle condizioni di accesso e definisce il ruolo di ciascun partecipante. Avendo sufficientemente approfondito le questioni relative ai sistemi sottoposti ad autorizzazione, l'attenzione andrà ora rivolta alle infrastrutture pubbliche totalmente decentralizzate. In esse nessun utente ha privilegi sugli altri, o può controllare le informazioni che vengono memorizzate nei registri, modificarle o eliminarle; nessuno può inoltre alterare il protocollo che determina il funzionamento del sistema[285]. I concetti di *permissionless* e *publicness* sono strettamente legati tra loro[286]: la rete potrà estendersi o contrarsi in base al numero di utenti che, a seconda dell'aspettativa di guadagno e dell'andamento dei prezzi dei *token,* ritengano conveniente prendervi parte.

L'aspetto più significativo – per molti versi rivoluzionario – di questa tipologia di reti distribuite sta nella creazione di *asset* dotati di scarsità artificiale a cui è attribuito, per *communis opinio,* un valore di mercato in virtù della fiducia degli utenti nell'infrastruttura in sé[287].

L'assenza di un soggetto qualificabile come *provider* fa venire meno l'intelaiatura giuridica della responsabilità connessa alla erogazione del servizio; non vi è infatti alcun partecipante al quale imputare i doveri di collaborazione con l'autorità previsti dagli artt. 14 ss. D. Lgs. 70/2003. Tali obblighi potrebbero trovare applicazione soltanto in una gestione parzialmente centralizzata del sistema informatico, che per definizione manca nelle infrastrutture pubbliche *permissionless*[288]. Ebbene, anche la questione relativa alla configurabilità di obblighi di garanzia subisce un notevole ridimensionamento: non si tratta qui di bilanciare l'esigenza della libertà e della

[284] Cfr. *Supra*, § 6.3. e Cap I, § 2.2. Nel primo caso chiunque può prendere parte alla rete, semplicemente scaricando il *software* base e mettendo a disposizione un *hardware* connesso al sistema; nel secondo caso sono previste delle particolari condizioni per il rilascio dell'autorizzazione a partecipare.

[285] È proprio alle *blockchain* pubbliche *permissionless* che il legislatore sembra aver fatto riferimento nel fornire la prima definizione di "tecnologie basate su registri distribuiti" (art. 8-*ter*, comma 1, D.L. 158/2018). Si è detto tuttavia come il requisito della non modificabilità nel registro vada inteso in modo *relativo* e non assoluto, poiché anche in un sistema totalmente decentralizzato il protocollo del consenso potrebbe prevedere, a determinate condizioni, la possibilità di intervenire sulla catena dei blocchi (v. *supra*, Cap. I, § 3.1.).

[286] Sul tema veda VALSECCHI V., *La classificazione delle Blockchain: pubbliche, autorizzate e private,* in https://spindox.it, 20 giugno 2018; SARZANA DI S. IPPOLITO, NICOTRA M., *Diritto della blockchain,* cit., 21 ss.

[287] Si parla a tal proposito di sistemi *trustless* e disintermediati, non governati da alcuna autorità centrale.

[288] Il tramonto della figura del *provider* solleva le problematiche di non poco conto anche sul fronte processuale (in particolare per l'acquisizione della prova informatica e per l'esecuzione delle misure cautelari reali, v. *infra,* Cap. V, § 6 ss.).

sicurezza della rete o di valutare l'esistenza di una posizione di garanzia in capo ai titolari o agli operatori del sistema, quanto piuttosto di riuscire a individuare un centro di imputazione della responsabilità. La fiducia nelle infrastrutture totalmente decentralizzate sembra giustificarsi proprio in virtù della disintermediazione negli scambi, che rappresenta un fattore di garanzia contro i possibili abusi da parte dell'autorità centrale, ma anche un fattore di rischio per la prevenzione e la repressione di eventuali condotte illecite[289]. Da un punto di vista politico criminale sarebbe sicuramente opportuno individuare un responsabile, tenuto ad attivarsi per ridurre il rischio di un impiego sistematico della nuova tecnologia a fini illeciti. La ricerca di un garante tra i partecipanti alla rete pare tuttavia destinata all'insuccesso, non essendovi alcun utente in grado di controllare il flusso di informazioni o di incidere sulla formazione del consenso o sulla verifica delle transazioni.

Per far fronte alla necessità di "recuperare" un centro di imputazione, sembra che l'unica strada percorribile fosse quella di responsabilizzare gli intermediari professionisti che offrono servizi connessi o collegati alla circolazione di valori virtuali. In questa direzione è certamente condivisibile la scelta del legislatore di ampliare il novero dei destinatari della disciplina antiriciclaggio includendovi soggetti che, pur essendo "esterni" alla rete decentralizzata, intermediano la domanda e l'offerta di valori virtuali.

6.6. La responsabilità dell'*exchange* e del *wallet provider* a titolo di concorso omissivo in riciclaggio.

I soggetti che professionalmente operano sul mercato dei valori virtuali sono tenuti all'osservanza degli obblighi previsti dal Titolo II del D. Lgs. 231/2007; devono quindi identificare la clientela, registrare e conservare i dati e i documenti relativi alle operazioni compiute e segnalare le operazioni sospette. Non è questa la sede opportuna per entrare nel merito della disciplina preventiva del riciclaggio che sarà oggetto di trattazione nel capitolo successivo. Occorre tuttavia rilevare come la previsione di detti obblighi concorra ad individuare una posizione di garanzia *ex* art. 40, comma 2, c.p. in capo al fornire di servizi di cambio (*exchange provider*) e al gestore di portafoglio elettronico (*wallet provider*)[290].

Non vi è infatti alcun dubbio sulla volontà del legislatore di responsabilizzare gli intermediari professionisti al preciso fine di prevenire lo sfruttamento della finanza virtuale a fini di riciclaggio, né sulla possibilità per costoro di attivarsi per bloccare i trasferimenti illeciti di fondi o le operazioni manifestamente illecite. A differenza dei soggetti che gestiscono l'infrastruttura digitale, i prestatori di servizi relativi all'utilizzo

[289] Non può infatti tacersi come la decentralizzazione accresca ulteriormente la spinta criminogena alla commissione di reati informatici. *Amplius,* § 1.2.

[290] I prestatori di servizi di portafoglio digitale sono stati inclusi tra i destinatari degli obblighi antiriciclaggio ad opera del D. Lgs. 125/2019 (cfr. Art. 1, comma 2, lett. ff-*bis)* e art. 3, comma 5 lett. i)-*bis,* D. Lgs 231/2007).

delle valute virtuali[291] soddisfano appieno i requisiti delineati dalla dottrina[292] per l'esistenza di obbligo di garanzia. Il dovere di attivarsi deriva infatti da una fonte giuridica formale sufficientemente specifica, a cui si accompagna un potere impeditivo strettamente connesso alla fonte di rischio da prevenire (in questo caso l'utilizzo del sistema finanziario a scopo di riciclaggio e di finanziamento del terrorismo).

Benché detti intermediari esercitino una attività che, astrattamente, potrebbe rientrare nell'ambito di applicazione della normativa sul commercio elettronico, l'art. 1 del D. Lgs. 70/2003 esclude dal campo di applicazione del decreto stesso le disposizioni in tema di prevenzione del riciclaggio, effettuando in tal modo una netta restrizione per materia[293] della clausola di limitazione dalla responsabilità. Ciò sembra confermare l'assunto che gli *exchange* e i *wallet provider* non siano affatto esonerati dall'obbligo generale di sorveglianza e che, qualora abbiano omesso di attivare gli opportuni rimedi[294], risponderanno per concorso omissivo del reato commesso dagli utenti della piattaforma, laddove l'omissione sia assistita dal necessario dolo di partecipazione.

In questo caso l'addebito per omesso impedimento del reato sembra trovare una spiegazione razionale anche alla luce della teoria dell'imputazione obiettiva dell'evento[295]; l'equivalenza tra l'azione e il *non facere* antidoveroso è sorretta da un solido nesso di rischio tra l'evento non impedito e la fonte di rischio l'ordinamento mirava a prevenire.

7. Considerazioni finali e prospettive *de lege ferenda*.

Giunti a conclusione dell'indagine, riteniamo di dover esprimere qualche considerazione finale in merito ai doveri di controllo e alla posizione di garanzia nel cyberspazio.

In un contesto privo di confini fisici e territoriali il paradigma del reato omissivo improprio si rivela profondamente inadeguato. Emerge, da un lato, la difficoltà di rinvenire categorie di soggetti (*provider*) titolari di un obbligo di garanzia; dall'altra quella di raggiungere la prova circa la sussistenza del dolo di partecipazione nel reato commesso dagli utenti del servizio.

Quanto al primo aspetto, molteplici sono i fattori che si oppongono alla individuazione di una posizione di garanzia rilevante *ex* art. 40, comma 2, c.p. In primo luogo l'impossibilità di rinvenire nell'ordinamento obblighi finalizzati a prevenire il fatto illecito altrui: nel bilanciamento di interessi tra la libertà e la sicurezza della rete

[291] Così li definisce l'art. 1, comma 2, lett. ff) del D. Lgs. 21 novembre 2007 n. 231.
[292] Per gli opportuni riferimenti bibliografici di rinvia alla dottrina citata alle note 175 e 190.
[293] In argomento, INGRASSIA, *Il ruolo dell'ISP nel* ciberspazio, cit., 40
[294] L'art. 41, comma 2, del D. Lgs. 231/2007 in materia di operazioni sospette prevede che le segnalazioni debbano essere *«effettuate senza ritardo, ove possibile prima di eseguire l'operazione, appena il soggetto tenuto alla segnalazione viene a conoscenza degli elementi di sospetto»*
[295] Per una breve disamina del fondamento della teoria dell'imputazione obiettiva dell'evento si rinvia al § 6.1.2.

il legislatore ha ritenuto di far prevalere il principio della *net neutrality*, da cui deriva l'assenza di controlli preventivi sul materiale immesso e condiviso in rete. I fornitori del servizio saranno tenuti ad attivarsi soltanto in un momento successivo alla commissione del reato, per limitarne le conseguenze dannose e agevolare l'individuazione dei responsabili. Pur volendo ammettere la sussistenza di obblighi di garanzia, l'addebito omissivo sarebbe comunque ostacolato dall'inesigibilità di un controllo "a tappeto" sulla mole enorme di dati circolanti in rete e dalla mancanza di potere impeditivo specifico. A differenza di un contesto "umano" di azione – dove l'individuo può governare le forze della natura, attivandosi per prevenire un evento antigiuridico – nell'ambiente virtuale l'equiparazione tra il *facere* e il *non facere* rischia di tradursi in una mera responsabilità per posizione.

Con riferimento al secondo aspetto, deve notarsi che le fattispecie delittuose in astratto configurabili come "reato-transazione"[296] sono punite tutte a titolo di dolo. La clausola di equivalenza tra l'azione e l'omissione potrà dunque operare a condizione che il *non facere* antigiuridico sia assistito dal dolo di partecipazione nel fatto di reato commesso da terzi. Ciò evidenzia una sfasatura tra l'esigenza che è alla base della individuazione di soggetti in posizione di garanzia – quella di rendere la rete un luogo più sicuro – e l'area del penalmente rilevante. Il fornitore di servizi andrebbe infatti esente da pena in tutti quei casi in cui, pur essendo rimproverabile per negligenza, non vi sia la prova nel dolo di concorso. Ecco che il paradigma del reato omissivo improprio potrebbe condurre verso un eccessivo restringimento dell'area del penalmente rilevante oppure alimentare l'opposta tendenza – peraltro già nota alla giurisprudenza in materia penale-societaria[297] – alla macroestensione dello spettro del dolo eventuale.

Sarebbe pertanto auspicabile che il legislatore, presa coscienza degli evidenti limiti all'applicazione delle disposizioni di parte generale – specie con riferimento agli obblighi di garanzia – percorresse strade alternative al fine di responsabilizzare i fornitori di servizi digitali.

Una prima alternativa è quella di introdurre specifiche ipotesi di reato, costruite come fattispecie omissive proprie, legate all'inosservanza del provvedimento di rimozione/inibitoria impartito dall'autorità giudiziaria, da quella amministrativa o di pubblica sicurezza[298], rivelandosi all'uopo troppo blanda la tutela prevista in via generale dall'art. 650 c.p.

---

[296] Con questa locuzione indichiamo quelle transazioni che, tenuto conto dell'intenzione delle parti, dei presupposti della condotta o dei fini perseguiti, costituiscono di per sé reato (es. riciclaggio, finanziamento del terrorismo, sottrazione fraudolenta al pagamento delle imposte).

[297] In argomento, di recente, INGRASSIA A., *La Suprema Corte e il superamento di una responsabilità di posizione per amministratori e sindaci: una decisione apripista?* in *Diritto penale contemporaneo*, 14 febbraio 2013; CRESPI A., *Studi di diritto penale societario*, Milano, 2010, 40 ss.; CENTONZE, *Controlli societari e responsabilità penale*, cit., 222 ss.

[298] In tal modo l'azione del legislatore si porrebbe in linea con le scelte di criminalizzazione compiute in settori contigui dell'ordinamento (cfr. art. 170 D. Lgs 196/2003, di recente riformulazione, che punisce l'inosservanza dei provvedimenti del Garante *privacy* in particolari ambiti) in cui la delicatezza degli interessi in gioco legittima il ricorso alla sanzione penale. La lesione delle prerogative dell'autorità e,

In alternativa, il legislatore potrebbe sperimentare nuove fattispecie di reato che sanzionano l'agevolazione colposa dell'altrui condotta illecita. È questo un terreno ancora inesplorato che potrebbe sondarsi proprio con riferimento alla responsabilità dell'*internet service provider*. L'inerzia del fornitore di servizi – il quale, ad es., non ha provveduto all'esame delle segnalazioni effettuate dagli utenti, non ha adottato le misure di sicurezza adeguate al rischio o non si è preoccupato di 'monitorare' utenti già individuati come sospetti – potrebbe così integrare gli estremi della colpa penalistica e assumere rilievo come fattore di agevolazione dell'altrui condotta illecita.

7.1. Una proposta per l'introduzione di una fattispecie di reato propria del *provider.*

Il legislatore potrebbe trarre ispirazione da alcuni paradigmi punitivi già esistenti per introdurre nel corpo nel D. Lgs. 70/2003 un nuovo art. 17-*bis* del seguente tenore:

(Omessa attivazione. Agevolazione colposa)

«1. Il prestatore di servizi il quale, avendo ricevuto denunce, segnalazioni o comunicazioni, comunque denominate, relative alla presenza o alla condivisione di materiale manifestamente illecito sui sistemi informatici o telematici posseduti, gestiti o controllati, omette di informare la competente autorità o di disabilitare l'accesso a dati o ai sistemi, o di porre fine alle violazioni commesse, è punito…».

«2. Il prestatore di servizi il quale, dopo che fu commesso un delitto e fuori dei casi di concorso nel medesimo, avendo ricevuto comunicazioni, richieste, o prescrizioni da parte dell'autorità giudiziaria o di quella di pubblica sicurezza, omette di fornire le informazioni dovute o di disabilitare l'accesso ai dati o ai sistemi informatici o telematici, agevolando colposamente la commissione di ulteriori reati da parte di uno o più destinatari del servizio è punito, se un reato è commesso,…».

La norma contiene due distinte fattispecie di reato, facenti leva sul comune presupposto della delazione di una notizia sulla presenza di attività illecite

La fattispecie del *primo comma* è costruita come un reato di pura omissione, che sanziona la violazione dell'obbligo di informare l'autorità (prescritto dall'art. 17, comma 2, D. Lgs. 70/2003) o di inibire l'accesso ai dati o ai sistemi, o di porre fine alle violazioni commesse. Soggetto attivo del reato è il prestatore di servizi, per tale intendendosi non proprietario del sistema informatico o telematico, quanto piuttosto il soggetto che attivamente lo possiede, lo gestisce o lo controlla.

L'incriminazione delle summenzionate condotte mira a responsabilizzare i *provider* in tutti quei casi in cui essi si astengano dall'intervenire pur in presenza di fatti o circostanze che rendono evidente che un reato sia stato commesso. Un tale

indirettamente, degli interessi degli individui porta a ritenere insufficiente il ricorso alla sanzione amministrativa.

obbligo di attivazione scatta soltanto nel caso in cui abbia ricevuto segnalazioni relative alla presenza o alla condivisione di materiale manifestamente illecito[299].

Le prescrizioni imposte dalla norma sono alternative, sicché il fornitore si servizi potrà assolvere all'obbligo informando l'autorità, o disabilitando l'accesso oppure ponendo fine alle violazioni commesse. Il bene giuridico tutelato non è l'amministrazione della giustizia[300], bensì quello che la norma incriminatrice violata dall'attività manifestamente illecita mirava a proteggere: lo scopo dell'incriminazione è di evitare che un reato commesso *online* possa propagare i propri effetti dannosi a causa dell'inerzia del *provider*.

Così, ad esempio, se viene condiviso materiale coperto da *copyright*, pedopornografico o diffamatorio, il dovere di attivarsi gravante sul provider costituirà una sorta di "tutela di secondo grado", rispettivamente, del diritto d'autore, della dignità del minore, dell'onore.

Il *secondo comma* introduce invece una fattispecie di agevolazione colposa, avente quale presupposto una comunicazione qualificata da parte dell'autorità circa l'avvenuta commissione di un reato sulla piattaforma gestita dal *provider*. L'inciso iniziale ("dopo che fu commesso un delitto e fuori dei casi di concorso nel medesimo") vuole evitare che la norma trovi applicazione nel caso in cui il *provider* sia responsabile per concorso commissivo doloso nel reato commesso dall'utente. Il presupposto della previa commissione di un delitto esclude la configurabilità del reato laddove l'illecito precedentemente commesso sia punito a titolo contravvenzionale[301].

La *ratio* della disposizione è quella di far sì che il fornitore del servizio, a fronte della segnalazione dell'autorità circa la commissione di un illecito, impedisca la commissione di ulteriori reati. Si tratta di una particolare ipotesi omissiva che, superando il modello dell'omesso controllo puro, attribuisce rilevanza penale alla violazione dell'obbligo sancito dall'art. 16, comma 2, lett. b) del Codice del commercio elettronico[302].

Il presupposto della condotta ("avendo ricevuto comunicazioni, richieste, o prescrizioni da parte dell'autorità giudiziaria o di quella di pubblica sicurezza") è descritto facendo riferimento alle forme di comunicazione dotate di particolare serietà, tali da "attualizzare" il dovere di controllo da generale e astratto a specifico e concreto.

La componente omissiva della condotta ("omette di fornire le informazioni dovute o di disabilitare l'accesso ai dati o ai sistemi informatici o telematici,") è formulata

[299] Ciò appare sufficiente a contenere l'area del penalmente rilevante entro limiti razionali, superando le criticità relative all'inesigibilità della condotta e alla violazione dei principi della *net neutrality*.

[300] Non si tratta infatti di una classica ipotesi di omessa denuncia.

[301] Appare infatti ragionevole far scattare un obbligo di collaborazione penalmente sanzionato, al di là dell'ipotesi contravvenzionale prevista dall'art. 650 c.p., soltanto per quei fatti che il legislatore considera di più grave allarme sociale, configurati come delitti.

[302] La norma prevede che nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non sia responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che «*non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso».*

facendo riferimento alla violazione degli obblighi di attivazione e di collaborazione con l'autorità sanciti dalla normativa sul commercio elettronico, superando così ogni possibile frizione con il principio di legalità.

La componente commissiva, descritta con l'espressione "agevolando il compimento di reati" evidenzia non solo l'esigenza di un legame causale tra l'omissione del *provider* e la commissione del reato da parte del destinatario del servizio, ma anche di un nesso con il reato precedentemente commesso per il quale è intervenuta la segnalazione da parte dell'autorità.

Sarà pertanto necessario accertare, secondo le cadenze delineate dalla giurisprudenza in punto di causalità omissiva e di causalità nella colpa, che l'inerzia del *provider* abbia facilitato l'altrui azione delittuosa. Il reato è punito, a titolo di colpa "se un reato è commesso", inciso che richiama alla mente la tecnica descrittiva utilizzata dall'art. 57 c.p.

Anche in questo caso la norma appresta una tutela "di secondo grado" del bene giuridico leso dalla commissione del delitto presupposto, al fine di evitare ulteriori e successivi reati riconducibili a quello in precedenza commesso.

Quanto al rapporto tra le due fattispecie, si ritiene possa esservi concorso di reati, nel caso in cui il *provider*, in presenza di un contenuto manifestamente illecito, abbia dapprima omesso di informare l'autorità (o di inibire l'accesso) e successivamente, avendo ricevuto la segnalazione qualificata, si sia astenuto dal compiere le attività doverose agevolando la commissione di ulteriori reati.

È bene precisare che si tratta di una tesi avanguardista che, per il momento, non ha trovato seguito in dottrina. L'introduzione di simili ipotesi di reato riuscirebbe a colmare la lacuna che ha talvolta indotto la giurisprudenza a forzare le categorie tradizionali pur di farvi rientrare la responsabilità del *provider* a titolo di concorso omissivo[303]. L'opera di supplenza giudiziaria è un chiaro indice dell'inadeguatezza

[303] Ci si riferisce in particolare alla recente sentenza di legittimità (Cass. Pen., Sez. V, 27 dicembre 2016 n. 54946 in *Giurisprudenza Penale Web*, 2017, 1, con nota di MIGLIO M., *I gestori di un sito internet rispondono penalmente per i commenti offensivi pubblicati dagli utenti*) che ha ritenuto ammissibile in concorso omissivo in diffamazione del gestore di un sito web per omessa rimozione dei contenuti offensivi, *rectius* per aver *«mantenuto consapevolmente l'articolo sul sito, consentendo che lo stesso esercitasse l'efficacia diffamatoria».* La sentenza ha suscito diverse reazioni in dottrina v. BUFFA F., *Responsabilità del gestore di sito Internet*, in *Questionegiustizia.it*, 9 gennaio 2017; INGRASSIA A., *Responsabilità penale degli* internet service provider*: attualità e prospettive*, in *Dir. pen. Proc.*, 2017, 12, 1621 ss.; PANATTONI, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di* notice and take down, cit., 253. Alcuni ritengono che non si tratterebbe di una responsabilità concorsuale, ma monosoggettiva per omessa rimozione tenuto conto che il provider interviene quando il reato è già consumato (e non vi è più possibilità di impedirlo). Contrariamente si afferma che la diffamazione telematica dà luogo a un illecito permanente, sicché la legge richiederebbe al *provider* un intervento diretto per impedire la continuativa consumazione del reato: nel momento in cui il provider è edotto che attraverso il suo *server* si sta realizzando un comportamento lesivo permanente, egli concorre nel fatto altrui se non interrompe la visibilità del messaggio illecito, rimuovendo il dato informatico in questione o bloccando l'accesso allo stesso. A nostro modo di vedere, il reato di diffamazione è un reato istantaneo che si consuma con la pubblicazione in rete del contenuto offensivo, per cui un obbligo di rimozione di quello stesso contenuto sarebbe possibile solo post-consumazione. Non deve infatti essere confuso il *reato permanente* – legato al perpetuarsi della condotta antigiuridica del reo – con la *permanenza degli effetti* del reato: nel primo caso sarebbe ammissibile un concorso successivo alla

dell'attuale quadro normativo e della necessità di un intervento del legislatore in prospettiva di una maggiore responsabilizzazione dei fornitori di servizi digitali. La previsione di sanzioni penali per la violazione dell'*obbligo di attivazione* è una scelta di politica criminale che, in un ordinamento chiaramente orientato verso modelli di cooperazione pubblico-privato, si rivela decisamente opportuna.

L'introduzione di una autonoma fattispecie di agevolazione colposa permette di superare le criticità relative all'inesigibilità della condotta del *provider* e alla prova dell'elemento psicologico del dolo di concorso. Inoltre, il *focus* sulla violazione del dovere di collaborazione come fattore concausale del reato altrui è un utile espediente per evitare di sanzionare penalmente di condotte di mera inosservanza[304].

Venendo infine all'oggetto della presente trattazione, si ritiene che l'introduzione di ipotesi di reato come quelle sopra descritte sortirebbe un *effetto responsabilizzante* per coloro che gestiscono sistemi *blockchain* privati o ibridi, che attualmente godono di una zona franca da responsabilità penale[305]. Desta forti perplessità la scelta di non sanzionare la violazione degli obblighi di collaborazione imposti dal D. Lgs. 70/2003, che appare in controtendenza rispetto alla necessità di contenere il rischio di un impiego sistematico della nuova tecnologia per propositi criminosi. I gestori delle reti private si trovano in posizione tale da poter attivamente cooperare per segnalare le operazioni sospette, rimuovere i contenuti illeciti e disabilitare l'accesso a dati o informazioni (siano esse rappresentativi di file multimediali o di valori virtuali): la punizione di condotte omissive che abbiano agevolato l'altrui azione criminosa troverebbe così una razionale giustificazione nella sintesi tra tecnicamente possibile e giuridicamente doveroso.

Rimarrebbe però irrisolto il problema della responsabilità nella gestione delle infrastrutture totalmente decentralizzate, nelle quali il dovere di collaborazione con l'Autorità ricade in parte su soggetti esterni alla rete (ad es. sugli intermediari del mercato degli *asset* digitali). L'assenza di controllori è un fattore fisiologico nello spazio virtuale, emerso sempre più chiaramente a partire dalla fine degli anni 90 con la diffusione delle reti *peer-to-peer* e la crescente tendenza alla democratizzazione della rete. Anziché insistere nella spasmodica ricerca di un responsabile, il legislatore dovrebbe riflettere sulle cause del fenomeno, ricercando una valida soluzione di carattere *preventivo*; il modello di cooperazione pubblico-privato rappresenta, in questa direzione, un valido incentivo per la condivisione di buone prassi tra gli operatori del settore.

realizzazione del fatto; nel secondo caso non vi è invece alcuno spazio per una responsabilità concorsuale per omesso impedimento del reato già consumato.

[304] Si attribuirebbe in tal modo rilevanza penale alle sole omissioni realmente offensive, in quanto abbiano agevolato il compimento di reati.

[305] Il titolare delle infrastrutture private o ibride è qualificabile come un *content provider* e, in quanto tale, difficilmente potrà essere ritenuto titolare di una posizione di garanzia.

8. Azione, omissione ed evento in *blockchain*. Un quadro di sintesi.

La trattazione svolta in questo capitolo ha toccato diverse problematiche di parte generale che la tecnologia a registro distribuito potrebbe lentamente portare alla deriva; si tratta di questioni che non sono certamente nuove per il diritto penale dell'informatica. Già da tempo la dottrina[306] ha evidenziato come l'azione, l'omissione e l'evento nel cyberspazio assumano dei connotati del tutto peculiari, che potrebbero far apparire obsolete le categorie tradizionali, concepite per l'agire umano nella realtà materiale. Le sfide lanciate dalla *blockchain* non rappresentano altro che la riedizione contemporanea, con un più alto grado di sofisticazione, di problematiche che da sempre caratterizzano la commissione di reati mediante strumenti informatici o telematici. Si tratta dunque di temi "sempreverdi", irrorati da nuova linfa per effetto l'ampio utilizzo dei nuovi ritrovati tecnologici.

Con riferimento al concetto penalistico di *azione*, si è detto come le categorie dell'*agere* umano abbiano assunto contorni ancor più sfumati non solo per la presenza di una moltitudine di registri interconnessi, ma anche a causa della previsione di precise regole sul consenso e sulla convalida delle transazioni. Nella catena dei blocchi può ben darsi che l'operazione non giunga a compimento per fatti simultanei (omessa convalida) o sopravvenuti (caducazione della catena dei blocchi). Nel qual caso sarà complesso stabilire quali siano le conseguenze sul piano della responsabilità penale dei soggetti coinvolti, che, per fattori indipendenti dalla loro volontà, non siano riusciti a portare a termine l'*iter criminis.*

L'evanescenza del concetto penalistico di azione si deve inoltre alla progressiva emersione degli agenti *software* autonomi. Il compimento di attività giuridicamente rilevanti per il tramite di *smart contract* solleva questioni di non poco conto sul piano della responsabilità penale, allorché il contratto sia utilizzato per scopi illeciti ovvero sia esso stesso il mezzo esecutivo del reato. Si rivela una tendenziale rottura del rapporto di *autoria* tra transazione e operatore fisico, destinata ad incidere sull'accertamento della responsabilità della persona fisica. I contratti *smart* eseguono la prestazione al verificarsi di determinate condizioni, che spesso non dipendono direttamente ed esclusivamente dalla volontà del predisponente, né da quella del beneficiario. Quanto alla posizione del soggetto che ha programmato il *software*, potrebbe darsi che questi non sia in grado di predeterminare *ex ante* se lo *smart contract* verrà attivato e, soprattutto, se sarà strumentalizzato per finalità illecite; il tema è strettamente connesso a quello dei *dual-use software*, vale a dire quei programmi informatici che, pur possedendo un elevato potenziale offensivo, possono essere impiegati non solo per finalità illecite, ma anche scopi legittimi.

L'accertamento del dolo in capo agli utenti di un *smart contract* presenta inoltre una ulteriore criticità. Una volta concluso il contratto, le parti si spogliano interamente della discrezionalità nella relativa esecuzione: l'automazione dell'*enforcement* del

[306] PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, cit., 842.

contratto comporta così delle deroghe all'ordinario regime di responsabilità penale, che dovrà essere parametrato all'impossibilità per la parte obbligata di recuperare il controllo sulla fase esecutiva.

Il concetto di *evento* viene spesso in rilievo nella dimensione virtuale come risultato logico-informatico della elaborazione di dati o di alterazione del funzionamento di uno o più sistemi informatici. Laddove la fattispecie di reato sia costruita attorno alla verificazione di un *exitus* di carattere tecnico-informatico, per determinare il foro competente si dovrebbe aver riguardo al luogo di produzione del danno. In questo caso la delocalizzazione delle risorse sulla *blockchain* è un fattore di evidente complicazione; la natura ubiquitaria della tecnologia a registro distribuito ha fornito una ulteriore conferma dell'impossibilità di ricorrere ai criteri tradizionali dettati dal codice penale per determinare in modo univoco la giurisdizione e la competenza.

Per quel che riguarda, infine, la possibilità di configurare degli obblighi di garanzia in capo ai soggetti che, a vario titolo, gestiscono o utilizzano l'infrastruttura decentralizzata, l'indagine si è sviluppata attorno al tema della responsabilità del *provider;* la conclusione è stata nel senso dell'inadeguatezza del paradigma ascrittivo del reato commissivo mediante omissione *ex* art. 40, comma 2, c.p. L'auspicio per il futuro è che il legislatore colga la sfida lanciata dalla nuova tecnologia per mettere mano al sistema e sperimentare nuovi modelli di responsabilità.

CAPITOLO III

VALUTE VIRTUALI E NUOVE FRONTIERE DELLA CRIMINALITÀ ECONOMICA.

SOMMARIO: 1. Le funzioni economiche dei valori virtuali. Una premessa di ordine metodologico. – 1.1. Valute virtuali e moneta avente corso legale. – 1.2. Bitcoin e funzioni tipiche della moneta. – 1.3. Speculazione finanziaria e volatilità del prezzo della criptomoneta. – 1.4. Mercato valutario virtuale e variabili macroeconomiche. Spunti di riflessione sulla condizione di equilibrio nel modello keynesiano della moneta. – 1.5. Conclusioni in punto di natura giuridica delle valute virtuali dalla prospettiva del diritto penale. – 1.5.1. Ricchezza virtuale e "profitto" in senso penalistico. – 1.5.2. L'*asset* virtuale come documento informatico. Brevi cenni sulla punibilità del falso *ex* art. 491-*bis* c.p. – 2. Alcuni aspetti definitori delle valute virtuali. – 2.1. I primi tentativi di 'messa a fuoco' del fenomeno. La posizione delle autorità bancarie e finanziarie tra scetticismi e dubbi interpretativi. – 2.2. La definizione di valuta virtuale nell'attuale quadro normativo. – 2.3. Conclusioni sulla definizione di valuta virtuale. – 3. Il riciclaggio dei proventi delittuosi nell'era della *distributed economy*. – 3.1. Riciclaggio (art. 648-*bis* c.p.) e *cyberlaundering*. – 3.1.1. In particolare: l'utilizzo delle valute virtuali per fini di riciclaggio. – 3.2. Valori virtuali e *cyber-self-laundering* – 3.3. Gli operatori professionali sul mercato valutario virtuale. – 3.3.1. Piattaforme di *trading* e prestatori di servizi di cambio. – 3.3.2. Servizi di *mixing*. – 3.4. Valute virtuali e prevenzione del riciclaggio: dal D. Lgs. 90/2017 alla direttiva 2018/843/UE. – 3.5. La responsabilità degli intermediari professionisti per concorso in riciclaggio. – 3.5.1. La responsabilità dell'*exchange provider* per concorso omissivo in riciclaggio. Rinvio. – 3.5.2. Intestazione fittizia di *asset* virtuali e trasferimento fraudolento di valori. Incertezze applicative e aporie sistematiche. – 3.6. Cenni sulla tutela penale secondaria e sull'apparato sanzionatorio amministrativo per le violazioni della disciplina preventiva del riciclaggio. L'introduzione di una ipotesi speciale di confisca. – 3.7. Valute virtuali e riciclaggio. Uno sguardo all'ordinamento svizzero. – 3.8. Considerazioni finali. – 4. Il contrasto al finanziamento del terrorismo tra prevenzione e repressione. Cenni all'evoluzione normativa. – 4.1. *Virtual currencies and terrorist financing*. Note a margine del recente studio condotto dal Parlamento Europeo. – 4.2. Valute virtuali e finanziamento di condotte con finalità di terrorismo (art. 270-*quinquies*.1 c.p.). – 4.3. La criptomoneta come mezzo di scambio per l'acquisto di beni intrinsecamente illeciti sul *dark web*. Mercati neri virtuali e dintorni. – 5. La valuta virtuale come oggetto (im)materiale del reato. Furto e indebita sottrazione di chiavi crittografiche. – 5.1. Tra proprietà e possesso. *Dominium* crittografico, signoria di fatto e atti dispositivi in *blockchain*. – 5.2. L'applicabilità della fattispecie comune di furto tra equilibrismi interpretativi ed esigenze di tassatività. – 5.2.1. Portafogli elettronici e indebita sottrazione di valuta virtuale. Chiarimenti in ordine ai reati configurabili tra accesso abusivo a sistema informatico e frode informatica aggravata. – 5.2.2. L'appropriazione indebita di chiavi crittografiche da parte del fornitore di servizi di portafoglio digitale. – 5.3. Una ipotesi residuale di applicazione dell'art. 624 c.p.? Il *mining* abusivo tra furto, frode informatica e truffa comune. – 5.4. Frode informatica e sottrazione indebita di valuta virtuale: gli obblighi di criminalizzazione contenuti nella Direttiva 2019/713/UE – 6. Valute virtuali e reati tributari nella nuova dimensione dell'economia. – 6.1. L'assoggettamento al regime IVA delle operazioni di cambio di valuta virtuale. I principi affermati dalla Corte di Giustizia UE. – 6.1.1. Oltre la sentenza della Corte di Giustizia. Cenni sul regime IVA applicabile alle cessioni di beni, alla prestazione di servizi e all'attività di *mining*. – 6.2. La posizione dell'Agenzia delle Entrate sul regime fiscale applicabile alle cessioni e ai redditi derivanti da operazioni in valuta virtuale. – 6.3. Profili di rilevanza penale dell'evasione delle imposte sui redditi e sul valore aggiunto relative ad operazioni in valuta virtuale. – 6.4. La sottrazione fraudolenta al pagamento delle

imposte. – 6.5. Le novità in materia di monitoraggio fiscale e i connessi profili sanzionatori. – 7. Ablazione patrimoniale e confisca di valori virtuali. – 7.1. La valuta virtuale come profitto del reato. Inafferrabilità della ricchezza digitale e limiti applicativi alla confisca. – 7.2. Risparmio d'imposta e confisca diretta del denaro. *Quid iuris* nel caso della moneta virtuale? – 7.3. Osservazioni conclusive.

1. Le funzioni economiche dei valori virtuali. Una premessa di ordine metodologico.

Nel corso del precedente capitolo si è fatto più volte cenno alla dimensione economica-finanziaria della *blockchain*, sottolineando come sia l'ambito che più facilmente può essere strumentalizzato per finalità illecite.

La tecnologia a registro diffuso non ha soltanto spianato la strada a nuove manifestazioni criminose – il furto di chiavi crittografiche, per dirne una – ma ha mutato *funditus* le modalità commissive di illeciti tradizionali. Basti pensare alle nuove frontiere del riciclaggio o di finanziamento del terrorismo, alla proliferazione di *criminal market places* per lo scambio di beni intrinsecamente illeciti, all'evasione fiscale dei redditi di capitale, e a tutti quei reati *lato sensu* economici, "riscoperti" grazie alla diffusione del circolante virtuale.

La creazione di valori digitali, registrati elettronicamente e scambiati con sofisticate tecniche di crittografia, permette agli utenti della rete di effettuare transazioni in modo anonimo e al riparo da qualunque forma di intermediazione o di ingerenza statale. L'ampia diffusione nei nuovi valori ha contribuito alla crescita di un fiorente mercato di scambio, una piazza virtuale di incontro tra la domanda e l'offerta di *asset* digitali. Ma la caratteristica che più di ogni altra ha segnato il successo delle applicazioni economico-finanziarie della *blockchain* è rappresentata dalla accettazione come mezzo di scambio per la fruizione di beni o servizi, che lascia intravedere una funzione *lato sensu* monetaria dei nuovi valori.

A differenza delle altre forme di *virtual currency*[1], la criptomoneta è accettata da un numero sempre maggiore di utenti e può essere riconvertita in valuta *fiat* presso appositi "sportelli" cambiavalute (flusso c.d. bidirezionale); vista da questa prospettiva la criptomoneta sembra offrire una alternativa al contante tradizionale per l'acquisto di determinati panieri di beni o per la realizzazione di operazioni strumentali alla successiva riconversione in valuta avente corso legale. A tal fine è stata coniata la definizione di "valuta virtuale" – che di recente ha pure fatto ingresso nel lessico del legislatore – per indicare sinteticamente «la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente»[2]. Benché il

[1] Prima dell'avvento di Bitcoin, le valute virtuali permettevano l'acquisto di un numero estremamente limitato di beni o di servizi all'interno di una piattaforma e non potevano essere riconvertite in valuta avente corso legale.

[2] Art. 1, comma 2, lett. qq) del D. Lgs. 21 novembre 2007 n. 231, introdotto dal D. Lgs. 25 maggio 2017 n. 90; successivamente la quinta Direttiva antiriciclaggio 2018/843/UE (art. 1, par. 1, punto 3) ha

legislatore abbia fornito una definizione che ne sottolinea – in positivo come in negativo – i connotati monetari[3], in dottrina è ancora molto discussa la natura giuridica da attribuire alle valute virtuali[4]; l'opera classificatoria è resa estremamente difficoltosa per via dell'elevata propensione degli attori economici ad acquistarle e scambiarle per finalità meramente speculative che, contrapponendosi alla funzione monetaria, evidenziano delle forti similitudini con le *securities* finanziarie.

La natura potenzialmente ibrida dei nuovi valori solleva numerose criticità in punto di disciplina applicabile, dovendosi di volta in volta stabilire a quale regime giuridico debbono essere soggetti[5]. Non essendo chiaramente possibile stabilire in astratto se la funzione monetaria sia prevalente o recessiva rispetto a quella finanziaria[6], e viceversa, si dovrà aver riguardo alla *ratio* di ciascun istituto e ai principi che regolano la materia (diritto tributario, finanziario, societario, amministrativo). È evidente come la soluzione relativa del problema si estenda *per relationem* anche alle fattispecie di reato che hanno ad oggetto o si realizzano per il tramite dei valori virtuali[7]; il perimetro di rilevanza penale di determinate condotte sarà delimitato dalla qualificazione giuridica da attribuire alle operazioni economiche, alle attività e ai servizi connessi all'utilizzo della criptomoneta.

Date tali premesse, riteniamo opportuno, ai fini di una ordinata trattazione, prendere dapprima in considerazione l'ambito di rilevanza penale relativo all'utilizzo delle valute virtuali in funzione monetaria (come mezzo di scambio e veicolo di ricchezza). Trattandosi di utilità economicamente apprezzabili, le valute virtuali potranno essere esaminate facendo riferimento a una classificazione già nota nella

codificato la seguente definizione «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 è stata ribadita dall'art. 2 della Direttiva 2019/713/UE.

[3] Occorre tuttavia rilevare che con l'entrata in vigore del D. Lgs. 125/2019, che recepisce la quinta direttiva antiriciclaggio, il legislatore ha modificato la definizione previgente inserendo nella norma l'inciso «o per finalità di investimento», che lascia preludere all'abbandono di un criterio definitorio basato sulla natura strettamente monetaria delle valute virtuali.

[4] LEMME G., PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin,* in *Rivista di diritto bancario*, 2016, 11, 10 ss.; GASPARRI G., *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* in *Dir. Inf.*, 2015, 1, 429; VARDI N., *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. Inf.*, 2015, 1, 450 ss.

[5] Si pensi, ad esempio, alla qualificazione a fini fiscali delle plusvalenze derivanti da investimenti in valuta virtuale oppure ai dubbi sulla riserva di attività per l'emissione o lo scambio di *asset* assimilabili a prodotti finanziari.

[6] A conferma della natura ibrida delle valute virtuali il legislatore – recentemente intervenuto per adeguare la normativa antiriciclaggio alle disposizioni della direttiva 2018/843/UE – ha fatto leva sul connotato finanziario di tali valori per evitare che gli obblighi preventivi avessero un campo di applicazione eccessivamente ristretto.

[7] Così, ad esempio, l'affermazione della natura finanziaria dell'emissione o dello scambio di valori virtuali renderà configurabili alcune fattispecie di esercizio abusivo previste dalla disciplina di settore (artt. 130 ss. D. Lgs. 385/1993; artt. 166 ss. D. Lgs. 58/1998); allo stesso modo la possibilità di considerare un *capital gain* la plusvalenza di investimento potrà assumere rilevanza per l'integrazione dei reati di omessa dichiarazione o omesso versamento di imposte dirette (cfr. artt. 5 ss. D. Lgs. 74/2000).

sistematica del diritto penale: come *strumento del reato*, quando la condotta delittuosa si realizzi per il tramite di esse[8]; come *profitto* o *prezzo del reato*, qualora siano il corrispettivo dato o promesso per la commissione del reato, ovvero l'utilità economica che ne deriva in via diretta e immediata[9]; come *oggetto del reato*, quando l'azione delittuosa insista su di esse[10].

Il capitolo successivo sarà invece dedicato alle fattispecie di reato configurabili allorché i nuovi valori vengano inquadrati come cripto-attività finanziarie (strumenti, prodotti o derivati) in una prospettiva di tutela del mercato[11].

1.1. Valute virtuali e moneta avente corso legale.

La diffusione delle valute virtuali è stata accompagnata da una suggestione generale[12] circa l'affermazione di una nuova forma di moneta del cyberspazio[13]. Sebbene la questione relativa alla natura giuridica dei nuovi valori tocchi in modo soltanto marginale l'oggetto della nostra analisi, si ritiene nondimeno utile un breve inquadramento dello stato dell'arte; ciò renderà più agevole la sussunzione della criptomoneta tra gli elementi tipici di alcune fattispecie di reato[14].

Alcuni studiosi[15] iniziarono a riflettere sulla riconducibilità del circolante virtuale alla nozione giuseconomica di moneta in un tempo in cui – almeno in Italia – nessuno sospettava che il fenomeno avrebbe assunto dimensioni così imponenti. Il *core* del problema non riguarda tanto l'equiparazione delle valute virtuali alla moneta avente corso legale – che è chiaramente da escludere – quanto piuttosto l'assolvimento da parte delle prime delle funzioni tipiche della seconda.

---

[8] DELOGU T., *Lo 'strumento' nella teoria generale del reato*, in *Riv. it. dir. proc. pen.,* 1974, 273 ss.

[9] Cfr. ALESSANDRI A., *Criminalità economica e confisca del profitto*, in DOLCINI E., PALIERO C.E. (a cura di), *Studi in onore di Giorgio Marinucci*, Milano, 2006, 203 ss.; MAUGERI A.M., *Le moderne sanzioni patrimoniali tra funzionalità e garantismo*, Milano, 2001; GRASSO G., sub *Art. 240*, in ROMANO M., GRASSO G., PADOVANI T. (diretto da), *Commentario sistematico del codice penale*, vol. III, Milano, 2011, 611 ss.; FUX A.,, *Ulteriori precisazioni sui confini della nozione di profitto: è necessaria l'"esternalità"*, in *Cass. pen.*, 2014, 5, 3253 ss.; MUCCIARELLI F., PALIERO C.E., *Le Sezioni Unite e il profitto confiscabile: forzature semantiche e distorsioni ermeneutiche*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2015, 4, 246 ss.

[10] In argomento si vedano le monografie di GIANNITI F., *L'oggetto materiale del reato,* Milano, 1966 e di ROCCO A., *L'oggetto del reato e della tutela giuridica penale,* Torino, 1913, 2 ss.

[11] Per quanto sia indubitabile che la diffusione degli *asset* virtuali abbia offerto nuovi strumenti per delinquere, agevolando la commissione di reati appartenenti alla c.d. *underground economy*, si deve del pari ammettere che il loro utilizzo per finalità pienamente lecite meriterebbe una protezione da parte del legislatore.

[12] GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin,* cit., 431

[13] DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, in *Dir. pen cont. – Riv. Trim*, 2018, 9, 104; BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. Inf.*, 2017, 1, 27.

[14] Così, ad es., si sosterrà l'impossibilità di sussumere la valuta virtuale nel concetto di "denaro" di cui all'art. 648-*bis* c.p. (ma piuttosto in quello di "altre utilità") oppure nella nozione penalistica di "cosa mobile" di cui all'art. 624 c.p.

[15] Si richiama il contributo di LEMME, PELUSO, *Criptomoneta e distacco dalla moneta legale*, cit., la cui pregevole ricostruzione sarà sinteticamente illustrata nel corso del paragrafo.

Sebbene non mancassero voci di segno contrario[16], qualche tempo addietro era diffusa opinione che l'espressione "moneta legale"[17] andasse intesa come moneta fisica, ossia le banconote cartacee e il denaro metallico[18]; ogni pagamento di tipo diverso, ancorché di comune accettazione (assegno o giroconto bancario, cambiale, postagiro) poteva tuttalpiù dare luogo a una *datio in solutum*.

Nello scenario attuale, l'impossibilità di equiparare i due concetti – e più in generale la conclamata perdita di centralità della moneta fisica come mezzo di pagamento – è divenuta un dato quasi incontrovertibile. L'utilizzo del contante sta oramai progressivamente venendo meno per effetto di una duplice azione erosiva: dall'alto, a livello normativo, per l'imposizione di presidi antiriciclaggio che limitano l'uso del denaro liquido; dal basso, a livello empirico, per la digitalizzazione dei rapporti economici e la progressiva estensione del paniere di beni acquistabili *online*, che rendono il denaro elettronico uno strumento di pagamento più pratico e maggiormente fungibile.

Con il tramonto del *gold standard* la moneta circola essenzialmente sulla base di un rapporto di fiducia verso l'emittente che, negli ordinamenti moderni, coincide con la banca centrale. Può certamente darsi che all'interno di una comunità si concordi sull'utilizzo di mezzi alternativi di adempimento delle obbligazioni, accettando *in solutum*, su base fiduciaria, valori rappresentativi di unità di conto. Nel passato come nel presente l'idea della concorrenzialità del mercato della moneta ha affascinato gli economisti[19], radicando la convinzione che la sovranità statuale sia una scelta politica, motivata da esigenze di controllo sociale più che dall'impossibilità tecnico-giuridica di accettare la presenza contemporanea di più valute concorrenziali[20]. Oggi più che mai queste teorie godono di terreno fertile a causa della progressiva dismissione del

---

[16] La dottrina più avanguardista sosteneva infatti che l'espressione "moneta legale" si riferisse essenzialmente alla moneta che assolve alla funzione di pagamento. In argomento LEMME G., *Moneta scritturale e moneta elettronica*, Torino, 2003; ID., *La rivoluzione copernicana della cassazione: la moneta legale, dunque, non coincide con la moneta fisica*, in *Banca, borsa e titoli di credito*, 2008, 2, 553 ss.

[17] Cfr. art. 1277 c.c.,

[18] Nonostante con il passare del tempo si fossero diffuse altre forme di circolazione monetaria, quali la moneta scritturale o bancaria e quella elettronica, l'equiparazione tra moneta legale e moneta fisica tendeva a perpetuarsi. La stessa dottrina osserva infatti come *«vi erano notevoli resistenze ad ammettere che questa identificazione, in certo qual modo scontata all'epoca di redazione del codice civile, fosse stata superata»*. L'attenzione degli studiosi si era concentrata sull'individuazione delle forme più diffuse di moneta alternativa al contante: nessuno in realtà dubitava che la moneta scritturale e quella elettronica si ponessero all'interno della sovranità monetaria, sicché l'oggetto della discussione era circoscritto al solo soddisfacimento del "valore legale". Per approfondimenti, LEMME, PELUSO, *Criptomoneta e distacco dalla moneta legale*, cit., 2

[19] KLEIN B., *The competitive supply of money*, in *Journal of Money, Credit and Banking*, 1974, vol. 6, 4, 423 ss.; BERENTSEN A., *On the private provision of fiat currency*, in *European Economic Review*, 2006, 7, 1683; più di recente, a proposito della diffusione delle valute virtuali, WAKNIS P., *Competitive Supply of Money in a New Monetarist Model*, MPRA Paper No. 75401, 11 settembre 2017, https://mpra.ub.uni-muenchen.de

[20] Uno dei più autorevoli sostenitori della teoria del libero mercato della moneta fu HAYEK F. A., *Denationalisation of Money*, London, 1976, secondo cui la privatizzazione monetaria sortirebbe un effetto profondamente positivo sul circuito economico.

monopolio pubblico della moneta come paradigma assoluto. Secondo alcuni un punto di svolta decisivo si è avuto con l'emanazione della Direttiva sui servizi di pagamento 2007/64/CE[21] la quale, armonizzando a livello eurounitario l'attività svolta dagli istituti di pagamento, avrebbe definitivamente segnato il passaggio dal modello dello Stato-produttore a quella dello Stato-regolatore dell'offerta di moneta[22].

Sebbene l'idea della democratizzazione monetaria di Hayek risalga a tempi precedenti rispetto alla diffusione di Internet, i primi progetti finalizzati alla creazione di una moneta unica della rete risalgono alla metà degli anni novanta[23]; bisognerà tuttavia attendere fino all'indomani del nuovo millennio perché la teoria veda una nuova alba. Ci si riferisce naturalmente all'avvento di Bitcoin che ha riacceso le speranze dei fautori di una moneta sottratta alle prerogative del controllo statale[24]. Alla base della trovata rivoluzionaria di Nakamoto vi è la combinazione della crittografia asimmetrica a doppia chiave con la tenuta di un registro distribuito e di un protocollo pubblicamente accessibile che rende superfluo il ruolo degli intermediari[25] nei pagamenti. Dacché ci si è chiesti se questa nuova forma di circolante virtuale possa considerarsi, dal punto di vista funzionale, come una vera e propria moneta. È risaputo che l'interrogativo ha ricevuto risposta negativa da parte della Banca Centrale Europea (BCE) che, in documento ufficiale[26], ha sottolineato con fermezza l'impossibilità di ricondurre la criptomoneta alla moneta legale[27], anche quando sia convertibile in euro presso intermediari autorizzati. Ancor più conservativo è l'approccio dell'Autorità

[21] La direttiva è stata recepita nel nostro ordinamento con D. Lgs. 27 gennaio 2010, n. 11 (Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno).
[22] Cfr. LEMME, PELUSO, *Criptomoneta e distacco dalla moneta legale*, cit., 3.
[23] Si ricorda, ad esempio, il tentativo di David Chaum di brevettare un sistema, denominato "ecash". Il progetto ebbe vita breve (1995- 1998) probabilmente a causa dell'eccessiva precocità dei tempi (ancora troppo immaturi per accettare l'idea di una novità così rivoluzionaria) accompagnata dall'obiettiva scarsa diffusione della rete Internet.
[24] La letteratura scientifica sul tema è piuttosto ampia. Oltre al contributo del fondatore NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, pubblicato su https://bitcoin.org, si richiamano, senza pretese di esaustività, le opere di BRITO J. (a cura di)., *The law of Bitcoin*, Bloomington, 2015; GUTTMANN B., *The Bitcoin Bible. Gold edition*., Norderstedt, 2013; ROSEMBUJ T., *Bitcoin*, Barcelona, 2016; AMATO M., FANTACCI L, *Per un pugno di bitcoin. Rischi e opportunità delle valute virtuali*, Milano, 2016.
[25] Bitcoin è basato su un sistema di registri distribuiti totalmente decentralizzato, il cui protocollo può essere scaricato da chiunque intenda prendere parte alla rete; la ricchezza digitale è controllata e autoprodotta secondo un meccanismo di ricompense per coloro che validano le transazioni. A differenza della moneta legale, la quantità di unità in circolazione non è controllata da alcuna autorità centrale ma è gestita in modo immodificabile dallo stesso protocollo di sistema (l'ammontare massimo è di 21 milioni). Le unità vengono create mediante un processo di *data mining*, in cui i partecipanti alla rete forniscono la loro potenza di calcolo, verificano e registrano le transazioni sulla *blockchain* e per questo ricevono in cambio le nuove unità appena coniate oltre alle commissioni di transazione.
[26] Il richiamo è al documento *Virtual currency schemes – a further analysis*, pubblicato sul sito https:/ecb.europa.eu nel Febbraio del 2015.
[27] Ne consegue che l'emissione e lo scambio di valuta virtuale sono attività che non rientrano nel campo di applicazione della Direttiva sui servizi di pagamento. La Banca Centrale conclude dunque nel senso che *«from the economic and legal perspectives […] virtual currencies should not be bundled into the generic words of money or currency, even though their technical appearance takes a form which has some similarities to scriptural money and/or electronic money»* (pag. 25).

Bancaria Europea (EBA) che, in un rapporto di poco precedente[28], aveva espresso serie preoccupazioni per la possibile destabilizzazione dell'integrità finanziaria dell'Unione a causa della crescita del mercato valutario virtuale.

1.2. Bitcoin e funzioni tipiche della moneta.

È bene anzitutto precisare che la nozione stessa di "moneta" è suscettibile di almeno due diverse declinazioni, a seconda che si prediliga l'approccio statocentrico o quello funzionale[29]. Adottando questo secondo e più flessibile criterio, la dottrina si è interrogata sulla capacità di Bitcoin – e delle valute virtuali nel loro complesso – di assolvere alle tre principali funzioni della moneta tradizionalmente ricondotte a mezzo di scambio, unità di conto e riserva di valore. Secondo alcuni Bitcoin altro non sarebbe che una forma di investimento speculativo[30], che, ben lungi dal soddisfare le funzioni della moneta, sarebbe stato creato al solo scopo di creare un mercato parallelo a quello dei titoli finanziari. Secondo altri, invece, le valute virtuali assolvono appieno alle funzioni della moneta e sarebbero, quindi, il più valido concorrente della *fiat currency*, che, nel prossimo futuro, potrebbero addirittura essere soppiantata, in tutto o in parte[31].

Partendo dalla prima delle predette funzioni, è stato rilevato[32] che Bitcoin come *mezzo di scambio* differisca in modo sostanziale dalle valute aventi corso legale specialmente in relazione alle cosiddette "esternalità di rete"[33]. Il coefficiente di utilizzo come medium negli scambi è direttamente proporzionale al numero utenti (*vendors* e *customers*) che adoperano la criptomoneta per la compravendita di beni o servizi: riducendosi il numero dei venditori/fornitori disposti ad accettare Bitcoin, i consumatori saranno meno inclini a procurarsi riserve di moneta virtuale; allo stesso modo i primi saranno meno disposti ad accettarlo *in solutum*, se sono pochi gli utenti a volerlo adoperare nelle transazioni. Affinché Bitcoin possa diventare una valuta globale di scambio, dovrebbe superare l'*impasse* tipico di questa esternalità di rete: i consumatori dovrebbero *«convincersi a usarla e i venditori/fornitori ad accettarla come strumento di pagamento consueto e ordinario»*[34].

---

[28] Si richiama il rapporto denominato *Opinion on virtual currencies* del 04 luglio 2014, in https://eba.europa.eu/

[29] Cfr. VARDI, *"Criptovalute" e dintorni*, cit., 450; GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin,* cit., 417; DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 108.

[30] YERMACK D., *Is Bitcoin a real currency? An economic appraisal*, NBER Working Paper No. 19747, National Bureau of Economic Research, Cambridge (MA), 2013.

[31] GANS J.S., HALABURDA H., *Some Economics of Private Digital Currency*, in GOLDFARB A., GREENSTEIN S., TUCKER C. (a cura di), *Economic Analysis of the Digital Economy*, Chicago, 2015; PLASSARAS, N.A., *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, in *Chicago Journal of International Law*, 2013, 14, 377 ss.

[32] Cfr. LEMME, PELUSO, *Criptomoneta e distacco dalla moneta legale*, cit., 13; GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin,* cit., 418.

[33] Sulle esternalità di rete nei sistemi di pagamento elettronico v. GOWRISANKARAN, G., STAVINS, J., *Network externalities and technology adoption: lessons from electronic payments,* in *Rand Journal of Economics*, 2004, vol. 35, 2, 260 ss.

[34] Così, LEMME, PELUSO, *Criptomoneta e distacco dalla moneta legale*, cit., 17

La seconda funzione tipica della moneta è quella di *unità di conto*, vale a dire la capacità di misurare il valore di scambio e di mercato di beni e servizi; a tal fine essa dovrà possedere due caratteristiche essenziali: la divisibilità e la stabilità del potere di acquisto nel breve periodo. *Nulla quaestio* sul primo requisito, ampiamente soddisfatto dalla possibilità di frazionare ogni Bitcoin (฿) fino alla milionesima unità (detta *satoshi*, ь)[35]. Il prezzo di Bitcoin è, tuttavia, estremamente volatile e soggetto a continue oscillazioni, tanto da rendere assolutamente incerto e imprevedibile il valore di ogni singola unità nel prossimo futuro. Ciò incide negativamente sull'andamento del mercato, creando disorientamento tra gli attori economici[36].

La funzione di *riserva di valore* descrive l'attitudine della moneta a conservare il proprio valore nel tempo perché possa essere accantonata e utilizzata in futuro senza correre il rischio della sua improvvisa svalutazione. Tutte le valute statali hanno una tendenza inflazionistica: la stabilità del potere d'acquisto è solitamente garantita dalla Banca Centrale, che sovrintende alla politica monetaria regolando l'offerta di moneta a livello macroeconomico. Si è detto che la misura massima del circolante di Bitcoin è predeterminato; ciò spiega perché molti ritengono che abbia una tendenza deflazionistica in grado di farne apprezzare il valore con il passare del tempo (c.d. scarsità artificiale), rendendolo immune dalle scelte politiche dei governi[37]. Rimane tuttavia l'ostacolo dell'estrema volatilità del prezzo, che impedisce di fatto di preservare la ricchezza al riparo dal rischio di una repentina svalutazione[38]. Sono invece privi di fondamento i dubbi circa la capacità della *blockchain* di garantire la sicurezza delle transazioni, sollevati a proposito dei prelievi indebiti di somme depositate presso piattaforme di scambio; risulta infatti evidente come la vulnerabilità sia insita nel sistema informatico degli intermediari e non nell'algoritmo di criptazione delle valute virtuali.

La volatilità del prezzo rappresenta dunque il vero limite al riconoscimento della natura monetaria di Bitcoin. Il *discrimen* rispetto alle valute tradizionali emerge chiaramente dall'impossibilità di adempiere in modo perfetto alle funzioni di mezzo di scambio, unità di conto e riserva di valore. È tuttavia bene precisare come una tale conclusione sia soltanto provvisoria, non potendosi chiaramente escludere – in base

[35] Si potrebbe al limite sollevare il dubbio di una eccessiva divisibilità, tale da rendere scarsamente intellegibile il valore nominale di ogni singola sottounità di conto (che il più delle volte è espressa da svariate cifre decimali dopo lo zero, es. 0.000004 ฿).

[36] Le frequenti variazioni di prezzo determinano effetti negativi rilevanti per tutti gli attori del mercato. I venditori/fornitori dovranno necessariamente adeguare i prezzi per evitare cali di redditività o competitività, a seconda che le oscillazioni siano in positivo o in negativo; il che rischia di creare intoppi alla filiera produttiva causati dalla discrepanza tra i prezzi di mercato dei prodotti finiti e i costi sostenuti per la produzione. Parimenti, i consumatori incontreranno non poche difficoltà nell'individuare i veri prezzi relativi dei beni e dei servizi che vorrebbero acquistare e nell'effettuare le migliori scelte in base al proprio vincolo di bilancio.

[37] Cfr. PLASSARAS, *Regulating Digital Currencies*, cit., 390

[38] Si potrebbe opinare che le oscillazioni del prezzo sono un fenomeno di breve termine, mentre nel lungo periodo il valore di Bitcoin è senza dubbio cresciuto in modo costante. L'obiezione presta tuttavia il fianco alla critica dell'impossibilità di dimostrare l'assunto a soli dieci anni dalla creazione della criptomoneta.

alla teoria funzionale – la possibilità che in futuro il circolante virtuale assuma tutti i connotati tipici della moneta[39].

1.3. Speculazione finanziaria e volatilità del prezzo della criptomoneta.

Appurato dunque che l'elevata volatilità della criptomoneta nel breve periodo[40] ne diminuisce la capacità di rappresentare un'unità di conto effettiva[41], ci si chiede quale siano le cause di un andamento così altalenante.

È risaputo come il fascino del mercato valutario virtuale sia dovuto alla possibilità di ottenere, in un breve periodo, plusvalenze di investimento piuttosto generose: la maggior parte degli utenti compra e vende per motivi volti al conseguimento di un profitto, piuttosto che per l'acquisto di beni o servizi. L'assunto trova conforto in alcune statistiche di recente pubblicazione[42], dalle quali si ricava l'esistenza di una relazione di proporzionalità diretta tra l'aumento del prezzo del titolo e il numero di transazioni sulla *blockchain*[43]. Per contro, se la valuta fosse utilizzata dai più come mezzo di scambio per la fruizione di beni o servizi, il numero di transazioni non sarebbe così strettamente legato alle oscillazioni del prezzo, poiché la necessità di fruire di beni o servizi non è funzione del valore nominale di una moneta.

Il ridotto impiego delle valute virtuali come strumento di pagamento si deve a cause che, verosimilmente, vanno oltre le oscillazioni del prezzo e riguardano da vicino quelle "esternalità di rete" di cui si è detto pocanzi. Benché la capitalizzazione del mercato sia in continua crescita, non vi è ancora un diffuso consenso sull'accettazione

---

[39] Riteniamo al riguardo di poter condividere le riflessioni di LEMME, PELUSO, *Criptomoneta e distacco dalla moneta legale*, cit., 39, i quali ritengono comprensibile che ci sia ancora un certo margine di indeterminatezza circa il meccanismo di formazione del prezzo. Gli autori osservano come la volatilità di Bitcoin potrebbe tendere a diminuire con la progressiva affermazione come mezzo di pagamento, con conseguente riduzione della voracità speculativa del mercato, sebbene la tendenza deflazionistica possa divenire un problema *«proprio perché Bitcoin, raro e limitato, tenderebbe a divenire più un bene rifugio che un mezzo normale di adempimento delle obbligazioni pecuniarie»*.

[40] Per una panoramica aggiornata in tempo reale dell'andamento del prezzo di ciascuna valuta dalla sua prima quotazione si consulti il sito https://coinmarketcap.com/charts/

[41] YERMACK D., *Is Bitcoin a real currency? An economic appraisal*, cit., 4. Si è detto che le frequenti variazioni del prezzo causano costi diretti e indiretti agli attori economici che accettano pagamenti in valuta virtuale e la perdita di competitività sul mercato. Difatti, mentre i fattori di produzione e gli *input* intermedi si pagano in valuta *fiat*, i beni finali vengono venduti (anche) per BTC; l'oscillazione del prezzo può causare uno scarto significativo nei prezzi tra *input* e *output* con il conseguente effetto di confondere i consumatori e le stesse imprese.

[42] KRISTOUFEK L., *What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis*, 15 aprile 2015, in https://journals.plos.org

[43] Si tratta, tuttavia, di una relazione non perfetta e contenuta dalla ridotta scalabilità dell'infrastruttura. Basti pensare che nel 2017, anno in cui la popolarità di Bitcoin è esplosa, l'elevato numero di transazioni ha congestionato la rete, portando il costo medio delle transazioni a salire alle stelle. in periodi di elevato traffico, ossia in cui avvengono moltissime transazioni, il costo medio della *fee* si alzi, perché più transazioni "competono" tra loro per essere verificate sulla *blockchain*. Quando i prezzi del Bitcoin aumentano, anche i costi di transazione sembrano aumentare e quando i costi di transazione raggiungono livelli che i partecipanti al mercato non possono più sostenere, il prezzo del Bitcoin spesso trova un equilibrio verso il basso.

delle stesse come mezzo di estinzione delle obbligazioni. A ciò si aggiungano le difficoltà legate all'ottenimento di una provvista in criptovaluta. Gli utenti possono infatti acquisire scorte monetarie partecipando attivamente al processo di *data mining* oppure scambiando valuta *fiat* sulle piattaforme[44], *tertium non datur*. Si ritiene che l'*impasse* dell'esternalità potrà essere superata soltanto nel momento – futuro o futuribile – in cui il denaro virtuale verrà pagato come corrispettivo per prestazioni in natura (lavorative, prestazione di opera, prezzo per la fruizione di beni o servizi).

Per concludere, pare che la tendenza deflazionistica che caratterizza la maggior parte delle valute sia l'ostacolo più significativo all'affermazione del circolante virtuale come strumento di pagamento[45]. La generalità dei progetti *blockchain* presenta un numero di circolante limitato, tale per cui chi acquista criptoattività sarà portato a detenere per lungo tempo l'*asset* – pratica in gergo definita "Hodl" – sperando in una sua rivalutazione: la sua natura deflattiva, in uno con l'alta volatilità, ostano dunque a una sua generale diffusione come "moneta" in senso funzionale.

1.4. Mercato valutario virtuale e variabili macroeconomiche. Spunti di riflessione sulla condizione di equilibrio nel modello keynesiano della moneta.

Sebbene il circolante virtuale assolva soltanto in parte alla funzione di moneta complementare, essendo acquistato e scambiato in misura ben più significativa per fini soltanto speculativi, ciò non toglie che, in qualche modo, possa comunque influire sulle variabili di un sistema macroeconomico. Tutte le valute virtuali appaiono caratterizzate da una funzione astrattamente monetaria (attitudine ad essere impiegate come mezzo di pagamento) e dalla tendenza deflazionistica (attitudine ad accrescere il proprio valore nel tempo come un prodotto o un derivato finanziario); la maggior parte di esse è gestita in modo diffuso e pienamente concorrenziale da parte di fornitori di servizi e degli utenti che intendono scambiarla da e per moneta reale. È dato dunque ipotizzare che gli investitori troveranno conveniente comprare o vendere gli asset virtuali in base ai fabbisogni individuali e alle aspettative di investimento.

La quotazione nei mercati finanziari tradizionali di titoli legati all'andamento di valori virtuali[46] ha portato alla luce i numerosi "portali" di comunicazione tra i due universi paralleli: il mondo della finanza tradizionale risulta oggi tutt'altro che impermeabile agli sviluppi dell'economia virtuale. Esistono, a nostro avviso, forti

[44] Nel primo caso si ha una restrizione all'accesso dovuto alle ingenti spese da sostenere per l'acquisto degli elaboratori e dell'energia necessari a ottenere le ricompense; nel secondo l'acquisto è inscindibilmente legato al previo possesso di somme in valuta legale, di talché se l'utente non ne ha disponibilità non potrà ricevere criptomoneta.

[45] In un periodo di deflazione rapida gli individui e le imprese tendono a rimandare spese ed investimenti, sperando in una futura caduta dei prezzi, ed in un ambiente (fortemente) deflazionistico, come anche in un contesto fortemente inflazionistico, una valuta perde la sua funzione di unità di conto. Cfr. CANTARELLA M., *Il Bitcoin e la dottrina della deflazione,* 13 maggio 2015, in https://rethinkecon.it

[46] Basti pensare alla vicenda relativa alla quotazione a Wall Street dei *futures* su Bitcoin verso la fine del 2016.

segnali dell'interferenza tra queste due dimensioni dovuti *in primis* alle scelte di investimento del singolo operatore economico che, dovendo decidere dove investire la propria ricchezza, si troverà di fronte all'alternativa tra strumenti finanziari e valori virtuali.

Senza pretendere, in questa sede, di dar conto dei riflessi macroeconomici della *blockchain* con la dovizia ricostruttiva che ciò richiederebbe, dovremo limitarci ad un sommario esame della questione al fine di meglio comprendere le numerose interferenze tra le due dimensioni finanziarie[47]. Nel dettaglio, ci si chiede se la circolazione dei nuovi valori possa condizionare il mercato reale e la produzione aggregata in base al modello IS-LM, dando luogo a una sorta di fungibilità tra moneta reale e moneta virtuale in grado di incidere sull'equilibrio del sistema macroeconomico[48].

Come noto, il modello IS-LM (*Investment Saving - Liquidity Preference Money Supply*) rappresenta tuttora un pilastro fondamentale della macroeconomia[49], intorno al quale si è sviluppato un ampio dibattito tra gli economisti sulla sua capacità di spiegare quanto avviene in un sistema economico, con particolare riguardo alla valutazione degli effetti di politica fiscale e di politica monetaria sulla determinazione del reddito di equilibrio[50]. Assumendo a postulato l'interferenza reciproca tra il mercato valutario virtuale e le variabili dell'economia reale – poiché la scelta di convertire la moneta *fiat* in valuta virtuale dipende *inter cetera* dall'aspettativa di ritorno dell'investimento, o meglio dal *surplus* che l'investitore prevede di poter realizzare acquistando criptomoneta anziché investire nei titoli mercato finanziario reale – può dedursi che l'offerta di moneta reale da una parte e il *rate of interest* dei titoli nel mercato finanziario siano condizionati dalla circolazione dei nuovi valori.

In un sistema economico in cui i valori virtuali assolvono alla duplice funzione di strumento di investimento e di mezzo di scambio per l'acquisto di beni o servizi è verosimile che la domanda di criptomoneta dipenda in misura direttamente proporzionale dal volume complessivo delle transazioni[51] ed inversamente

---

[47] Si veda, sebbene con riferimento ai valori virtuali di emissione statale, il recente lavoro di BARRDEAR J., KUMHOF M., *The macroeconomics of central bank issued digitalcurrencies*, Bank of England Staff Working Paper No. 605, luglio 2016, in https://bankofengland.co.uk

[48] Per una analisi delle implicazioni del circolante virtuale sulla politica monetaria delle banche centrali si rinvia al documento di discussione del Parlamento Europeo denominato "Cryprocurrency and monetary policy", luglio 2018, in http://europarl.europa.eu

[49] Il modello è stato costruito a partire dalla autorevole lezione di KEYNES J. M., *The General Theory of Employment, Interest, and Money*, New York, 1936. La curva di investimento/risparmio (IS) è una variazione del modello di spesa/reddito, che incorpora i tassi di interesse di mercato (domanda), mentre la curva di liquidità/equilibrio dell'offerta (LM) rappresenta la quantità di denaro disponibile per l'investimento (offerta).

[50] In argomento, nella manualistica, IMBRIANI C. – LOPES A., *Teorie macroeconomiche e sistema finanziario*, Novara, 2011, 164; PIVETTI M., *Economia politica*, Bari, 2002, 125; ARCELLI M., DONGILI P., *Economia monetaria*, Padova, 1977, 35 ss. a cui si rinvia per gli opportuni approfondimenti sulla costruzione e sul funzionamento del modello.

[51] Che, come si è detto, a sua volta dipende dal numero di beni o servizi che gli utenti possono acquistare in valuta virtuale e dall'aspettativa di aumento del valore nel breve periodo.

proporzionale dal costo opportunità di detenere gli *asset* finanziari reali[52]. Se il tasso di interesse praticato sui mercati finanziari reali diminuisce, aumenta la domanda di moneta reale e la propensione a convertirne una parte in valuta virtuale a fini speculativi[53]; viceversa, un maggior rendimento dei titoli del mercato finanziario reale riduce la domanda di moneta reale e, per l'effetto, anche quella di moneta virtuale poiché gli attori economici troveranno conveniente detenere meno liquidità ed investire in strumenti finanziari[54].

La verificabilità empirica di queste variabili dipende dal grado di *sensibilità* della domanda di moneta virtuale alle variazioni del tasso di interesse praticato sul mercato finanziario reale; in un sistema economico in cui vi è un alto *fabbisogno monetario* per unità di reddito gli operatori sono meno sensibili all'aumento del tasso di interesse sul mercato finanziario e, pertanto, sarà necessaria una maggiore quantità di moneta fiat per convertirne una parte in moneta virtuale[55].

Il modello appena descritto è applicabile, con buon grado di approssimazione, soltanto a un sistema economico caratterizzato dalla fungibilità reciproca di moneta reale e moneta virtuale e dall'alta propensione degli operatori economici a servirsi dell'una o dell'altra in base al reddito, alla produzione aggregata di beni o servizi che possono essere acquistati in valuta virtuale e alle aspettative di investimento. Si ritiene chiaramente prematuro applicare questo modello al contesto economico attuale, caratterizzato da una fase ancora embrionale della *distributed economy*[56]. Ma se il circolante virtuale dovesse davvero affermarsi come moneta in senso funzionale, divenendo una concreta alternativa al circolante reale, l'interazione tra il mercato dei beni ed economia virtuale diverrebbe sempre più stretta.

A scioglimento della riserva formulata in apertura del paragrafo si ritiene pertanto di poter concludere nel senso di un *condizionamento parziale* dell'economia reale per effetto della circolazione dei nuovi valori. Benché un simile sistema non trovi riscontro

[52] Se la domanda di moneta virtuale dipende in modo positivo dall'importo complessivo delle transazioni e negativamente dal costo opportunità di investire il denaro sul mercato finanziario reale, le due variabili e dovranno giocoforza interagire per mantenere l'equilibrio.

[53] Volendo ipotizzare gli effetti sul piano macroeconomico generale secondo il modello IS-LM, l'espansione potrebbe sortire effetti reali sulla produzione in conseguenza della riduzione del tasso di interesse. Quindi, se si considera costante il volume delle transazioni in valuta virtuale, l'aumento dell'offerta di moneta fa diminuire il tasso di interesse sul mercato finanziario reale, poiché gli operatori economici, per far fronte all'inflazione di circolante virtuale, tenderanno ad acquistare strumenti finanziari cedendo le riserve monetarie aggiuntive: ciò innalza il prezzo dei titoli e fa scendere il tasso di interesse, aumentando la produzione.

[54] A fronte di un'offerta di moneta costante, gli operatori economici tenderanno a vendere strumenti finanziari per ottenere delle scorte monetarie aggiuntive: ciò deprime il prezzo dei titoli e innalza il tasso di interesse.

[55] La *sensibilità della domanda di moneta* e il *fabbisogno monetario per unità di reddito* variano in base al sistema economico considerato. Nell'attuale scenario della finanzia virtuale sembra registrarsi una scarsa sensibilità degli investitori all'acquisto di moneta virtuale per effetto dell'andamento del rendimento dei titoli del mercato finanziario reale. Nondimeno, vi è motivo di credere che il valore di sia destinato ad aumentare nel lungo periodo, con la progressiva stabilizzazione del mercato dei valori virtuali e l'incremento della fiducia che gli operatori economici ripongono in esso.

[56] Cfr. LAMBIN J., *A Distributed and Collaborative Economy*, in ID., *Rethinking the market economy*, London, 2014, 164.

nella realtà attuale, la progressiva crescita del mercato valutario virtuale lascia presagire come, nel prossimo futuro, la ricostruzione diverrà sempre più verosimile.

1.5. Conclusioni in punto di natura giuridica delle valute virtuali dalla prospettiva del diritto penale.

Allo stato, non pare dunque possibile equiparare la criptomoneta alla moneta avente "corso legale"[57]. Quand'anche le si volesse accordare valore monetario – secondo i dettami della teoria c.d. funzionale – occorrerebbe tenerla distinta dalla moneta elettronica, con la quale condivide soltanto il sostrato digitale[58].

La valuta virtuale non presenta né il requisito dell'emissione dietro ricevimento di fondi per effettuare operazioni di pagamento né quello della rimborsabilità in denaro a richiesta del detentore[59]. Sul piano definitorio non sfuggono le profonde differenze rispetto alla nozione di moneta elettronica prevista dal TUB, con cui si indica «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 […] e che sia accettato da persone fisiche e giuridiche diverse dall'emittente»[60].

Il *token* scambiato sui mercati virtuali non è rappresentativo di un credito nei confronti dell'emittente[61], non possiede alcun valore intrinseco, né potrebbe essere rimborsato per valuta corrente. Non si deve incorrere nell'errore di ritenere soddisfatto il requisito della convertibilità per il solo fatto della presenza di soggetti privati (*exchange provider*) disposti ad acquistare valute virtuali per moneta corrente; oltre a trattarsi di una circostanza del tutto eventuale è evidente come la conversione sia operata da un soggetto terzo, diverso rispetto all'emittente, sulla base di un negozio giuridico rimesso all'autonomia delle parti.

---

[57] Trattandosi di valori di privata emissione, svincolati da qualsiasi ente emittente centralizzato e monopolistico, difficilmente potranno assolvere a una funzione monetaria secondo l'approccio statualista.

[58] Sul punto, DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 108

[59] Cfr. art. 11 della Direttiva 2009/110/CE concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica. Gli emittenti moneta virtuale non saranno dunque soggetti alla vigilanza prudenziale cui sono invece sottoposti gli emittenti moneta elettronica (Cfr. Titolo V-*bis* TUB, introdotto dall'art. 1 del D.lgs. 45/2012, e in particolare l'art. 114-*quinquies*.2).

[60] Art. 1, comma 2, lett. *h-ter)* TUB introdotta dal D. Lgs. 16 aprile 2012, n. 45, definizione mutuata quasi testualmente dall'art. 1, par. 1, n. 2) della Direttiva. Ai sensi dell'art. 114-*bis* TUB, l'emissione di moneta elettronica è riservata alle banche e agli istituti di moneta elettronica; il successivo art. 114-*ter* prevede che l'emittente di moneta elettronica debba rimborsare, su richiesta del detentore, la moneta elettronica in ogni momento e al valore nominale, secondo le modalità e le condizioni indicate nel contratto di emissione in conformità con l'art. 126-*novies*. La Banca d'Italia iscrive in un apposito albo gli istituti di moneta elettronica autorizzati in Italia e le relative succursali, previa verifica sul possesso dei requisiti di cui all'art. 114-*quinquies* TUB.

[61] Nelle *blockchain* pubbliche non sarebbe peraltro possibile individuare l'emittente del *token*, mancando un centro di imputazione e una *governance* centralizzata. Di certo non si potrà qualificare tale il partecipante che ha "minato" il singolo blocco per l'ovvia ragione che, così argomentando, vi sarebbero tanti "emittenti" quanti sono i nodi della rete.

Ci si domanda ora quali siano le conseguenze in punto di responsabilità penale delle asserite differente tra il circolante virtuale e la moneta *stricto sensu* considerata. Sul piano della tassatività nell'applicazione della fattispecie e del generale divieto di analogia *in malam partem*, ne deriva un ostacolo insormontabile all'inquadramento nei concetti di "denaro" (artt. 314, art. 317 ss., 377, 416-*ter* c.p., 644, 646, 648 ss. c.p.) e di "moneta" (artt. 453, 458, 693 c.p.). Se ciò non apre maglie di irresponsabilità per quelle ipotesi di reato descritte in termini assai ampi mediante il richiamo alle "altre utilità"[62], lo stesso non può dirsi per tutte le altre che fanno riferimento al concetto di "cosa" (così, ad es. per la ricettazione e l'appropriazione indebita). Si tratta di un tema particolarmente spinoso, che sarà approfondito nel prosieguo allorché si passerà a considerare la valuta virtuale come oggetto della tutela penale[63]. Deve invece affrontarsi in questa sede la questione relativa alla impossibilità di considerare la valuta virtuale come "denaro", sostantivo che *prima facie* potrebbe apparire più ampio rispetto al termine "moneta". Non occorre scomodare la semantica[64] per dimostrare che i due termini sono sinonimi: il denaro indica ogni tipo di moneta metallica o cartacea[65]. Pertanto, si cadrebbe fuori dal perimetro dell'interpretazione estensiva se si pretendesse di applicare a fatti commessi mediante l'impiego di valute virtuali fattispecie descritte unicamente con riferimento al "denaro"[66].

1.5.1. Ricchezza virtuale e "profitto" in senso penalistico.

Nessun dubbio che la moneta virtuale possa rientrare nel lato concetto penalistico di "profitto", rilevante per l'integrazione di alcune fattispecie di reato (artt. 640, 640-*ter* c.p.) e ai fini della confisca (artt. 240, 240-*bis*, 322-*ter*, 640-*quater* c.p.; art. 12-*bis* D. Lgs. 74/2000; art. 11 L. 146/2006). La determinazione della nozione di profitto è questione indubbiamente delicata poiché la giurisprudenza in materia tende talora a dilatare a dismisura il concetto o a restringerlo in base all'ipotesi di reato considerata o all'oggetto dell'ablazione patrimoniale[67].

Quanto al primo aspetto, in dottrina si contrappongono due accezioni di profitto. Secondo alcuni esso indicherebbe il soddisfacimento di qualsiasi interesse o utilità,

[62] Come avviene per tutti gli indicati delitti contro la pubblica amministrazione e per le ipotesi di riciclaggio, reimpiego e autoriciclaggio (artt. 648-*bis* ss., che saranno oggetto di specifico approfondimento).
[63] In questo capitolo, *infra* § 5.2. ss.
[64] Dal latino denarĭum nūmmum, lett. 'moneta da dieci' (deriv. di dēni). Cfr. CASTIGLIONI L, MARIOTTI S., *Vocabolario della lingua latina*, Torino, 2007, voce *denarium*.
[65] Secondo il dizionario Garzanti della lingua italiana per "denaro" si intende *«ogni tipo di moneta metallica o cartacea. Soldi, ricchezze, quattrini»*.
[66] Così, ad esempio, non potrebbe rispondere di scambio elettorale politico-mafioso chi ottenga la promessa di voti in cambio di un accredito in criptovaluta poiché l'art. 416-*ter* si riferisce unicamente al "denaro" e non anche ad altre utilità.
[67] MAUGERI A.M., voce *Confisca (diritto penale*), in *Enc. Dir.,* Annali VIII, 2015, § 7

anche morale, spirituale o psicologica[68]; altri rilevano invece come, in relazione ad alcune fattispecie[69], il profitto assuma una marcata accezione patrimonialistica, e andrebbe dunque identificato con l'accrescimento della ricchezza o un suo mancato decremento[70]. Il codice penale non sembra ancorare il profitto a parametri di riferimento certi, sicché è inevitabile che sul profitto si sia formata una casistica giurisprudenziale sottratta a qualsiasi regola generale ed astratta[71].

Parimenti non vi è unanimità di vedute sulla nozione di profitto confiscabile, che la giurisprudenza intende in modo variabile in base alle differenti tipologie di confisca presenti nel nostro ordinamento. In base all'orientamento maggioritario il profitto del reato deve essere identificato con il *«beneficio aggiunto di tipo patrimoniale […] a esso pertinente secondo un rapporto 'causa-effetto'»*, nel senso che il profitto deve essere *«una conseguenza economica immediata ricavata dal fatto di reato […] che per essere tale deve rappresentare un risultato positivo»*[72], definizione che però è stata progressivamente erosa dalla proliferazione di ipotesi speciali di confisca per equivalente[73]. Ancor più discussa è la possibilità di confiscare il risparmio di spesa e alla natura dell'ablazione patrimoniale (diretta o per equivalente) derivante dalla commissione di un reato tributario. La questione sarà affrontata *funditus* con riferimento ai delitti di in materia di dichiarazione e versamento delle imposte sulle plusvalenze di investimento in valuta virtuale (artt. 4 ss. D. Lgs. 74/2000), e al reato di

---

[68] In tal senso v. ANTOLISEI F., *Manuale di diritto penale – Parte speciale*, vol. II, Milano, 2008, 374, il quale ritiene che il concetto penalistico di profitto debba essere ricostruito in modo unitario, non potendo assumere un significato diverso in ciascuna ipotesi di reato (così, ad es., la nozione di profitto quale fine del dolo specifico nel furto dovrà corrispondere a quella di profitto quale evento della truffa).

[69] Nel sistema dei reati contro il patrimonio il profitto si presenta per lo più come contenuto del dolo specifico. Per questo motivo esso subisce un secondo processo di 'smaterializzazione': non importa che sia accertato il suo effettivo conseguimento da parte dell'agente, basta che costituisca lo scopo a cui il soggetto attivo tende. Rimangono tuttavia quelle fattispecie costruite come reato di evento (artt. 629, 640 c.p.) in cui vi è una diffusa tendenza al recupero del connotato patrimoniale.

[70] Cfr. FIANDACA G., MUSCO E., *Diritto penale – Parte speciale*, vol. II, Bologna, 2014, 189, secondo cui la componente patrimoniale del profitto emergerebbe piuttosto chiaramente, ad es., nella truffa.

[71] Osserva SGUBBI F., voce *Patrimonio (reati contro il)*, in *Enc. Dir.*, XXXII, 1982, § 24 che *«nel nostro ordinamento, per effetto congiunto del dettato legislativo e dell'elaborazione interpretativa, il profitto costituisce un elemento di fattispecie che non esprime una realtà naturalistico-materiale certa; il profitto non viene inteso in termini economici, come vantaggio o utilità o incremento patrimoniale: non viene inteso in quei termini descrittivi e materiali che lo renderebbero dotato di sufficiente certezza e sicurezza operativa: il profitto, nel sistema dei reati contro il patrimonio, non è il lucro: non è l'equivalente, non è il reciproco-opposto (dalla parte dell'agente) di ciò che è il danno dalla parte della vittima. Il profitto consiste in una utilità, vantaggio, soddisfazione, piacere di qualsiasi natura, patrimoniale o non patrimoniale».*

[72] Cfr. Cass. Pen., Sez. Un., 2 luglio 2008, n. 26654, in *Diritto penale contemporaneo*, 20 aprile 2015, con nota di MUCCIARELLI F., PALIERO C.E., *Le Sezioni Unite e il profitto confiscabile: forzature semantiche e distorsioni ermeneutiche*; Cass. Pen., Sez. Un., 25 giugno 2009, n. 38691, in *Riv. it. dir. proc. pen*., 2011, 2, 783 ss., con nota di MAUGERI A.M., *La confisca per equivalente ex art. 322*-ter *tra obblighi di interpretazione conforme ed esigenze di razionalizzazione*.

[73] Come noto, la confisca di beni, denaro o utilità di valore equivalente allontana la confisca dal paradigma della misura di sicurezza, avvicinandola a quello della pena. Il legislatore ha in tal modo eroso il legame di diretta derivazione causale del profitto dall'illecito superando a piè pari le difficoltà sollevate dal successivo reimpiego della ricchezza (profitto c.d. indiretto). Per approfondimenti, MAUGERI, voce *Confisca (diritto penale*), cit., § 8

sottrazione fraudolenta al pagamento delle imposte commesso mediante operazioni fraudolente di cambio (art. 11)[74]. Non sono del resto trascurabili neppure le criticità connesse alla esecuzione dell'ablazione patrimoniale, che, come si vedrà, si scontrano con la particolare inafferrabilità dei valori virtuali[75].

Pur con le riserve sopra rappresentate e salva la necessità di un ulteriore approfondimento, possiamo concludere nel senso della piena riconducibilità dei valori virtuali alla nozione penalistica di profitto. Trattandosi di utilità economicamente apprezzabili, scambiate sul mercato da e per valuta corrente, integrano la predetta nozione anche nell'accezione minimale di accrescimento del patrimonio o un suo mancato decremento delineata dalla dottrina a proposito di alcuni reati del titolo XIII[76].

1.5.2. L'*asset* virtuale come documento informatico. Brevi cenni sulla punibilità del falso ex art. 491-*bis* c.p.

Si potrebbe discutere sulla riconducibilità della valuta virtuale al "documento informatico", quale rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, secondo la definizione del Codice dell'Amministrazione Digitale (art. 1, comma 1, lett. p, D. Lgs. 7 marzo 2005, n. 82). La definizione del CAD rappresenta oggi un elemento normativo rilevante ai fini dell'integrazione di alcune fattispecie poste a tutela della fede pubblica[77].

Con la legge di conversione del c.d. Decreto semplificazioni il legislatore ha disciplinato l'efficacia probatoria della memorizzazione di un documento informatico su un registro distribuito[78], prevedendo in particolare che i contratti *smart* possano

[74] In questo capitolo, *infra* § 6.4.
[75] Al tema sarà dedicato ampio spazio nell'ultimo capitolo, nella parte dedicata alle misure cautelari reali (*infra*, Cap V, § 7).
[76] FIANDACA - MUSCO, *Diritto penale*, ult. cit.
[77] L'introduzione nell'ordinamento giuridico italiano della nozione di documento portò il legislatore (con L. 23.12.1993, n. 547) ad inserire nel codice penale l'art. 491-*bis* rubricato «Documenti informatici». La disposizione estendeva le falsità in atti ai documenti informatici pubblici o privati, disponendo l'applicabilità delle disposizioni del capo III, titolo VII, libro II, c.p. concernenti rispettivamente gli atti pubblici e le scritture private. Nella sua prima formulazione, l'articolo conteneva, in omaggio al principio di determinatezza della fattispecie, una nozione di documento informatico valido ai fini penali: «per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». La norma è stata modificata dall'art. 3 della legge di ratifica della Convenzione di Budapest La nuova formulazione, che si distingue dalla precedente per l'eliminazione della controversa definizione di documento informatico, ha mantenuto inalterata la scelta di fondo del legislatore del 1993 in ordine ad una incriminazione «per rinvio» delle falsità aventi ad oggetto documenti informatici. Da ultimo il D. Lgs. 15 gennaio 2016, n. 7 ha eliminato dalla disposizione il riferimento ai documenti informatici privati e alle disposizioni concernenti le scritture private, in ragione dell'abrogazione del reato di falso in scrittura privata di cui all'art. 485. Per approfondimenti sulle falsità informatiche, v. CORVINO G., La tutela penale del documento informatico, in PLANTAMURA V., MANNA A., *Diritto penale e informatica*, Bari, 2007, 26; GROTTO M., *Regime giuridico del falso informatico dubbi sulla funzione interpretativa dell'art. 491 bis c.p.*, in *Dir. Inf.*, 2006, 589. con L. 23.12.1993, n. 547.
[78] Art. 8-*ter* D.L. 135/2018, convertito con modifiche dalla legge n. 12/2019.

soddisfare il requisito della forma scritta[79]. La novella ha anche esteso, a determinate condizioni, gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 alla registrazione di un documento informatico in *blockchain*. L'aver attribuito alla memorizzazione in registri distribuiti una particolare efficacia probatoria e il valore di marcatura temporale rende evidente come il documento informatico registrato in *blockchain* rientri appieno nel raggio d'azione della tutela penale apprestata dall'art. 491-*bis* c.p.

Si potrebbe tuttavia discutere se la valuta virtuale rientri o meno nella ampia nozione di documento informatico dettata dal CAD. Tecnicamente ciascun *token* viene individuato attraverso una stringa alfanumerica di caratteri che, pur non potendo esprimere un "atto" o un "fatto", può rappresentare un "dato" giuridicamente rilevante. In questa direzione, la idoneità dei dati ad individuare il soggetto legittimato a una prestazione[80] potrebbe confermare la natura documentale dei valori virtuali.

Di diverso avviso è quella parte della dottrina che, condivisibilmente, esclude la riconducibilità alla nozione di documento informatico[81] evidenziando come l'informazione digitale che individua ciascuna unità di criptomoneta non rappresenti un dato, ma sia scambiata valore in sé, fruibile per fini economici o speculativi[82]. L'elemento della rappresentazione può essere diversamente inteso come requisito *interno* o *esterno* al dato informatico: nel primo caso esso contiene l'informazione rilevante, che è almeno in parte traducibile in linguaggio umano, e dunque intellegibile; nel secondo caso l'insieme di *bit* e *byte* è privo di autonomo valore giuridico e non avrebbe alcun significato se non vi fosse una convenzione esterna sul relativo significato. La stringa di codice che compone ciascuna valuta virtuale è priva di significato "umano" e assume un valore giuridico in base alla *communis opinio* sul valore le può essere attribuito[83]; sembra dunque cogliere nel segno la tesi di chi ne disconosce il valore rappresentativo[84].

La questione assume, in ogni caso, un rilievo piuttosto marginale per l'oggetto della presente trattazione, stante il ristretto campo di applicazione delle ipotesi di falsità informatica, ormai circoscritto alle sole falsità in documenti informatici pubblici. Del

[79] A condizione che le parti interessate siano identificate, attraverso un processo avente i requisiti fissati dall'AgID. Il legislatore ha così inteso attribuire alla Autorità amministrativa l'individuazione degli standard tecnici che debbono essere rispettati affinché al contratto possa essere riconosciuta forma scritta.

[80] Si veda BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. Inf.*, 2017, 1, 27 ss.; DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 109.

[81] Cfr. IEMMA P., CUPPINI N., *La Qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, in *Rivista di diritto bancario*, 08 marzo 2018, § 3.1; CAPOGNA A. *et al., Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione*, in *Diritto, mercato e tecnologia*, 2015, 3, 44.

[82] Sembra in effetti piuttosto arduo sostenere che l'insieme di bit sia un dato rappresentativo di qualcosa, specialmente tenuto conto dell'utilizzo della crittografia asimmetrica a doppia chiave per rendere l'informazione inintelleggibile ma verificabile.

[83] La conclusione ci sembra anche in linea con la *ratio* di fondo di tutela del documento informatico, da individuarsi nella trasposizione in logica binaria del linguaggio e della volontà umana.

[84] CAPOGNA *et al., Bitcoin: profili giuridici e comparatistici,* cit., 44

resto, quand'anche si qualificasse la valuta virtuale come documento informatico, pare piuttosto arduo ipotizzare la commissione di un fatto penalmente rilevante[85]. Si potrebbe casomai discutere sulla rilevanza penale delle condotte di falso consistenti nell'alterazione del registro delle transazioni, rese possibili dall'abuso dei meccanismi del consenso o dallo sfruttamento di vulnerabilità nel protocollo di sistema.

A ben vedere, l'oggetto del mendacio non affatto rappresentato dal valore virtuale – come *quid* dotato di autonomo valore giuridico – ma dal libro mastro distribuito, che regola la circolazione e la titolarità dei diritti in *blockchain*. Sarebbe infatti riduttivo riferire la falsità informatica al singolo valore in sé, omettendo di considerare che la sua esistenza, come anche la circolazione, dipende dalla trascrizione sul registro informatico distribuito. Si realizza una sorta di commistione tra il valore e la registrazione[86].

2. Alcuni aspetti definitori delle valute virtuali.

Mettendo da parte la questione relativa alla natura giuridica, l'attenzione andrà ora rivolta alla individuazione di una precisa nozione di valuta virtuale. Ciò permetterà di fare chiarezza su alcuni aspetti definitori che, per la successiva analisi dei reati configurabili, appaiono di fondamentale importanza.

Si suol dire che la criptomoneta appartiene alla categoria delle valute virtuali a c.d. *flusso bidirezionale*, poiché, una volta acquistata è riconvertibile in *fiat currency*. L'affermazione, piuttosto ricorrente in dottrina[87], richiama la tripartizione effettuata dalla Banca Centrale Europea[88]. Alla prima categoria appartengono le valute *a schema chiuso* che non possiedono alcun legame con l'economia reale perché totalmente "autoreferenziali" e destinate ad essere utilizzate unicamente su piattaforme di *gaming online* (es. acquisto di abbonamenti a giochi di ruolo o equipaggiamenti fantasy)[89]. La seconda categoria è occupata dalle valute *a flusso unidirezionale*, che, acquistate per moneta reale ad un tasso di scambio predefinito, non possono tuttavia essere riconvertite (es. i crediti *Facebook*). Le monete virtuali *a flusso bidirezionale* si caratterizzano invece per la possibilità di compravendita e cambio per valuta reale, e

[85] La 'materiale' falsificazione della stringa alfanumerica è resa estremamente difficoltosa dall'utilizzo di complessi algoritmi crittografici, mentre la falsità ideologica è esclusa *a priori* dall'assenza di un contenuto rappresentativo di atti o fatti giuridicamente rilevanti.

[86] L'utente, a stretto rigore, non dispone del dato informatico trascritto in *blockchain*, ma soltanto delle chiavi crittografiche che gli permettono di disporne. Sicché, ogni eventuale alterazione dell'informazione digitale non potrà che avere ad oggetto il *public ledger*.

[87] *Ex multis* v. ROSEMBUJ, *Bitcoin*, *cit*., 62; VARDI, *"Criptovalute" e dintorni, cit.,* 444.

[88] Si richiama il documento denominato *Virtual Currency Schemes*, disponibile sul sito internet istituzionale https://www.ecb.europa.eu

[8989] Alcuni autori la definiscono anche moneta virtuale "pura" giacché non ha interazioni con l'economia reale, non essendo possibile né acquistare beni o servizi reali, né riconvertirla in moneta fiat. Essa può essere acquistata e spesa solo all'interno di una comunità virtuale (in genere quelle dei *Multi-Media On-line Game*). Sul punto DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 98.

viceversa, senza alcun limite[90]; a differenza delle precedenti aprono un portale di comunicazione con il mondo dell'economia reale, sollevando interrogativi di non poco conto sul piano legale.

All'interno di quest'ultima categoria possono individuarsi ulteriori distinzioni. Si definiscono *valute centralizzate* quelle create e controllate da un emittente privato; *valute decentralizzate* quelle generate in modo diffuso dagli utenti che compongono l'infrastruttura distribuita[91]. Quale che sia la formula di emissione e la tipologia di *blockchain* utilizzata, gli utenti possono acquistare tali valute con moneta tradizionale su una piattaforma di scambio ovvero riceverle al proprio indirizzo di conto. Solitamente la criptomoneta, *rectius* le chiavi crittografiche di spendita, sono conservate in un portafoglio digitale utilizzato per effettuare acquisti o rimesse in favore di terzi. I fornitori di servizi di cambio e di deposito rivestono dunque un ruolo fondamentale per la fruizione dei nuovi valori, poiché alimentano il dinamismo in settore che, altrimenti, sarebbe statico e ristretto a una cerchia di pochi esperti[92].

L'attività svolta da questi soggetti sarà compiutamente esaminata nei paragrafi successivi, allorché passeremo all'esame delle novità introdotte dal D. Lgs. 90/2017; sarà invece opportuno dar conto ora dello stato dell'arte precedente all'intervento del legislatore, caratterizzato da una diffusa diffidenza nei confronti delle applicazioni economico-finanziarie della *blockchain.*

2.1. I primi tentativi di 'messa a fuoco' del fenomeno. La posizione delle autorità bancarie e finanziarie tra scetticismi e dubbi interpretativi.

Le applicazioni finanziarie della *blockchain* sono entrate "di forza" negli ordinamenti nazionali, rivoluzionando alcuni settori di primario interesse per l'economia interna: il finanziamento delle imprese, il mercato dei titoli e quello degli scambi. In assenza di una regolazione a livello internazionale e nella consapevolezza dei rischi connessi alla perdita del controllo statuale della *distributed economy*, l'approccio delle istituzioni pubbliche non poteva che essere cauto.

Alcuni legislatori per il timore di soffocare l'innovazione[93] hanno preferito monitorare in via precauzionale il fenomeno, anziché regolarlo preventivamente; altri

[90] In questi termini il rapporto della BCE: «*This virtual currency is similar to any other convertible currency with regard to its interoperability with the real world. These schemes allow for the purchase of both virtual and real goods and services*».

[91] Sulla distinzione tra *blockchain* pubbliche e private, con particolare riguardo alle diverse dinamiche di creazione dei valori virtuali si veda *supra* Cap. I, § 2.2.

[92] I servizi di cambio di moneta virtuale per moneta reale hanno accresciuto la tendenza alla speculazione; non è infatti un caso che la crescita del coefficiente di capitalizzazione del mercato sia stata accompagnata dall'apertura di nuove piattaforme di *trading*.

[93] Il riferimento è al *caveat* espresso dalla Commissione Europea nella Proposta di Direttiva 2016/0208 di modifica della quarta direttiva antiriciclaggio. Si afferma espressamente che la distribuzione della moneta digitale offre vantaggi potenziali in termini di efficienza, proprio perché, a differenza delle operazioni in contanti, si fonda su un registro pubblico di annotazione continua dei trasferimenti. Così si legge a pagina 14 della Proposta *«La misura proposta prende in considerazione il potenziale del*

hanno invece posto le basi normative affinché gli investitori scegliessero *à la càrte* il proprio ordinamento, in quanto più permissivo[94]. L'Unione Europea ha seguito la prima linea di azione, intervenendo con atti normativi vincolanti soltanto in tempi recenti, all'esito di un lungo periodo di osservazione, per contenere il rischio di un impiego sistematico del sistema finanziario (virtuale) a scopo di riciclaggio e finanziamento del terrorismo. Per quanto l'approccio liberista del legislatore europeo possa giustificarsi per via degli effetti positivi della nuova tecnologia sui mercati finanziari, non sono mancate opinioni di segno contrario sulla prevalente necessità di regolamentare in fenomeno in modo rigoroso, al fine di tutelare gli interessi dei risparmiatori e l'integrità finanziaria dell'Unione nel suo complesso.

Tra le posizioni maggiormente critiche vi è quella delle istituzioni bancarie[95] che, fin dai periodi di prima espansione del fenomeno, segnalavano l'opportunità di individuare delle misure di *mitigation* degli innumerevoli rischi posti dal mercato valutario virtuale[96].

Non potendosi qui dar conto, men che meno in modo esaustivo, delle criticità individuate dalle Autorità di settore, basti ricordare che la EBA elenca ben settanta rischi specifici[97]. Una attenzione particolare è rivolta alle implicazioni sul sistema macroeconomico nel suo complesso: le *virtual currencies* potrebbero destabilizzare l'integrità finanziaria dell'Unione, incentivando il finanziamento del terrorismo e nuove forme di riciclaggio, erodendo il controllo pubblico sui sistemi elettronici di pagamento ed eludendo l'attività delle Autorità pubbliche di vigilanza. Per far fronte a tali rischi la EBA ha ritenuto necessario un *«immediate and consistent regulatory response across the EU»*[98] per disciplinare in modo adeguato le attività di scambio, vendita e trasferimento di valori virtuali. È curioso osservare come nel documento si fornisca una definizione di valute virtuali analoga a quella recepita dal legislatore con l'emanazione della direttiva 2018/843/UE[99]. Similmente, anche la Banca centrale

mercato delle valute virtuali in termini di innovazione delle modalità di interazione tra governi e cittadini per quanto riguarda la condivisione dei dati, la trasparenza e la fiducia, nonché in termini di nuovi spunti per la definizione della titolarità e della provenienza dei beni e della proprietà intellettuale».

[94] Si vedano, ad es., le recenti esperienze regolatorie di Malta, Svizzera, San Marino.

[95] Cfr. il Rapporto della *European Banking Authority* (EBA), *«Warning to consumers on virtual currencies»,* 12 dicembre 2013, nonché la *Opinion on virtual currencies*, 04 luglio 2014, più volte citati.

[96] Esso, infatti, non solo fa venir meno la necessità dell'intermediazione di soggetti terzi nelle transazioni tra privati, ma, vieppiù, minimizza l'ingerenza dello Stato sul mercato della moneta e, in generale, nella gestione dei sistemi digitali di pagamento.

[97] La tassonomia dei rischi viene ordinata in macro-categorie, sistemate in una tabella sinottica (pag. 22 del Report). Partendo da rischi per gli utenti (distinti a seconda che le valute virtuali siano utilizzate come strumento di pagamento ovvero di investimento) e quelli a carico dei professionisti e delle imprese, il documento individua oltre trenta minacce per il sistema economico nel suo complesso, che incombono, in particolare, sull'integrità finanziaria, sui sistemi di pagamento in valuta corrente, e sulle Autorità pubbliche di vigilanza.

[98] v. *Opinion on virtual currencies*, cit., 45.

[99] La EBA definisce le valute virtuali come *«a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically»* (Cfr. *Opinion on virtual currencies*, cit., 11).

europea ha identificato il circolante virtuale come una rappresentazione digitale del valore che, in alcune circostanze, può essere utilizzato come alternativa al denaro[100], salvo poi specificare – nel parere sulla bozza di direttiva antiriciclaggio – che la definizione dovrebbe far leva non solo sul requisito della accettazione come mezzo di scambio o per altri scopi, ma anche sul dato della trasferibilità e archiviazione elettronica[101].

Per quanto vi fosse in seno alle istituzioni europee una tacita concordia sulla nozione di valuta virtuale, la mancanza di una definizione legislativa aveva dato luogo non poche incertezze sull'applicazione degli atti normativi dell'Unione in materia strumenti di pagamento e di investimento (normative EMD e MiFID) e sulla tassazione indiretta (direttiva VAT). Ben presto alcune questioni furono sottoposte al vaglio della Corte di Giustizia UE. Un esempio paradigmatico fu la sentenza *Skatteverket c. David Hedqvist* relativo alla imponibilità ai fini IVA delle operazioni di cambio di valute virtuali, questione risolta dal Collegio in senso negativo[102]; sulla pronuncia si tornerà nella parte dedicata agli illeciti fiscali[103].

In tempi più recenti la Commissione ha elaborato un *Fintech Action Plan* con l'intento di accrescere la sensibilità del settore finanziario dell'UE verso le opportunità offerte dalle nuove tecnologie[104]. Trattandosi di un tema strettamente connesso alla dimensione finanziaria della *blockchain* è opportuno anche qui riservarne l'esame al prosieguo della trattazione[105].

Rivolgendo ora lo sguardo al panorama nazionale, si rinviene un certo disorientamento nella qualificazione giuridica delle operazioni aventi ad oggetto gli *asset* virtuali. La tendenza è quella di non considerare l'*ubi consistam* delle valute virtuali – vale a dire le loro particolari caratteristiche ontologiche – bensì la funzione socio-economica ad esse sottesa. Ne consegue una visione tutt'altro che unitaria del fenomeno, che assume contorni talvolta poliedrici o addirittura ibridi, in base ai principi che regolano ciascuna materia.

La Consob, ad esempio, ha ritenuto che i valori virtuali, a determinate condizioni, debbano essere inquadrati come prodotti finanziari e sottoposti alla relativa

---

[100] Cfr. *Virtual currency schemes – a further analysis*, cit., 25 secondo cui *«for the purpose of this report, and based on the characteristics currently observed, virtual currency can therefore be defined as a 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»*.

[101] In questo senso la *Opinion of the European Central Bank of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849*, 2016, 6-7.

[102] CGUE, Sez. V., sent. 22 ottobre 2015, Skatteverket c. David Hedqvist, causa C-264/14. La Corte inquadra il cambio di valuta virtuale tra le operazioni esenti rilevando che *«le operazioni relative a valute non tradizionali, vale a dire 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»*.

[103] V. *infra*, § 6.1.

[104] Il riferimento è al piano della Commissione Europea denominato '*The FinTech action plan'*, in https://ec.europa.eu

[105] Si veda in particolare il Cap. IV, § 1.2.

disciplina[106]. Di recente l'Autorità ha aperto un tavolo di discussione per proporre i lineamenti della futura regolazione del fenomeno delle ICO e del *trading* di valori virtuali, ribadendo come la qualificazione giuridica delle operazioni non possa essere astratta dal caso concreto[107].

In materia di offerta di valori virtuali è intervenuta anche la Banca d'Italia che ha evidenziato i rischi connessi all'utilizzo delle stesse, condividendo gli orientamenti delle autorità bancarie europee pocanzi richiamati[108]. L'Autorità nega alle criptovalute la qualificazione di moneta legale o elettronica, soffermandosi sulla loro funzione eminentemente speculativa ed evidenziando come l'assenza di un quadro legale certo circa la natura giuridica delle valute virtuali nonché una sottovalutazione dei rischi insiti nelle stesse può concretizzarsi nell'erosione del patrimonio di vigilanza e della stabilità stessa degli intermediari finanziari[109].

Quanto agli aspetti fiscali, la sentenza della Corte di Giustizia ha indotto l'Agenzia delle Entrate a ritenere che alle operazioni di cambio valuta si applichi il regime di esenzione di cui all'art. 10, comma 1, n. 3), del D.P.R. 26 ottobre 1972, n. 633[110]; il valore pseudo valutario dell'operazione non vale tuttavia a sottrarre le plusvalenze di investimento alla tassazione dei redditi di capitali o di altra natura. In assenza di indicazioni normative la qualificazione giuridica appare anche qui incerta e per molti versi fumosa, tanto da rendere opportuno un intervento del legislatore.

2.2. La definizione di valuta virtuale nell'attuale quadro normativo.

Con l'emanazione del D. Lgs. 25 maggio 2017 n. 90[111] il legislatore italiano ha esteso la disciplina preventiva del riciclaggio alle operazioni realizzate tramite cambio

---

[106] In alcune delibere l'Autorità ha ravvisato nell'offerta al pubblico di "portafogli di investimento" in cripto-valute con rendimenti mensili gli estremi di un'offerta al pubblico di prodotti finanziari, definita nell'art. 1, comma 1, lett. t), del TUF. Cfr. Delibera Consob del 06/12/2017, n. 20207; Delibera Consob del 20/04/2017, n. 19968, entrambe su https://consob.it. Sul punto, si veda CONSO A., DI GIORGIO A., MARTINOTTI L., *Un caso recente: divieto di offerta al pubblico di "portafogli di investimento" in criptovalute*", in *Rivista di diritto bancario*, 29 ottobre 2018.

[107] Si veda il Documento per la discussione denominato *'Le offerte iniziali e gli scambi di criptoattività'*, 19 marzo 2019, in https://consob.it (*infra*, Cap. IV, § 2.2.).

[108] La Banca d'Italia evidenzia i rischi e scoraggia l'acquisto di criptovalute motivato da aspettative di investimento. Cfr. *Rapporto sulla stabilità finanziaria*, 2018, 1, in https://bancaditalia.it, nel quale osserva che «*sebbene distributed ledger technology possa portare benefici all'economia, le criptoattività comportano numerosi rischi, in primo luogo per gli investitori che possono incorrere in perdite rilevanti. Tali rischi potrebbero avere implicazioni per la stabilità del sistema finanziario qualora la dimensione del mercato delle criptoattività diventasse significativa o gli intermediari finanziari acquisissero esposizioni verso queste attività, che li esporrebbero anche a rischi reputazionali*» (così pagina 9).

[109] In tal senso si veda anche la celebre *Avvertenza sull'utilizzo delle cosiddette "valute virtuali"* del 30 gennaio 2015 e la *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee* del 19 marzo 2018, entrambe disponibili su sito Internet indicato nella nota precedente.

[110] Si richiama la posizione espressa nella Risoluzione n. 72/ del 2 settembre 2016 e la Risposta n. 14 all'interpello n. 956-39/2018, sulle quali *amplius* v. § 6.2.

[111] Il decreto delegato, adottato in base alla legge 12 agosto 2016 n. 170, intitolato «*Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive*

e trasferimento di valute virtuali. La novella ha infatti modificato le definizioni contenute nel D. Lgs. 21 novembre 2007 n. 231 inserendovi una specifica definizione di valuta virtuale e di prestatore di servizi relativi all'utilizzo di valuta virtuale. Nella relazione governativa[112] si richiama l'attenzione sul fatto che la Commissione europea avesse presentato una proposta di direttiva per estendere il campo di applicazione della direttiva (UE) 2015/849 alle piattaforme di cambio e ai prestatori di servizi di portafoglio digitale; si comprende dunque che l'intento del Governo sia stato quello di "giocare" d'anticipo rispetto al legislatore dell'Unione, approfittando della delega per aggiornare i presidi antiriciclaggio ai rischi derivanti dalla nuova dimensione virtuale dell'economia[113].

Le novità introdotte dal decreto sull'attività degli intermediari (*exchange* e *wallet provider*) saranno debitamente approfondite nelle sedi opportune[114]; si dovrà ora concentrare l'attenzione sulla nozione di valuta virtuale che il legislatore delegato definisce in questi termini: *«la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente»* (art. 1, comma 2, del D. Lgs. 21 novembre 2007 n. 231 lett. qq). La definizione è per molti versi analoga a quella contenuta nell'art. 1, par. 1, lett. c) della Proposta di Direttiva[115], dalla quale differisce soltanto per alcuni adeguamenti stilistici e lessicali[116].

Dal testo della definizione emerge piuttosto chiaramente la *voluntas legis* di distinguere la valuta virtuale da quella moneta avente corso legale, così da sopire il dibattito sulla natura giuridica della criptomoneta. Non è tuttavia chiaro cosa debba intendersi per *rappresentazione di valore*, inciso che per certi versi risulta impreciso. Si è infatti detto che la valuta digitale potrebbe non essere rappresentativa di alcunché: il più delle volte essa viene scambiata sulla base di un rapporto fiduciario al prezzo

---

2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847» è entrato in vigore il 04 luglio 2017. Il decreto sostanzialmente riscrive il D. Lgs. n. 231 del 2007 (attuativo della precedente direttiva antiriciclaggio), introducendo diverse innovazioni che riguardano i soggetti destinatari degli obblighi) poteri delle UIF (Unità di informazioni finanziarie nazionali) e la collaborazione tra esse.

[112] Si richiama il dossier denominato *Prevenzione dell'uso del riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo* marzo 2017, Atto del Governo n. 389, in https://senato.it

[113] In dottrina sul tema, ACCINNI G.P., *Profili di rilevanza penale delle "criptovalute*", in *Arch. Pen*., 2018, 1, 4 ss.; DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 123; 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*, 2018, 1, 3.

[114] Sul regime autorizzatorio per l'esercizio dell'attività e le relative sanzioni si rinvia al capitolo successivo (Cap. IV, § 3.1.); sugli obblighi antiriciclaggio e connessi profili sanzionatori v. in questo capitolo § 3.1. ss.

[115] La Commissione definiva la «una rappresentazione di valore digitale che non è né emessa da una banca centrale o da un ente pubblico né è necessariamente legata a una valuta legale, ma è accettata da persone fisiche e giuridiche come mezzo di pagamento e può essere trasferita, memorizzata o scambiata elettronicamente» (art. 1, lett. c della Proposta).

[116] L'unica differenza degna di nota sta nel requisito oggettivo dell'utilizzo come "mezzo di scambio", che non figura nella definizione contenuta nella Proposta (nella quale si fa riferimento al concetto, soltanto in parte sovrapponibile, di "accettazione come mezzo di pagamento").

determinato dal mercato. A differenza delle valute *fiat*, che – almeno formalmente – rappresentano un credito nei confronti dello Stato emittente, la criptomoneta potrebbe non racchiudere in sé alcun rapporto giuridico[117]. Il valore cui si fa riferimento non è certamente quello "monetario memorizzato elettronicamente" di cui all'art. 1, comma 2, lett. *h-ter)* TUB, per l'ovvia ragione che l'emissione di quest'ultimo è sottoposto al controllo pubblico e riservato agli intermediari autorizzati.

Altrettanto enigmatico il richiamo a un collegamento con la valuta avente corso legale che, secondo la disposizione in commento, potrebbe anche non essere necessario. Il valore nominale della criptomoneta è dato da un insieme di fattori che solitamente non dipendono dal prezzo di cambio delle valute *fiat.* Potrebbe anche darsi che le oscillazioni del prezzo delle seconde incidano sul valore della prima, in quanto prodotto 'derivato' della conversione del denaro; si tratterebbe comunque di un effetto fisiologico, che investe più in generale ogni bene o servizio acquistabile con il denaro. Si ritiene che, con tale inciso, il legislatore abbia voluto includere nel perimetro della disposizione anche quelle valute virtuali originariamente concepite come circolante complementare, il cui prezzo di scambio è vincolato al prezzo nominale di scambio delle valute legali "forti"[118].

Quanto all'elemento della fruibilità come mezzo di scambio per l'acquisto di beni e servizi, pare che il legislatore abbia voluto mettere in particolare evidenza la funzione *lato sensu* monetaria delle valute virtuali. La scelta non è del tutto condivisibile, dal momento che tale utilizzo è decisamente recessivo rispetto alla compravendita per (prevalenti) finalità speculative. Vi è dunque il rischio che la maggior parte dei valori virtuali non rientri nella nozione in esame[119], nonostante abbia larga diffusione e sia liberamente scambiabile sulle piattaforme di *trading*. Sul piano interpretativo si pone dunque una alternativa: o ritenere che il legislatore abbia circoscritto il campo di applicazione della normativa antiriciclaggio alle sole valute virtuali attivamente utilizzate come *medium* negli scambi; ovvero credere che *lex minus dixit quam voluit*. Questa seconda ipotesi sembra più in linea con la *ratio* di fondo della riforma, essendo decisamente irragionevole escludere dal raggio di applicazione del D. Lgs. 231/2007 quelle operazioni in unità di conto virtuale prive di 'potere di acquisto'. Alla ristrettezza della definizione nazionale non ha posto rimedio il legislatore europeo con

[117] Si tratta dei *token* definiti di prima classe con funzione meramente rappresentativa della titolarità del *token* stesso. Nel dettaglio, rientrano in questa categoria tutte le criptovalute che costituiscono unità di registrazione e rappresentazione di valori scambiabili tra soggetti diversi (ad es. Bitcoin, Ripple, Litecoin). In argomento, SARZANA DI S. IPPOLITO F. – NICOTRA M., *Diritto della blockchain, intelligenza artificiale e IoT*, Vicenza, 2018, 21 ss.

[118][118] Si pensi, ad esempio, alla valuta Tether (USDT), quotata nelle più importanti piattaforme di scambio, il cui valore è stabilmente legato al prezzo di scambio del dollaro statunitense.

[119][119] Sono decisamente pochi i valori virtuali accettati come mezzo di scambio (es. Bitcoin, Ethereum, Litecoin, Ripple e, sul *darknet*, Monero).

l'emanazione della direttiva 2018/843/UE, benché al riguardo fossero stati proposti alcuni emendamenti[120].

La nozione introdotta in sede comunitaria[121] non presenta differenze sostanziali, distinguendosi da quella nazionale soltanto per la lapidaria previsione che la valuta virtuale non possiede lo *status* giuridico di valuta o moneta.

2.3. Conclusioni sulla definizione di valuta virtuale.

A nostro avviso ambedue le definizioni, chiaramente ispirate a quella inizialmente delineata dalla EBA[122], peccano di incompletezza; il legislatore avrebbe dovuto concentrare il *focus* definitorio non tanto (o non soltanto) sulle differenze ontologiche con la moneta legale, ma ampliare l'orizzonte a tutti i possibili utilizzi dei *token* virtuali, così da evitare possibili resistenze all'applicazione della normativa antiriciclaggio. Per quanto poco convincente, la nozione in commento è attualmente l'unico referente normativo in grado di orientare l'interprete nel nebuloso universo dei valori virtuali. Sembra dunque verosimile che le disposizioni definitorie entreranno nel dizionario giuridico comune, forse anche con scarsa consapevolezza delle diverse imperfezioni che la connotano.

Una possibile soluzione alternativa potrebbe essere quella di definire le valute virtuali come l'«informazione digitale, non necessariamente legata alla rappresentazione di valore monetario ma suscettibile di valutazione economica, utilizzata da persone fisiche e giuridiche come mezzo di scambio o strumento di investimento, anche di natura non finanziaria».

Questa nozione permetterebbe anzitutto di qualificare la valuta virtuale per quello che è, ossia una informazione digitale. Pur non possedendo un valore intrinseco o un rapporto giuridico sottostante (credito, diritto reale etc.), essa viene scambiata sul mercato come mezzo di pagamento o riserva di valore su basi puramente fiduciarie[123]. Il riferimento allo strumento di investimento fa rientrare nella nozione anche gli impieghi del contante virtuale per fini speculativi, sebbene allo stesso non vada sempre riconosciuta natura finanziaria[124] secondo la definizione maggiormente condivisa. Il

[120] Nel testo della proposta di direttiva del 09 marzo 2017 è contenuto un emendamento all'art. 1, par. 1, lett. c) per cui la valuta virtuale è utilizzata come «mezzo di scambio, ed eventualmente per altri fini»; le parole dopo la virgola sono tuttavia state espunte in sede di approvazione del testo definitivo.

[121] Nella elencazione dell'art. 3 della direttiva (UE) 2015/849 è stata inserita la definizione di valuta virtuale intesa come la *«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».*

[122] Cfr. European Banking Authority, *Opinion on virtual currencies*, cit., 11 (v. *supra*).

[123] La dottrina ha osservato che il *pactum fiduciae* tra utenti si basa sulla stabilità e sulla legittimità del protocollo informatico che governa la catena dei blocchi. La fiducia sarebbe minata alle fondamenta se l'infrastruttura fosse utilizzata prevalentemente o esclusivamente per scopi criminosi. Cfr. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta,* cit., 5.

[124] Secondo la Consob (Cfr. *Le offerte iniziali e gli scambi di criptoattività,* cit., 7 ss.) gli investimenti di natura finanziaria sono quelli che implichino la compresenza dei seguenti elementi: (i) impiego di

perimetro della nostra definizione comprende tutti i valori circolanti sul mercato valutario, che, interpretando fedelmente la lettera della legge, non potrebbero oggi qualificarsi come valute virtuali.

3. Il riciclaggio dei proventi delittuosi nell'era della *distributed economy*.

Esaminate in generale la natura e le funzioni della moneta virtuale, occorre ora rivolgere l'attenzione ai possibili ambiti di rilevanza penale connessi al suo utilizzo. Si tratterà nello specifico di individuare quali siano le fattispecie di reato maggiormente interessate dalle applicazioni economico-finanziarie della *blockchain.*

Il mercato delle valute virtuali sviluppa la maggior parte del proprio volume d'affari grazie alla prestazione di servizi di cambio di moneta virtuale per moneta reale, e viceversa. Sono queste attività esposte ad un elevato rischio di strumentazione per fini di riciclaggio, a causa dell'elevato potenziale della criptomoneta di disperdere le tracce della provenienza delle somme e di mantenere l'anonimato dei soggetti coinvolti[125]. La scelta di trattare per primi i profili connessi al riciclaggio ben si giustifica non solo per la drastica incidenza del fenomeno sul circuito dell'economia lecita[126], ma tanto più perché in quest'ambito si registrano le più importanti novità normative.

In apertura di questo capitolo abbiamo precisato come talvolta i valori virtuali possano considerarsi *strumento del reato*, quando la condotta delittuosa si realizza per il tramite di essi. Un esempio paradigmatico è dato proprio dall'utilizzo della criptomoneta come "denaro-ponte" in grado di interrompere la tracciabilità dei flussi di denaro, figura riconducibile al *riciclaggio digitale strumentale*. Partendo dalla definizione fornita dalla Convenzione di Strasburgo[127] (art. 1, lett. a e b) la dottrina[128] considera provento riciclabile ogni vantaggio economico derivante da reato, con esclusione comunque dei beni usati per commettere il reato, non essendo proventi, bensì strumenti del reato (art. 1, lett. c). Ecco dunque che, nel complesso *iter criminis* che caratterizza il lavaggio dei capitali di provenienza illecita, le valute virtuali avranno

---

capitale; (ii) promessa/aspettativa di rendimento di natura finanziaria, intendendosi per tale l'accrescimento della disponibilità investita, senza l'apporto di prestazioni da parte dell'investitore; (iii) assunzione di un rischio direttamente connesso e correlato all'impiego di capitale; (iv) prevalenza del connotato finanziario rispetto a quello di godere e disporre del bene acquisito con l'operazione; (v) effettiva e predeterminata promessa, all'atto dell'instaurazione del rapporto contrattuale, di un rendimento collegato alla *res.*

[125] Per approfondimenti v. *supra*, Cap. II, § 1.

[126] Secondo alcune stime recenti in Italia il riciclaggio dei proventi illeciti produrrebbe 410 milioni di euro ogni giorno, 17 milioni l'ora, 285 mila euro al minuto, 4.750 euro al secondo. Sul punto si veda GRASSO P., BELLAVIA E., *Soldi sporchi. Come le mafie riciclano miliardi e inquinano l'economia mondiale*, Milano, 2011.

[127] Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato, fatta a Strasburgo l'8 novembre 1990, ratificata e resa esecutiva in Italia con legge 9 agosto 1993, n. 328. La legge di ratifica ha, come noto, ampliato il catalogo dei delitti presupposto aperto a tutti i delitti non colposi.

[128] ZANCHETTI M., *Il riciclaggio di denaro proveniente da reato*, Milano, 1997, 328 ss.

un ruolo differente (oggetto della condotta o strumento del reato) a seconda della necessità o meno del piazzamento (*placement*) della ricchezza e di una successiva fase di *integration* nel passaggio tra la moneta reale e quella virtuale.

La dottrina che più di recente si è occupata del tema del riciclaggio mette in luce come il legame tra ripulitura del denaro e nuove tecnologie sia divenuto sempre più stretto[129]. Le preoccupazioni maggiori derivano proprio dalla diffusione del circolante virtuale: il "genetico anonimato"[130] offerto dalla criptomoneta, unito al diffondersi di servizi di *mixing* e alla possibilità di effettuare transazioni rapide ed irreversibili a livello transnazionale, darebbe luogo a un vero e proprio *"cyber-heaven"*[131] non solo per il crimine organizzato, ma anche per piccoli gruppi criminali alla ricerca di un *locus amoenus* per realizzare operazioni di lavaggio dei proventi delittuosi[132]. Le tecnologie della comunicazione e dell'informazione hanno permesso di superare uno dei più grandi ostacoli al riciclaggio, ovvero la movimentazione fisica di grosse quantità di denaro[133]. Quando il provento delittuoso è disponibile *ab origine* in forma elettronica l'operazione di ripulitura avviene in tempi brevi, con maggiori possibilità di sfuggire al sistema di controlli statali. La diffusione su scala mondiale della moneta *peer-to-peer* ha reso ancor più arduo il contrasto al fenomeno, poiché rischia di eludere il presidio più efficace, rappresentato dalla previsione di obblighi di segnalazione a carico degli intermediari autorizzati. Per questo motivo la Commissione Europea aveva espresso la propria preoccupazione per la progressiva affermazione di nuovi strumenti in grado di agevolare il lavaggio del denaro sporco[134], sottolineando la necessità di un rapido intervento del legislatore.

Prima di passare all'esame dei profili concernenti le valute virtuali, sarà bene ripercorrere cursoriamente lo stato dell'arte sul fenomeno del *cyberlaundering*. Per una ordinata trattazione del tema si ricorrerà alla distinzione, ormai nota, tra disciplina preventiva e repressiva, analizzando le questioni più rilevanti relative a ciascuna di esse.

---

[129] PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2018, 3-4, 591

[130] ACCINNI, *Profili di rilevanza penale delle "criptovalute*", cit., 8

[131] Un "paradiso virtuale", metafora probabilmente riferita ai "tax-heavens" del diritto tributario. In questi termini SIMONCINI E., *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, in *Riv. Trim. Dir. Pen. Econ*., 2015, 4, 907, il quale osserva che «*la crescente evoluzione dei sistemi informatici e delle nuove tecnologie ha consentito al crimine organizzato di infiltrarsi e inquinare uno dei luoghi considerati il vero «cuore pulsante» degli affari e della vita economica mondiale, ossia Internet*».

[132] Per un approfondimento sulle recenti tendenze della criminalità economica in rete, con particolare riguardo all'utilizzo delle valute virtuali si rinvia alle statistiche pubblicate da Europol negli ultimi Internet Organised Crime Threat Assessment (IOCTA), disponibili su https://europol.europa.eu.

[133] Basti pensare ai servizi di *money transfer* internazionale e alle carte prepagate, alla possibilità di usufruire dell'home banking per acquisti e/o scommesse *online*. Cfr. SIMONCINI, *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, cit., 899.

[134] Nella proposta di direttiva per la modifica della c.d. quarta direttiva sul riciclaggio si faceva presente come le valute virtuali fossero lo strumento più efficace nelle mani dei cybercriminali (cfr. pag. 14 della Proposta).

3.1. Riciclaggio (art. 648-*bis* c.p.) e *cyberlaundering.*

A dispetto della sua collocazione sistematica, l'attuale struttura del reato di riciclaggio (art. 648-*bis* c.p.)[135] evidenzia come l'incriminazione sia posta a salvaguardia di interessi pubblici superindividuali[136], in particolare quello dell'amministrazione della giustizia. Nel capitolo precedente si è fatto cenno ad alcuni elementi della fattispecie, in particolare al momento consumativo e alla natura del reato[137]; a scioglimento della riserva formulata in quella sede, dovremo ora esaminare, sia pur sinteticamente, la struttura dell'incriminazione.

Gli interventi legislativi succedutisi nel tempo hanno reso il riciclaggio un reato forma libera; al di là dell'ampliamento del novero dei reati presupposto, la legge 09 agosto 1993, n. 328 ha inserito un generico riferimento al compimento di *«altre operazioni»,* che estende il raggio d'azione della disposizione a tutte le condotte potenzialmente dissimulatorie. In dottrina prevale la tesi della natura di pericolo concreto[138] del riciclaggio: rientrano nel focus dell'incriminazione tutte le condotte idonee ad ostacolare l'identificazione della provenienza delittuosa del denaro, dei beni, e delle altre utilità.

Si suole tradizionalmente suddividere l*'iter* di ripulitura del denaro in tre fasi successive, indicate con i termini anglosassoni *placement, layering, integration*[139]. La prima fase si caratterizza per il "piazzamento" dei proventi delittuosi nel circuito dell'economia legale, attività che, fino a qualche tempo fa, richiedeva la movimentazione consistenti flussi di denaro *cash*. I limiti imposti all'utilizzo del denaro contante da un lato, e la digitalizzazione dei mezzi di pagamento dall'altro, rendono quasi inevitabile il passaggio del denaro per istituti di credito o intermediari

---

[135] La legge 9 agosto 1993, n. 328 di ratifica della Convenzione di Strasburgo sul riciclaggio ha riformulato l'art. 648-*bis* c.p., ampliando il catalogo dei reati presupposto a tutti i delitti non colposi. L'attuale formulazione punisce chi «*fuori dei casi di concorso nel reato […] sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa*».

[136] Nella manualistica v. ANTOLISEI F., *Manuale di diritto penale. Parte speciale*, Vol. II, Milano, 2016, 463; MANTOVANI F., *Diritto penale – Parte speciale*, Vol. II, Padova, 2018, 289 ss.; MEZZETTI E., *Reati contro il patrimonio*, Milano, 2013, p. 653 ss.; FIANDACA G.- MUSCO E., *Diritto penale. Parte speciale, II, I delitti contro il patrimonio*, Bologna, 2015, 247. In letteratura, senza pretese di esaustività, MANNA A., *Il bene giuridico tutelato nei delitti di riciclaggio e reimpiego: dal patrimonio all'amministrazione della giustizia, sino all'ordine pubblico ed all'ordine economico*, in ID. (a cura di), *Riciclaggio e reati connessi all'intermediazione mobiliare*, Torino, 2000, 53; COLOMBO G., *Il riciclaggio*, Milano, 1990; FLICK G. M., *La repressione del riciclaggio ed il controllo della intermediazione finanziaria. Problemi attuali e prospettive*, in *Riv. it. dir. proc. pen*. 1990, 1264 ss.; MANES V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, in *Riv. trim. dir. pen. econ*., 2004, 1-2, 39 ss.; ZANCHETTI M., *Art. 648 bis c. p.,* in CRESPI A.– FORTI G.– ZUCCALÀ G., *Commentario breve al codice penale*, Padova, 2008, 1939 ss.

[137] Ne avevamo fatto cenno a proposito della questione relativa alla omessa convalida della transazione, alle regole del consenso e alla caducazione del blocco (v. *supra*, Cap. II, § 2.3.).

[138] ZANCHETTI, *Art. 648- ter c.p.*, cit., 2297; MEZZETTI, *Reati contro il patrimonio*, cit., 653.

[139] Alcuni studi recenti si sono tuttavia interrogati sulla attuale tenuta di questo schema tipico, che molti versi potrebbe sembrare obsoleto alla luce degli sviluppi più recenti. Cfr. CASSELLA S. D., *Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete?,* in *Journal of Money Laundering Control,* Vol. 21, 4, 494 ss.

finanziari. Per eludere il sistema dei controlli preventivi[140], l'agente dovrà operare per interposta persona, servendosi della collaborazione di soggetti intranei all'intermediario finanziario.

La fase di *layering* è caratterizzata dal compimento di una serie (più o meno articolata) di operazioni finalizzata ad impedire la ricostruzione della traccia documentale (*paper trial*) o digitale (*digital trial*) che collega il provento ripulito al delitto dal quale origina.

Il ciclo si chiude con il consolidamento della ricchezza nelle mani del reo (*integration*): il capitale ritorna nella disponibilità dell'autore del reato presupposto – in forma liquida, pronto per essere reimpiegato nell'economia legale – al netto degli importi corrisposti ai concorrenti come compenso per l'attività prestata.

Date queste premesse sullo schema tipico del riciclaggio, occorre esaminare nel dettaglio in che modo le nuove tecnologie intervengano nelle diverse fasi del processo.

Il *cyberlaundering* rappresenta la nuova frontiera del *money laundering* e consiste nella "polverizzazione" [141] dei contanti via Internet; secondo alcuni autori esso rappresenta una delle forme di manifestazione del *cybercrime*[142] inteso in senso lato[143]. Benché sia spesso utilizzato con riferimento alle transazioni in valuta virtuale, il termine fu coniato per definire, in generale, ogni forma di sfruttamento delle nuove tecnologie finalizzata al riciclaggio[144]. Esistono, invero, varie forme di *cyberlaundering*, di complessità variabile, ciascuna delle quali caratterizzata da un veicolo per il "trasporto" della ricchezza dematerializzata[145]; uno dei predetti mezzi è costituito dalle valute virtuali che, a tal fine, si sono rivelate davvero formidabili.

Nel riciclaggio digitale, non diversamente da quanto prospettato per quello analogico, possono distinguersi le tre fasi del piazzamento o sostituzione (*placement*), dispersione o trasferimento dei valori (*layering*) e consolidamento (*integration*). Perché possa parlarsi di *cyberlaundering* è necessario che il provento delittuoso sia reso disponibile in forma dematerializzata: l'utilizzo delle nuove tecnologie in funzione

---

[140] Dei quali si dirà ampiamente poco oltre (v. *infra*, 3.5.).

[141] Così SIMONCINI, *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, cit., 897

[142] Secondo SIMONCINI, *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, cit., 899 il *cyberlaundering* costituisce semplicemente *«un aspetto del più ampio fenomeno del cybercrime, ovvero quel settore della criminalità che opera prevalentemente attraverso 'attacchi' ed azioni di tipo informatico»*.

[143] Osserva PICOTTI, *Profili penali del cyberlaundering,* cit., 609, che le fattispecie di riciclaggio *«sono riconducibili alla categoria dei cybercrime o reati informatici "in senso lato", in quanto possono essere integrate (anche) da condotte che si realizzano concretamente con tecniche informatiche e, più precisamente, nel Cyberspace, senza che la loro punibilità dipenda dalla specifica previsione di elementi tecnici descritti dalla stessa fattispecie legale»*. Sulla distinzione tra reati informatici in senso stretto e in senso lato v. Cap. II, § 1.2. *sub* nota 13.

[144] Per una prima disamina del fenomeno v. MASCIANDRO D., MANTICA A., *Evoluzione dei sistemi di pagamento, internet e cybericiclaggio: prime riflessioni*, in BRUNI E., MASCIANDRO D. (a cura di), *Mercati finanziari e riciclaggio*, Milano 1998; MULINARI S., *Cyberlaundering*, Torino, 2003.

[145] Si pensi, ad es., all'acquisto di una *smart card* prepagata con cui è possibile spendere la provvista illecita per effettuare pagamenti sul mercato legale o per fruire di servizi della società dell'informazione; oppure all'accreditamento diretto di fondi su una piattaforma di scommesse *online* per ripulire il denaro tramite le future vincite.

dissimulatoria andrà dunque a collocarsi in un momento successivo alla digitalizzazione del contante. Laddove il provento sia già disponibile sottoforma di *e-cash* ricorrerà la figura del riciclaggio totalmente digitale.

Preme fin d'ora osservare che le condotte *de quibus* sono tutte entro inquadrabili tra quelle contenute nell'art. 648-*bis* c.p., o alle distinte ipotesi di reimpiego (art. 648-*ter* c.p.) e di autoriciclaggio (art. 648-*ter*.1 c.p)[146]. Con ciò non si intende, beninteso, che nel complesso *iter* che caratterizza il riciclaggio digitale non possano ravvisarsi anche gli estremi di altre fattispecie di reato. La dottrina ha anzi rilevato come il ventaglio degli addebiti possa estendersi, a titolo esemplificativo, anche alla falsificazione o indebito utilizzo di carte di credito o di pagamento (art. 493-*ter* c.p.), all'abuso dell'identità digitale (art. 494; 640-*ter*, comma 3, c.p.), nonché, a seconda dei casi, a reati bancari, societari, tributari etc[147]; di queste ipotesi "contingenti", strettamente collegate alle concrete modalità di realizzazione del fatto, non ci occuperemo in questa sede.

Tratteremo invece delle questioni più significative connesse all'utilizzo delle valute virtuali per fini di riciclaggio, concentrando l'attenzione non solo sui profili sanzionatori, ma anche sulla disciplina preventiva di recente introduzione.

In dottrina si distinguono due diverse forme di *cyberlaundering*: il *riciclaggio digitale strumentale* e il *riciclaggio digitale integrale*[148]. L'*iter criminis* del primo di realizza soltanto parzialmente mediante strumenti informatici poiché occorrono delle attività preliminari per 'convertire' il denaro contante in moneta elettronica; nel riciclaggio totalmente digitale il denaro sporco è invece disponibile in forma dematerializzata. La dottrina da ultimo citata ritiene che le due forme si distinguano nettamente dal punto di vista strutturale. Mentre il riciclaggio digitale strumentale è costituito dalle tre fasi caratteristiche di *placement, layering, integration*, quello integrale si perfezionerebbe con il solo piazzamento della ricchezza, in grado di assorbire le due fasi successive[149]. La distinzione a nostro avviso non coglie nel segno. Anche quando il capitale illecito è spendibile digitalmente la singola operazione di acquisto non è sempre idonea ad ostacolare l'individuazione della provenienza delittuosa; potrebbero dunque essere necessarie operazioni intermedie di *layering* e una successiva operazione finale per riacquisire la disponibilità del contante ripulito[150].

---

[146] Di quest'ultima ci occuperemo nel paragrafo successivo (v. *infra*, § 3.3.).

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

[148] Si richiama la distinzione proposta da SIMONCINI, *Il cyberlaundering: la «nuova frontiera» del riciclaggio,* cit., 900.

[149] Nel *cyberlaundering* integrale la fase di *placement* si caratterizza per l'inserimento nel circuito legale dell'economia legale di denaro già disponibile in forma elettronica. Per riciclare il provento delittuoso sarebbe pertanto sufficiente anche una sola operazione. Si pensi al caso in cui il provento delittuoso sia *ab origine* disponibile su un conto corrente; ove l'intestatario lo utilizzi per l'acquisto di una automobile da collezione, il trasferimento di fondi potrà essere considerato, al tempo stesso, un collocamento della ricchezza e una operazione dissimulatoria.

[150] Nel caso sopra esemplificato potrebbe ben darsi che il trasferimento del denaro non sia idoneo di per sé ad ostacolare l'identificazione della provenienza del denaro e che per il consolidamento della ricchezza occorrano operazioni ulteriori (ad es. la vendita dell'automobile per denaro).

Dal punto di vista criminologico, la tecnologia informatica offre vantaggi di gran lunga maggiori rispetto ai canali "analogici" di lavaggio del denaro. Non solo i cybercriminali agiscono da remoto senza doversi interfacciarsi *de visu* con persone fisiche – circostanza che desensibilizza gli agenti, riducendo la percezione del disvalore sociale della condotta[151] – ma possono altresì contare sulla possibilità di reclutamento/adescamento di terzi fiduciari per il compimento delle operazioni di *layering*. In gergo tecnico vengono detti muli del denaro (*money mules*)[152] coloro che, a fronte del pagamento di una commissione, si sostituiscono al soggetto riciclatore nella realizzazione di una o più operazioni intermedie del processo di riciclaggio. Il più delle volte si tratta di soggetti contattati occasionalmente su *chat room* o giochi *online*, di giovane età, ignari e incensurati, non riconducibili in alcun modo al riciclatore o all'autore del delitto presupposto; ciò rende decisamente più complessa l'identificazione della provenienza delittuosa del denaro. Tra i punti di forza del *cyberlaundering* vi sono inoltre le indubbie difficoltà nell'individuazione del *locus commissi delicti* e dell'identità dei soggetti coinvolti nella filiera criminosa, diretta emanazione delle note caratteristiche di anonimità della rete e di transnazionalità dei reati informatici[153].

3.1.1. In particolare: l'utilizzo delle valute virtuali per fini di riciclaggio.

Nel corso della trattazione abbiamo fatto più volte riferimento alle proprietà criminogene delle valute virtuali, sottolineando come la decentralizzazione nella tenuta dell'infrastruttura informatica sia un volano per molte attività criminali, tra cui figura, *in primis*, il riciclaggio di denaro sporco. È infatti sufficiente il mero acquisto di Bitcoin con denaro di provenienza illecita per ostacolare significativamente la tracciabilità del flusso monetario; ciò può avvenire in vario modo sia convertendo fisicamente il denaro presso appositi sportelli ATM sia effettuando un bonifico in favore di un cambiavalute virtuale. A quel punto il capitale potrà essere facilmente scambiato con altre valute virtuali, a loro volta suscettibili di nuova negoziazione, in modo tale da rendere quasi impossibile la ricostruzione della "pista" digitale.

La criptomoneta massimizza i benefici del riciclaggio digitale, agevolando la movimentazione dei capitali e garantendo un più alto grado di anonimato. Nelle infrastrutture *blockchain* totalmente decentralizzate lo scambio avviene *peer to peer*, senza passare per soggetti terzi gravati dagli obblighi antiriciclaggio; è questo un problema tutt'ora aperto, mitigato ma certamente non risolto, dall'estensione della disciplina preventiva ai prestatori di servizi operanti sul mercato valutario virtuale. Il sistema è concepito per consentire l'invio e la ricezione di denaro con garanzie di

[151] Sulla desensibilizzazione soggettiva nei reati informatici v. *supra* Cap. II; § 1.3.
[152] Per approfondimento sull'attività dei *money mules* v. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling
[153] Cfr. SEVERINO P., *Sicurezza informatica e prevenzione del cybercrime*, in *LuissOpen*, 8 settembre 2017, 11, 6 (*amplius* v. Cap. II, § 1.1.).

anonimità pressoché impenetrabili, che fanno rientrare dalla finestra il segreto bancario che faticosamente il legislatore internazionale ha fatto uscire dalla porta[154].

Riservando per il momento l'esame della disciplina preventiva, l'attenzione andrà rivolta ai profili repressivi e sanzionatori. Ci si chiede, anzitutto se, avuto riguardo alle modalità esecutive della condotta e all'oggetto materiale del reato, il *cyberlaundering* commesso mediante operazioni in valuta virtuale possa essere ricondotto entro il perimetro applicativo dell'art. 648-*bis* c.p.

La premessa sulla struttura del delitto di riciclaggio lascia ben propendere per la soluzione affermativa. Non essendo richieste particolari forme, il disvalore di azione si impernia sulla idoneità della condotta ad ostacolare l'identificazione della provenienza illecita del denaro o delle altre utilità: *nulla questio* dunque sulla rilevanza penale delle transazioni in criptomoneta che rendono per definizione estremamente difficoltoso il tracciamento dell'origine delittuosa dei fondi. Altrettanto agevole è l'individuazione dell'oggetto materiale del reato, per definire il quale occorrerà sinteticamente richiamare i risultati dell'indagine svolta nel primo paragrafo. I principi della teoria c.d. *funzionale* della moneta portano a escludere l'assimilazione tra le valute virtuali e il denaro[155]; queste ultime assolvono soltanto in misura parziale e imperfetta alle funzioni di mezzo di scambio, unità di conto e riserva di valore. Trattandosi di valori di privata emissione, svincolati da qualsiasi ente emittente centralizzato e monopolistico, deve *a fortiori* negarsi la funzione monetaria secondo l'approccio statualista. Al riguardo è sufficiente richiamare le considerazioni sopra svolte in punto di tassatività nell'applicazione della fattispecie incriminatrice.

Ostacoli non meno significativi si oppongono alla sussunzione nella categoria dei "beni". Per quanto *prima facie* possano rientrarvi tanto i beni materiali quanto quelli immateriali, la tesi che va per la maggiore[156] è nel senso di includere le sole *res* tangibili, suscettibili di essere oggetto di diritti. Senza in alcun modo forza il dato letterale, le valute virtuali possono più facilmente essere ricondotte alle "altre utilità" indicate nella clausola finale dell'art. 648-*bis* c.p., formula tanto ampia da ricomprendere qualsiasi entità economicamente apprezzabile[157].

Il *cyberlaundering* "virtuale" potrà seguire lo schema del riciclaggio digitale strumentale o di quello digitale integrale, in base alla forma, analogica o digitale, del provento delittuoso. Nel primo caso la fase di *placement* avrà ad oggetto un'operazione

[154] È noto come il diritto internazionale pattizio ammetta oggi ampie deroghe al segreto bancario, in virtù degli accorsi di mutua collaborazione in materia penale e/o tributaria.

[155] *Amplius* v. §1.5.

[156] Cfr. FIANDACA-MUSCO, *Diritto Penale*, cit., 23 secondo cui *«è definibile cosa, nel senso del diritto penale, ogni oggetto corporale o fisico: in altri termini, ogni entità fisica del mondo esterno che presenti i caratteri della definitezza spaziale e della esistenza autonoma».* Si è già detto che le valute virtuali non sono altri che dati informatici; riprenderemo la questione definitoria più avanti quando tratteremo dell'indebita sottrazione di valuta virtuale (v. *infra*, § 5).

[157] In tal senso v. DI VIZIO, *Le cinte daziarie del diritto penale,* cit., 121; CAPACCIOLI S., *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015, 252. Contra, STURZO L., *Bitcoin e riciclaggio 2.0.*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2018, 5, 24, la quale ritiene che la valuta virtuale possa rientrare nell'ampio concetto di "bene" in senso penalistico, salva in ogni caso la riconducibilità alla categoria delle altre utilità.

di cambio del circolante per moneta elettronica o direttamente per Bitcoin[158]; nel secondo, essendo già disponibile allo stato di moneta elettronica, l'interessato potrà convertirla in valuta virtuale tramite una piattaforma di scambio, effettuando un semplice money *transfer*.

Questa prima fase è chiaramente la più delicata dell'intero *iter* di ripulitura del denaro. Affinché la ricchezza possa essere collocata nel circuito economico virtuale, i potenziali riciclatori dovranno giocoforza passare per l'intermediazione di alcuni soggetti (istituti di credito, cambiavalute virtuali, piattaforme di *trading*); si spiega dunque perché il legislatore abbia voluto estendere gli obblighi antiriciclaggio ai *provider* degli scambi.

Accanto a queste due forme di *cyberlaundering* potrebbe individuarsene una terza: il *riciclaggio virtuale integrale*. Ogniqualvolta il provento del reato sia *ab origine* disponibile in valuta virtuale[159] non sarà necessaria alcuna attività di *placement;* l'assenza di intermediari nella conversione rende questa forma di riciclaggio in assoluto la più difficile da contrastare.

La fase di *layering* consiste nella movimentazione di valuta virtuale tra più indirizzi appartenenti allo stesso soggetto o a terzi intestatari di comodo. Per agevolare tali operazioni è possibile accedere a servizi *mixing* di transazioni, aventi quale unico scopo quello di impedire l'associazione diretta tra il mittente e il destinatario di valuta virtuale in base alle risultanze della *blockchain*[160].

Il processo si chiude con il rientro dei capitali ripuliti (*integration*) nella disponibilità del reo. Ciò può avvenire in due diversi modi, a seconda delle aspettative di successivo reimpiego.

I valori virtuali potranno essere riconvertiti in moneta *fiat* da investire in attività economiche e/o speculative; ciò richiede un nuovo passaggio per gli intermediari nei sistemi di pagamento con tutti i pericoli connessi all'attivazione dei presidi antiriciclaggio. In alternativa, si potrà scegliere di abbandonare la dimensione finanziaria reale per investire la criptomoneta in fondi di investimento virtuali o spenderla per l'acquisto di beni o la fruizione di servizi[161]. La progressiva affermazione della criptomoneta come mezzo di scambio – valuta parallela e complementare a quella avente corso legale – apre orizzonti significativi per il consolidamento dei capitali di

[158] Esistono diversi modi per convertire il denaro contante in valuta virtuale. La via più immediata è quella di avvalersi di appositi ATM che accettino rimesse in contante e forniscano in cambio le chiavi crittografiche del *tantundem* in Bitcoin; in alcuni Stati (come ad esempio la Svizzera) questi sportelli sono diffusi e accessibili a chiunque. In alternativa sarà necessario un doppio passaggio: dapprima il deposito delle somme su conti correnti o carte prepagate, e poi l'acquisto di criptomoneta presso un cambiavalute virtuale.

[159] Si ipotizzi il caso in cui oggetto della ripulitura sia il prezzo pagato per l'acquisto di beni intrinsecamente illeciti sul *dark web* oppure il corrispettivo pagato per liberare un sistema informatico da un *ransomware*.

[160] *Amplius,* v. § 3.4.2.

[161] Alcune valute virtuali sono accettate come mezzo di pagamento da un crescente numero di operatori economici. Sicché il rientro nel circuito dell'economia lecita potrà realizzarsi anche senza la previa conversione in moneta avente corso legale, semplicemente acquistando beni o servizi della società dell'informazione.

provenienza illecita: alla più ampia accettazione come strumento di pagamento corrisponde una minore propensione allo scambio in valuta *fiat* da cui deriva una parziale sfasatura dello schema tipico del *cyberlaundering*. La fase di integrazione non è distinta dal successivo reimpiego: il valore virtuale ripulito rientra nel circuito dell'economia reale tramite l'acquisto di beni o la fruizione di servizi, senza necessità della previa conversione in valuta avente corso legale[162].

Per far fronte a queste nuove manifestazioni criminose il legislatore dovrebbe considerare l'opportunità di estendere gli obblighi antiriciclaggio anche in capo a coloro che, pur non prestando servizi connessi all'utilizzo di valute virtuali, le accettino come mezzo di pagamento. Si ritiene infatti che la conversione di queste valute in moneta reale sia una un passaggio destinato a un progressivo abbandono[163]. L'investimento diretto dei fondi virtuali i criminali diverrebbe così un *commodus discessus in* grado di neutralizzare il sistema di controlli preventivi del riciclaggio[164].

3.2. Valori virtuali e *cyber-self-laundering*

Se volessimo utilizzare una metafora per descrivere questa nuova frontiera del riciclaggio il paragone con la "lavatrice virtuale", facilmente programmabile e comoda da utilizzare, sarebbe certamente efficace. Per effetto dell'automazione del processo di lavaggio viene progressivamente il "mestiere" di molti intermediari della filiera del riciclaggio, alimentando l'opposta tendenza al "fai da te" e alla gestione *in-house* delle attività riciclatorie. Detto altrimenti, l'innovazione tecnologica ha aperto nuovi orizzonti all'autoriciclaggio, offrendo all'autore del reato presupposto un veicolo formidabile di movimentazione dei capitali illeciti. La prospettiva più allettante è quella del pieno controllo operazione, che fa venire meno i rischi della gestione esterna di alcune delicate fasi del processo nonché i costi per la remunerazione dei terzi concorrenti nel reato. L'impiego delle valute virtuali potrebbe in tal senso condurre a una smisurata espansione della sfera del *self laundering*, fenomeno alquanto preoccupante se solo si considera l'elevato potenziale di queste ultime di ostacolare l'identificazione della provenienza delittuosa del denaro.

Tanto premesso, non può che accogliersi con favore la scelta del legislatore di sfatare l'idolo del *post factum* non punibile[165] e di punire in via autonoma

[162] Basti pensare al caso in cui l'autore del delitto presupposto o il riciclatore investano il capitale ripulito nella propria attività d'impresa, acquistando materie prime da impiegare nella produzione.

[163] Le attività di "lavaggio virtuale" si svolgono interamente *online* e il transito per la dimensione dell'economia reale potrebbe non essere necessaria: l'estensione degli obblighi antiriciclaggio ai cambiavalute virtuale e ai *wallet provider* appare dunque insufficiente.

[164] Si può dunque concordare con quella parte della dottrina che, commentando le novità introdotte dal D. Lgs. 90/2017, ha osservato che *«porre il presidio antiriciclaggio in relazione a soggetti eventualmente, forse probabilmente, ma non certamente, ricompresi nella transazione non servirà ad affievolire l'elevata minaccia di riciclaggio intrinsecamente presente nelle caratteristiche del bitcoin»*, così STURZO, *Bitcoin e riciclaggio 2.0.*, cit., 30.

[165] In dottrina era diffusa l'opinione che i fatti di riciclaggio realizzati dallo stesso autore del reato presupposto dovessero essere considerati un mero *post factum* non punibile, figurando come uno

l'autoriciclaggio[166]. Il *novum* normativo ha riguardato anche la responsabilità delle persone giuridiche grazie all'interpolazione dell'art. 25-*octies* del D.Lgs. 231/2001, considerata dalla dottrina una "rima" quasi obbligata[167]. La non punibilità dell'autore del delitto presupposto sarebbe decisamente inopportuna nel contesto economico attuale in cui lo spazio virtuale si appresta a divenire il principale canale di lavaggio del denaro sporco.

L'autoriciclaggio è posto a presidio della libera concorrenza del mercato, la quale rischierebbe di essere falsata dall'impiego di capitali di provenienza illecita da parte di alcuni attori economici; depone in questo senso la previsione di una clausola di non punibilità delle sole condotte di destinazione alla mera utilizzazione e godimento personale. La struttura della fattispecie riflette quasi specularmente quella dell'art. 648-*bis* c.p., pur risultando da una sorta di ibridazione tra riciclaggio e reimpiego[168]. L'*iter criminis* si presta ad essere scomposto anche in questo caso in *placement*, *layering* ed *integration*, con la precisazione che a quest'ultima fase deve collegarsi l'immissione

---

sviluppo normale del delitto presupposto, se non addirittura come una forma indiretta di manifestazione del diritto di difesa (art. 24 Cost.). Cfr. senza pretese di esaustività, SEMINARA S., *I soggetti attivi del reato di riciclaggio tra diritto vigente e prospettive di riforma,* in *Dir. pen. proc.,* 2005, 236; CASTALDO A. R. – NADDEO M., *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio,* Padova, 2010, 92 ss.; BRICHETTI R., *Riciclaggio e autoriciclaggio,* in *Riv. it. dir. proc. pen*., 2014, 2, 684 ss.; NADDEO M., MONTEMURRO D., *Autoriciclaggio e teoria degli insiemi: un "privilegio" matematicamente sostenibile,* in *Riv. trim. dir. pen. econ*., 2011, 237 ss.

[166] L'art. 3 della L. 15 dicembre 2014 n. 186 ha introdotto nel codice penale, all'art. 648-*ter*.1 c.p. il delitto di autoriciclaggio: «*Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa […]*». In dottrina v. SGUBBI F., *Il nuovo delitto di "autoriciclaggio": una fonte inesauribile di "effetti perversi" dell'azione legislativa,* in *Diritto penale contemporaneo*, 10 dicembre 2014; CARACCIOLI I., *L'incerta definizione del reato di riciclaggio,* in *Il Fisco*, 2015, 4; CAVALLINI S., TROYER L., *Apocalittici o integrati? Il nuovo reato di auto riciclaggio: ragionevoli sentieri ermeneutici all'ombra del "vicino ingombrante"*, in *Diritto penale contemporaneo – Rivista trimestrale*, 1, 2015 95 ss.; BRUNELLI D., *Autoriciclaggio e divieto di retroattività: brevi note a margine del dibattito sulla nuova incriminazione*, ivi, 86 ss.; MUCCIARELLI F, *Qualche nota sul delitto di autoriciclaggio,* ivi, 108 ss.; CORSO P., *Il declino di un "privilegio": l'autoriciclaggio (anche da reato tributario) ha rilievo penale autonomo*, in *Corriere tributario*, 2015, 3, 159 ss.; D'AVIRRO A., GIGLIOLI M., *Autoriciclaggio e reati tributari*, in *Diritto penale e processo,* 2015, 145 ss.; GULLO A., *Autoriciclaggio e reati tributari,* in *Diritto penale contemporaneo*, 13 marzo 2018; MAUGERI A.M., *La lotta all'evasione fiscale tra confisca di prevenzione e autoriciclaggio La confisca dei proventi dell'evasione fiscale o dei redditi leciti non dichiarati fiscalmente?* , ivi, 2 marzo 2015.

[167] Tra i primi commentatori v. GAREGNANI G.-GALLI G.-TROYER L., *Brevi note sull'introduzione del nuovo delitto di autoriciclaggio nel novero dei reati presupposto della responsabilità amministrativa da reato di cui al D.Lgs. 231/01*, in *Rivista dott. comm.*,2015, 3, 467 ss.; D'ARCANGELO F., *Gli effetti penali della* voluntary disclosure *e la responsabilità da reato degli enti*, in *Responsabilità amministrativa delle società e degli enti*, 2015, 2, 9 ss.; PICCINNI L.M., DI FRANCO G., *Genesi normativa e peculiarità del money laundering: il delitto di riciclaggio quale reato presupposto per la configurazione dell'art. 25-*octies*, d.lgs. 231/2001. Da reato dei white collars, a diffuso illecito di criminalità economica*, ivi, 1, 32 ss.

[168] Cfr. GULLO A., voce *Autoriciclaggio*, in *Il libro dell'anno del diritto* 2016, in https://treccani.it ; CAVALLINI - TROYER, *Apocalittici o integrati*, cit., 98 ss.

del capitale ripulito in «*attività economiche, finanziarie, imprenditoriali o speculative*».

A tal riguardo ci si chiede se il collocamento del provento delittuoso sulla piazza finanziaria virtuale possa essere considerato per ciò solo un impiego in attività speculative[169]. In linea di principio la conversione denaro in criptomoneta è neutrale, nel senso che, pur essendo idonea ad ostacolare l'identificazione della provenienza delittuosa, potrebbe essere motivata dall'intento di spendere la riserva per l'acquisto di beni di consumo. D'altro canto, non può tacersi che lo scambio dei valori virtuali sia attualmente motivato da propositi di mera speculazione, mentre l'utilizzo come strumento di pagamento risulta decisamente recessivo. Tale circostanza rende piuttosto incerti i limiti della rilevanza penale delle condotte di sostituzione o impiego del denaro, che dipenderà anche dalla risoluzione del dubbio amletico della natura giuridica della valuta virtuali. Aderendo alla tesi della natura monetaria pura si dovrebbe escludere che la semplice conversione del denaro integri una attività speculativa: andrebbe infatti considerata alla stregua di un acquisto di valuta estera per valuta nazionale. Se al contrario si riconoscesse natura finanziaria alla criptomoneta, dovrebbe ammettersi la possibilità della rilevanza penale del mero acquisto *ex* art. 648-*ter.1* c.p.

A nostro avviso il problema non ammette una soluzione univoca ma chiama in causa inevitabili discettazioni sulla componente psicologica del reato. In dottrina non vi è unanimità di vedute sulla consistenza generica o specifica del dolo richiesto ai fini dell'integrazione del delitto in esame. Secondo la tesi maggioritaria l'autoriciclaggio è punito a titolo di dolo generico[170]: sarebbe dunque sufficiente che il reo abbia agito rappresentandosi tutti gli elementi del fatto tipico, nella consapevolezza della provenienza illecita della ricchezza e con la volontà di agire in modo da ostacolare concretamente l'individuazione l'origine delittuosa dei proventi e di investire gli stessi nell'ambito di attività di carattere economico, finanziario, imprenditoriale o speculativo. Altri qualificano il delitto come a dolo specifico, argomentando che ai fini dell'integrazione dell'elemento soggettivo l'agente debba agire a scopo di lucro mirando, dunque, all'ottenimento di un profitto. A sostegno di tale impostazione si è rilevato che il riferimento alle attività economiche e la contestuale presenza della causa di esclusione della punibilità c.d. "utilizzo/godimento personale" inducono a ritenere che, se il soggetto attivo non agisse al fine di conseguire uno scopo di lucro, non avrebbe alcuna ragione per reinvestire i proventi in attività di stampo economico[171]. Se si aderisse a questa seconda tesi, minoritaria in dottrina, l'integrazione del delitto dipenderebbe dalle finalità perseguite dall'agente, nel senso che la conversione sarebbe penalmente rilevante soltanto se motivata dal fine di conseguire un profitto. Laddove

[169] Si pensi al caso in cui il soggetto attivo di una truffa abbia convertito in Bitcoin il profitto del reato per occultarne la provenienza delittuosa, con l'intento ulteriore di ottenere plusvalenze di investimento. In argomento, da ultimo SICIGNANO G. J., *Bitcoin e riciclaggio*, Torino, 2019, 167 ss.
[170] Cfr. MUCCIARELLI, *Qualche nota sul delitto di autoriciclaggio*, cit., 114
[171] DI TULLIO D'ELISIIS A., *Autoriciclaggio. Applicazione e strategie difensive*, Rimini, 2015, 62 ss.

si propendesse per la punibilità a titolo di dolo generico – tesi più coerente con il testo della norma – rimarrebbe aperto il problema di fondo di stabilire se soggetto si fosse rappresentato o meno la natura speculativa dell'attività. In entrambi i casi l'accertamento giudiziale andrà rivolto alla ricerca di indici rivelatori della rappresentazione/volizione del soggetto di investire i capitali in attività finanziarie o speculative.

La dottrina che finora ha affrontato il tema esclude che la semplice conversione di valuta reale in valuta virtuale, e viceversa, dia luogo ad un'attività speculativa, interrogandosi piuttosto sulla riconducibilità delle stesse ad un'attività finanziaria[172]. Riteniamo all'opposto che la volatilità del prezzo delle valute virtuali dovrebbe far riflettere sulla qualificazione penalistica come attività speculativa[173]. Sarebbe del resto erroneo limitare il campo di applicazione dell'autoriciclaggio alle sole condotte in grado di esporre il sistema finanziario reale a infiltrazioni criminose, considerando estraneo alla *ratio* della disposizione la trasparenza del mercato dei servizi digitali. Una tale interpretazione si porrebbe in contrasto con la *voluntas legis* sottesa alla riforma del 2014, ovverosia la tutela della tutela della concorrenza nel mercato. Si è infatti avuto modo di constatare[174] che le due dimensioni economiche presentano numerosi punti di contatto, sicché l'investimento di capitali illeciti sul mercato virtuale aumenta la richiesta di circolante, fa crescere il prezzo dei *token*, e altera l'equilibrio sul mercato dei beni.

Con espressa riserva di esaminare nel prosieguo la questione relativa al concorso dell'*extraneus* in autoriciclaggio[175], ci limiteremo ora a considerare alcuni aspetti esteriori dell'impiego delle valute virtuali da parte dell'autore del delitto presupposto.

Dal punto di vista pratico-operativo, questa forma di *self-laundering* non richiede la conoscenza dei protocolli tecnici o della crittografia informatica, sicché anche l'utente medio di *internet* potrebbe procurarsi la disponibilità dei valori virtuali e effettuare operazioni di acquisto o conversione. Ciò conferma l'assunto di partenza che l'autore del delitto presupposto non ha più bisogno del supporto di terzi fiduciari, potendo fare tutto *manu propria*: aprire conti presso istituti di moneta elettronica, convertire il denaro in valuta virtuale, mixare le transazioni, scambiare valori in base alla quotazione di mercato, acquistare beni o servizi in Bitcoin etc. Tutte queste attività possono essere compiute dietro l'egida dell'anonimato grazie alla creazione di *account* fasulli sulle piattaforme di scambio o sui siti di gestione dei pagamenti, senza che sia più necessario ricorrere a prestanome o intermediari di comodo.

---

[172] Si veda STURZO, *Bitcoin e riciclaggio 2.0*, cit., 25. Sulla natura finanziaria dei valori virtuali di rinvia alle riflessioni svolte nel capitolo successivo (v. *infra*, Cap. IV, § 1 ss.).

[173] Il terreno risulta comunque scivoloso. Se si attribuisse rilevanza *ex* art. 648-*ter*.1 c.p. alle condotte di mero acquisto di valuta virtuale si potrebbe facilmente contravvenire al divieto di applicazione analogica *in malam partem* della disposizione.

[174] *Amplius* in questo capitolo § 1.4.

[175] La questione sarà esaminata quando tratteremo della responsabilità dei cambiavalute virtuali per concorso in riciclaggio (*infra*, § 3.5.1.).

Quando oggetto materiale della condotta è la moneta avente corso legale ricorre lo schema dell'autoriciclaggio virtuale strumentale: l'autore del reato presupposto cambia moneta *fiat* ricevendo in cambio *token*; se il provento criminoso risulta già disponibile in criptovaluta lo schema commissivo è quello del riciclaggio virtuale integrale[176].

3.3. Gli operatori professionali sul mercato valutario virtuale.

Alla base delle valute virtuali vi è un procedimento di emissione molto particolare, che dipende dalla tipologia di infrastruttura alla quale esse appartengono. La quantità di circolante, fissa o variabile che sia, viene predeterminata dal protocollo di sistema; ciò spiega la tendenza deflazionistica e il rapporto di proporzionalità diretta tra la potenza di calcolo della rete e il numero di informazioni che i partecipanti possono processare o scambiare; se così non fosse si presenterebbe il problema di dover elaborare un numero di transazioni superiore alla capacità computazionale del sistema.

Nelle *blockchain* pubbliche il meccanismo delle ricompense è alla base della creazione di nuovo valore; i soggetti che offrono risorse alla rete (*miner*) ottengono un corrispettivo per ogni transazione validata generando così nuove "preziose" informazioni[177]. Nelle reti private *permissioned* (siano esse parzialmente decentralizzate o centralizzate) la decisione sugli elementi essenziali dell'offerta di *token* (natura, tipologia e quantità) spetta al titolare del sistema oppure alla maggioranza dei partecipanti.

In entrambi i casi l'informazione sarebbe del tutto "autoreferenziale, se non vi fossero alcuni operatori in grado di creare un mercato a valle per lo scambio e la fruizione di questi dati informatici. In un sistema chiuso, i soggetti esterni non hanno possibilità, e tantomeno necessità, di entrare in possesso dei valori virtuali, rappresentativi unicamente della "forza lavoro" di coloro che operano all'interno della rete. L'informazione digitale acquisisce valore economico in misura proporzionale alla sua fruibilità, all'attitudine a poter essere utilizzata per fare qualcosa che altri non possono fare, o avere qualcosa che altri non possono avere.

Per quanto l'affermazione possa in astratto sembrare lapalissiana, la recente storia di Bitcoin fornisce all'assunto una dimostrazione empirica. La popolarità del progetto crebbe con la quotazione sul portale Mt. Gox che portò nel giro di pochi mesi il valore di scambio alla parità con il dollaro[178]. Successivamente, il prezzo continuò a crescere

[176] Deve opportunamente ribadirsi che in questo secondo caso non è necessario passare per la conversione del denaro; il reo potrà dunque agevolmente bypassare i presidi antiriciclaggio posti in capo ai fornitori dei servizi di *exchange.*

[177] Alla base di tale circostanza sta la necessità di rendere sicure le transazioni e di prevenire fenomeni di *double spending*; ogni transazione deve essere autenticata utilizzando un protocollo di codifica che richiede la potenza di calcolo di una rete di computer privati, chiamati *mining rigs.* Per ottenere una quantità minima di criptovaluta è necessario l'apporto di una potenza di calcolo via via crescente in base all'aumento della potenza di calcolo e alla quantità di criptovaluta circolante, che può essere fornita soltanto da elaboratori sofisticatissimi. *Amplius,* Cap. I, § 2.2.

[178] Per approfondimenti v. Cap. I, § 1. Cfr. LEMME, PELUSO, *Criptomoneta e distacco dalla moneta legale,* cit., 28

di pari passo con la diffusione di nuove di piattaforme di scambio e con l'accettazione come strumento di pagamento in molti siti di *e-commerce*; il successo di Bitcoin fu seguito dalla quotazione di molte altre valute virtuali che condusse alla formazione di un vero e proprio mercato valutario virtuale.

La "scarsità artificale" delle informazioni circolanti sui registri distribuiti non potrebbe attribuire alcun valore intrinseco ai *token*. La *blockchain* altro non rappresenta che una infrastruttura tecnologica per fare scambi: è il mercato a stabilire quanto gli operatori economici sono disposti a pagare per fruirne o per avere la disponibilità esclusiva di una quota parte delle informazioni in essa registrate. I fornitori di servizi di cambio, gestione e investimento di valuta virtuale divengono così una leva essenziale dell'economia della tokenizzazione, il vero fulcro del mercato valutario.

Non può del resto trascurarsi l'importante ruolo di questi soggetti come "centro di recupero" della centralizzazione in una dimensione economica ispirata alla disintermediazione degli scambi. Trattando del tema della prevenzione del riciclaggio occorrerà dapprima esaminare brevemente le diverse tipologie di attività svolte dagli intermediari, per poi concentrare l'attenzione sui doveri di collaborazione con l'Autorità e sui connessi profili di responsabilità.

3.3.1. Piattaforme di *trading* e prestatori di servizi di cambio.

La crescita del coefficiente di capitalizzazione del mercato valutario virtuale è stata dunque accompagnata dal proliferare delle piattaforme di *trading*[179].

Tra le operazioni di *trading*, in senso lato, rientrano le attività – comunque esse siano denominate – di acquisto, vendita, e cambio di moneta virtuale per moneta reale. Si è detto che, a differenza di altre forme di valori digitali, le criptovalute appartengono alla categoria delle valute virtuali a c.d. *flusso bidirezionale*, in cui la valuta reale può essere convertita in moneta virtuale utilizzabile per l'acquisto di beni o servizi (virtuali, ma anche reali), essendo a sua volta riconvertibile in valuta reale[180].

Le operazioni di acquisto, vendita e scambio assumono denominazioni differenti a seconda che si valorizzi la fisionomia delle valute virtuali come strumento finanziario (si preferisce in tal caso la denominazione acquisto/vendita) ovvero le si consideri "moneta" a tutti gli effetti (si parla allora di operazioni di "cambio")[181].

Al di là del profilo puramente terminologico, appare ben più rilevante ai nostri fini descrivere in cosa si sostanzia l'attività esercitata dagli intermediari nel *trading*. Le valute virtuali di più ampia diffusione (Bitcoin, Ethereum, Litecoin) corrono su registri

[179] In passato si sono registrati anche forti segnali di contrazione dell'erogazione di servizi di intermediazione nella compravendita di criptovaluta, a causa di falle nel sistema informatico o di attacchi ai *software* di gestione dei servizi di portafoglio digitale. Emblematico è il caso dell'*exchange* Mt. Gox ripetutamente "bucato" da attacchi informatici o il *crac* della piattaforma Bitfinex causato dalla sottrazione fraudolenta di oltre 200.000 Bitcoin, equivalenti allora a circa 72 milioni di dollari statunitensi.

[180] Si veda il già citato rapporto della Banca Centrale Europea *Virtual Currency Schemes* (*supra*, § 2.1.).

[181] Cfr. DI VIZIO, *Le cinte daziarie del diritto penale,* cit., 100

che utilizzano sistemi di validazione "diffusa" delle transazioni *peer-to-peer* (P2P). Nella maggior parte dei casi l'attività dell'intermediario consiste nel favorire l'incontro tra la domanda e l'offerta di criptomoneta tra utenti remoti ed anonimi, si parla in questo caso di *trading indiretto*, remunerato dalle commissioni di cambio, predeterminati in misura percentuale rispetto al valore dell'operazione. Altre piattaforme di cambio, invece, offrono un vero e proprio servizio di conversione a richiesta, consentendo agli utenti di acquistare valuta digitale in cambio di moneta elettronica reale (tramite bancomat, prepagate, PayPal, o carte di credito) ad un tasso di cambio predefinito. In questo caso l'attività è denominata *trading diretto.* Tali operatori, noti come cambiavalute virtuali operano sul mercato "rastrellando" valori virtuali, che acquistano ad un prezzo vantaggioso o "autoproducono" attraverso il *mining*. La raccolta è finalizzata al successivo cambio in valuta reale ad un prezzo sicuramente maggiore di quello di acquisto o di "produzione".

Oltre a favorire l'incontro tra domanda e offerta (*trading*) vengono anche offerti servizi di custodia e trasferimento dei *token* (*post-trading*)[182]. Le piattaforme che consentono la negoziazione dei *token* vengono indicate come *exchange*, mentre la custodia ed il trasferimento dei *token* sono realizzati attraverso i *wallet*[183]. I due concetti vengono spesso confusi poiché le piattaforme di *exchange* operano frequentemente anche come *wallet provider*. Nel recente documento per la discussione proposto da Consob si distingue anche tra le piattaforme organizzate con un vero e proprio *book* che provvede al *matching* di ordini (*platform with order book*) e piattaforme che invece consentono una negoziazione diretta tra le parti (*direct trading* o P2P). Oltre a queste, l'Autorità individua anche un terzo modello in cui gli utenti negoziano in via esclusiva con il relativo gestore (*dealer*), che detiene un proprio registro degli ordini (*dealer type model*). Quanto ai servizi collaterali di custodia e di trasferimento dei *token*, è opportuno osservare che, laddove l'utente depositi i valori sulla piattaforma di *trading*, le chiavi private e pubbliche che identificano ciascun utente nella *blockchain* saranno affidate alla gestione del *provider*. Pertanto, nel caso in cui l'ammontare sia convertito direttamente dal *dealer*, non vi saranno spostamenti di informazioni in *blockchain*, ma soltanto uno scambio di chiavi crittografiche associata a una registrazione contabile di dare/avere.

Quale che sia la tipologia di servizio offerta, deve ribadirsi come l'attività degli *exchange* e dei *wallet provider* rappresenti il motore dell'intero mercato valutario virtuale; senza di essi la criptomoneta sarebbe fruibile soltanto da pochi esperti del settore, magari motivati da propositi criminosi. La semplicità di accesso e di utilizzo a

[182] Sul punto si veda il Documento di consultazione pubblicato da Consob, *Le offerte iniziali e gli scambi di criptoattività,* cit. *sub* nota 105, 11.

[183] Un portafoglio è un programma per elaboratore che salva le chiavi pubbliche e le chiavi private, installabile direttamente su proprio dispositivo o costituito da un *hardware* specifico, come un dispositivo di memoria esterna. Esistono diversi tipi di portafogli in base alle caratteristiche di sicurezza, alle finalità specifiche del portafoglio o alle diverse attività di business; per una classificazione v. DI VIZIO, *Le cinte daziarie del diritto penale,* cit., 101. Sulla distinzione tra *hot wallet* e *cold wallet* ai fini delle attività investigative e alle misure cautelari esperibili v. Cap. V, § 6.

questi servizi ha contribuito alla crescita del mercato della criptomoneta, facendo interessare all'economia virtuale anche l'investitore medio.

La centralità del ruolo occupato dai prestatori di servizi di deposito e cambio non è sfuggita all'attenzione del legislatore, recentemente intervenuto per porre un freno allo sfruttamento degli strumenti virtuali per fini di riciclaggio e finanziamento del terrorismo. La scelta appare certamente condivisibile in considerazione della indiscutibile "forza centripeta" che detti soggetti sono in grado di esercitare sull'economia distribuita. Da recenti studi[184] si apprende che il modello operativo attualmente dominante sul mercato valutario virtuale è quello delle piattaforme centralizzate che operano sia come piattaforma di *trading* che come fornitore del servizio di *wallet.* Per partecipare alle attività di negoziazione gli utenti trasferiscono i propri valori sulla piattaforma *exchange,* che registra tali attività su un proprio *database*[185]. In tale modello operativo, dunque, le attività di negoziazione non generano alcun trasferimento di *asset* sulla *blockchain*, che viene aggiornata esclusivamente per registrare i trasferimenti, relativi alle fasi di deposito e ritiro di *token*, che intercorrono tra gli investitori e la piattaforma *exchange*.

3.3.2. Servizi di *mixing.*

Le transazioni in criptomoneta sono annotate sulla *blockchain* e associate all'indirizzo di portafoglio delle parti. Pertanto, le movimentazioni in valuta virtuale, anche se anonime, sono in linea di principio perfettamente tracciabili. Per non dare l'apparenza del compimento di attività "sospette" – ed evitare quindi un passaggio di "denaro" diretto tra due portafogli digitali – si dovrebbe spezzare la concatenazione di trascrizioni sul "libro mastro" pubblico.

A tal fine è possibile affidarsi a servizi di *mixing*, il cui funzionamento può essere sinteticamente descritto nei termini seguenti[186]. Un utente deposita un determinato ammontare di criptovaluta su uno o più conti di ingresso, per poi riprendersi il denaro virtuale su conti di uscita preesistenti o appositamente creati[187]. Il *mixer* farà in modo che non sia possibile associare direttamente l'ammontare di denaro depositato all'ammontare ritirato alla fine, e tratterà – quale corrispettivo della propria intermediazione – una percentuale sul valore della transazione.

I prestatori di servizi di *mixing* utilizzano due espedienti. Una prima tecnica consiste nell'invio "a catena" di moneta da numerosi portafogli, dai quali poi si dipartiranno altre operazioni dirette ad altri conti. L'obiettivo è quello di rendere la

---

[184] *Le offerte iniziali e gli scambi di criptoattività,* cit., 12

[185] Secondo la Consob l'*exchange* agisce anche da "internalizzatore di regolamento", registrando sui propri sistemi il trasferimento di token (ed eventualmente di valuta corrente) conseguente alle negoziazioni.

[186] Per un inquadramento del *mixing* tra gli *smart contract,* con particolare riguardo alle problematiche relative all'assenza di dolo del fatto da parte del programmatore v. *supra* Cap. II, § 3 ss.

[187] In argomento D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta,* cit., 11; DI VIZIO, *Le cinte daziarie del diritto penale,* cit., 102.

rete dei passaggi a tal punto complessa da rendere quasi impossibile la ricostruzione dei singoli passaggi intermedi. Gli indirizzi che partecipano a questa attività sono chiamati "conti di rimbalzo" (conti *bounce*).

Diversamente, è possibile raggruppare i fondi di più utenti che si sono rivolti al servizio di *mixing* in un unico indirizzo, detto conto *pool* o *pot*, e poi spedirli nuovamente a più indirizzi[188]. Questo tipo di operazione potrà essere gestita mediante contratti *smart* in grado di agevolare le operazioni di *layering* virtuale che, come si è detto, sollevano non poche problematiche sul piano dell'accertamento del dolo di concorso del programmatore nel reato di riciclaggio commesso dai fruitori del servizio[189].

Per garantire un servizio di *mixing* efficiente esistono alcuni sistemi di pagamento virtuale concepiti *by design* per impedire la ricostruzione del flusso di transazioni[190]. L'aumento degli scambi di questi valori [191] è un dato certamente allarmante poiché funge da cartina di tornasole per una analisi quantitativa delle transazioni illecite.

A differenza del *trading* – attività della cui liceità, pure prima che fosse introdotto un particolare regime autorizzatorio[192], nessuno ha mai dubitato – quella di *mixing* è avvolta da un'aura tale di sospetto sull'impiego a fini criminosi (in particolare al fine di ostacolare l'identificazione della provenienza dei flussi di valuta virtuale), da poter essere considerata in sé intrinsecamente illecita. Non si vede infatti per quale altra ragione un utente debba avvertire la necessità di ricorrere ad un siffatto servizio, se non al fine di disperdere le tracce di una operazione economica o di un flusso di denaro. Esistono, in realtà, alcuni *software* potenzialmente *dual-use* che, pur avendo come effetto quello di "mixare" le transazioni, perseguono una finalità socio-economica (almeno apparentemente) lecita. Si era addotto l'esempio del programma per la raccolta di fondi a scopo benefico, in cui il *mixing* serve a preservare l'anonimato dei contribuenti[193]. In tal

[188] Un tipico sistema di *mixing* si avvale, quindi, di almeno quattro categorie di conti che assolvono funzioni diverse: di ingresso (gateway o di deposito*), bounce, pool* e di uscita (*withdrawing*).

[189] Ma qui un *dolo del fatto*, poiché il programmatore non è in grado di predeterminare *ex ante* se lo *smart contract* verrà attivato e, soprattutto, se sarà strumentalizzato per fini di riciclaggio (*amplius*, Cap. II, § 3.1).

[190] Per garantire l'anonimato e la non tracciabilità delle transazioni il protocollo informatico di Monero è stato impostato al fine di non rendere possibile affermare che il destinatario del flusso di denaro sia un'unica persona (non associabilità – *unlinkability*) e non rendere possibile affermare che vi sia stato scambio di denaro fra gli stessi (non tracciabilità – *untraceability*). Per gli opportuni approfondimenti bibliografici sia consentito rinviare a CALZONE O., *Servizi di mixing e Monero*, in *Gnosis*, 28 luglio 2017, disponibile sul sito internet istituzionale del SISR https://sicurezzanazionale.gov.it

[191] A luglio del 2017 Monero ha raggiunto ha una capitalizzazione di quasi seicento milioni di dollari statunitensi, così figurando tra le prime dieci criptovalute in circolazione.

[192] Tra le novità introdotte dal D. Lgs. 90/2017 vi è anche quella di aver introdotto un comma 8-*bis* all'art. 17-*bis* del D. Lgs. 13 agosto 2010 n. 141, che prevede l'obbligo per i cambiavalute virtuali di iscriversi in un registro costituito presso l'Organismo di cui all'art. 128-*undecies* TUB. Tale obbligo è stato esteso, con l'entrata in vigore del D. Lgs. 125/2019 anche ai prestatori di servizi di portafoglio digitale (Cfr. *supra*, § 3.4.).

[193] Cfr. Cap. II, § 3.3. a proposito delle problematiche sollevate dal *dual use smart contract.*

caso il *software* potrebbe essere utilizzato anche per scopi leciti, sicché l'accertamento della responsabilità del *provider* a titolo di concorso dipenderà dai margini applicativi del dolo eventuale[194].

3.4. Valute virtuali e prevenzione del riciclaggio: dal D. Lgs. 90/2017 alla direttiva 2018/843/UE.

L'ampia premessa sul fenomeno del *cyberlaundering* ci consente ora di passare all'esame dei profili più strettamente connessi alla prevenzione del riciclaggio e, in particolare, delle disposizioni introdotte dal D. Lgs. 27 maggio 2017, n. 90. Con esso il legislatore, giocando addirittura d'anticipo rispetto alle istituzioni dell'Unione Europea, ha adeguato la disciplina antiriciclaggio ai nuovi rischi derivanti dalla dimensione virtuale dell'economia[195].

Oltre ad aver definito le valute virtuali[196], l'intervento riformatore ha toccato numerose disposizioni del Decreto Legislativo 21 novembre 2007, n. 231; tra le novità più rilevanti spicca l'inclusione dei prestatori di servizi relativi all'utilizzo di valuta virtuale tra i destinatari degli obblighi antiriciclaggio. L'art. 1, comma 2, lett. ff) del D. Lgs. 21 novembre 2007 n. 231 definisce questi ultimi 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»*[197].

Gli intermediari professionali del mercato valutario virtuale erano inseriti nel novero degli operatori non finanziari di cui all'art. 3, comma 5, solo *«limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso»*[198], prima che con la recente novella legislativa, l'ambito oggettivo fosse

---

[194] È questo un tema già affrontato *funditus* in altra sede, alla quale si rinvia per ogni opportuno approfondimento (v. nota precedente).

[195] In dottrina v. ACCINNI, *Profili di rilevanza penale delle "criptovalute",* cit. 20; STURZO, *Bitcoin e riciclaggio 2.0*, cit., 27; LUCEV R., BONCOMPAGNI F., *Criptovalute e profili di rischio penale nella attività degli exchanger*, in *Giurisprudenza Penale Web*, 2018, 3.

[196] Sulla definizione di valuta virtuale v. *amplius*, § 2.2.

[197] Anche tale definizione è stata interpolata dal D. Lgs. 125/2019 che, con il chiaro intento di ampliarne la portata applicativa, ha coniato la seguente nozione: prestatori di servizi relativi all'utilizzo di valuta virtuale: *«ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute»*.

[198] L'art. 3 riporta una lunga lista di soggetti obbligati, distinguendo tra operatori finanziari, non finanziari e prestatori di servizi di gioco. Per quel che qui rileva, la lettera i) del quinto comma prevede che rientrino «*nella categoria di altri operatori non finanziari: […] i prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso»*. Con l'entrata in vigore del D. Lgs. 125/2019 anche i "prestatori di servizi di portafoglio digitale" sono entrati a far parte della categoria degli operatori non finanziari (lett. i-*bis*); è stato inoltre soppressa la limitazione all'attività prestata dai cambiavalute virtuali, con la

ampliato a tutti i prestatori di servizi, tra cui anche i *wallet provider*. La scelta di collocare detti intermediari tra gli operatori non finanziari poteva essere intesa come un segnale della volontà di escludere implicitamente la natura finanziaria delle valute virtuali, prima che il legislatore, tornando su suoi passi, emendasse la relativa nozione includendovi anche le rappresentazioni digitali di valore utilizzate per finalità speculative[199].

Nella formulazione previgente alcuni operatori non finanziari[200] erano già gravati dagli obblighi di adeguata verifica della clientela, di registrazione e conservazione della documentazione e di segnalazione delle operazioni sospette; l'elencazione era tuttavia tassativa e non prendeva in considerazione l'attività degli *exchange*. Deve notarsi che tra i destinatari della disciplina non rientrano tutti i fornitori di servizi connessi all'utilizzo delle valute virtuali, ma soltanto i cambiavalute virtuali. Secondo alcuni autori ciò sarebbe indicativo della volontà di delimitare il campo di applicazione del D. Lgs. 231/2007 alle sole «*aree di diretta interferenza delle valute virtuali con le monete correnti e l'economia reale*»[201]; secondo altri[202] si tratterebbe di una scelta discutibile in quanto ingiustificatamente restrittiva.

La novella del 2017 ha anche modificato alcune disposizioni del D. Lgs. 13 agosto 2010, n. 141, imponendo agli *exchangers* l'iscrizione in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli Agenti e dei mediatori creditizi; l'intervento del legislatore ha posto fine allo *status* di profonda incertezza sul regime giuridico applicabile all'esercizio nei confronti del pubblico dell'attività di scambio di valori virtuali. Erano infatti stati sollevati alcuni dubbi sulla configurabilità delle ipotesi di abusivismo previste dalla normativa di settore; il tema sarà approfondito nel capitolo successivo, allorché ci occuperemo della tutela penale del mercato finanziario[203].

Dopo circa un anno dalla emanazione del D. Lgs. 90/2017 è stata approvata la quinta direttiva antiriciclaggio con cui il legislatore dell'Unione – nel modificare le disposizioni della direttiva 849/2015 – ha esteso agli operatori professionali sul mercato delle valute virtuali le disposizioni sulla prevenzione del riciclaggio e del finanziamento del terrorismo[204]. Benché la normativa del 2015 avesse aggiornato i

---

conseguenza che oggi sono divenuti destinatari della disciplina tutti i prestatori di servizi connessi all'utilizzo delle valute virtuali.

[199] Sembra che il legislatore abbia voluto mettere n evidenza la funzione di mezzo di scambio della moneta virtuale rispetto ai possibili impieghi finanziari. Si tratta comunque di una classificazione rilevante ai soli fini dell'applicazione delle disposizioni del D. Lgs. 231/2007, che difficilmente potrebbe risolvere la questione relativa alla natura giuridica dei valori virtuali.

[200] Ci si riferisce ai professionisti (art. 12 prev.), ai revisori contabili (art. 13 prev.) e agli altri soggetti (art. 14 prev.), inseriti nella lunga lista dell'art. 3.

[201] In questi termini, DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 87.

[202] Secondo STURZO, *Bitcoin e riciclaggio 2.0*, cit., 30 la scelta di includere tra i destinatari della disciplina soggetti che solo eventualmente figurano come intermediari nella transazione «*non servirà ad affievolire l'elevata minaccia di riciclaggio intrinsecamente presente nelle caratteristiche del bitcoin*».

[203] *Infra*, Cap IV, § 3.1.

[204] Con la presentazione della Proposta di Direttiva 2016/0208 (COD) la Commissione aveva posto in evidenza la improrogabile necessità di inserire i prestatori di servizi connessi alle valute virtuale tra i destinatari della quarta direttiva antiriciclaggio. Così recitava il considerando n. 6 della Proposta, oggi n. 8 della Direttiva: «*È di fondamentale importanza ampliare il campo di applicazione della direttiva*

presidi antiriciclaggio per far fronte alle nuove manifestazioni della criminalità economica, i tempi di elaborazione e di recepimento impedirono di estendere il campo di applicazione anche alla negoziazione pseudo-anonima dei valori virtuali che all'epoca aveva ancora ridotta diffusione[205]. Per questo motivo sul finire del 2015 il Consiglio Europeo sollecitava un nuovo intervento in materia di contrasto al riciclaggio[206] che condusse la Commissione ad elaborare una proposta di modifica della quarta direttiva già in corso di recepimento[207]. La quinta direttiva pone l'accento sulle nuove tendenze con cui i gruppi criminali finanziano la loro attività e sul fatto che «taluni servizi basati sulle moderne tecnologie stanno diventando sempre più popolari come sistemi finanziari alternativi»[208]. Con particolare riguardo alla fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale e di portafoglio digitale, si mette in luce come l'assenza di obblighi di segnalazione delle operazioni sospette e di identificazione dei clienti permetta ai criminali di trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali, dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme. L'esistenza di un regime di favore rispetto agli intermediari nei pagamenti – che invece sono destinatari dei suddetti obblighi – dà luogo a una lacuna intollerabile, oltre che profondamente contradditoria rispetto allo scopo ultimo della normativa antiriciclaggio.

Tra le novità più significative spicca l'inclusione dei *wallet provider* tra i destinatari della disciplina. L'art. 3, punto 19, della direttiva 2015/849/UE, nel testo modificato dall'art. 1, par. 2, lett. d) della direttiva 2018/843/UE, definisce il prestatore di servizi di portafoglio digitale come il «*soggetto che fornisce servizi di salvaguardia*

(UE) 2015/849 in modo da includere le piattaforme di cambio di valute virtuali e i prestatori di servizi di portafoglio digitale. È necessario che le autorità competenti possano monitorare l'uso delle valute virtuali. Ciò consentirebbe un approccio equilibrato e proporzionale, salvaguardando i progressi tecnici e l'elevato livello di trasparenza raggiunto in materia di finanziamenti alternativi e imprenditorialità sociale».

[205] Il tema delle valute virtuali aveva da poco cominciato ad essere oggetto di attenzione da parte di alcuni organismi sovranazionali e autorità nazionali (v. *supra*, § 2.1); nella coscienza collettiva non era ancora percepito il pericolo di uno sfruttamento sistematico del sistema monetario virtuale a fini di riciclaggio. Il rapporto del Gruppo d'Azione Finanziaria Internazionale (GAFI), *Virtual Currencies – Potential AML/CFT Risks*, del giugno 2014 auspicava un intervento delle istituzioni europee per definire un quadro normativo armonizzato che riservasse a soggetti autorizzati l'esercizio dell'attività di cambiavalute virtuale, mettendo in evidenza i rischi dovuto all'anonimato delle transazioni e alla mancanza di norme e di autorità di controllo.

[206] Nella riunione del Consiglio Europeo del 17 dicembre 2015 si discusse, *inter cetera*, delle ulteriori misure da adottare per contrastare il finanziamento del terrorismo e il riciclaggio. Per approfondimenti v. https://consilium.europa.eu

[207] Proposta di direttiva COM 2016/450 del 5 luglio 2016, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. Dopo circa due anni la direttiva è stata approvata seguendo la procedura legislativa ordinaria e dovrà essere recepita dagli Stati membri entro il 10 gennaio 2020.

[208] Così il *considerandum* n. 2 alla direttiva.

di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali»[209].

I fornitori di servizi di portafoglio e di cambio dovranno dunque verificare costantemente l'adeguatezza della clientela, nonché effettuare, laddove ne ricorrano i presupposti, segnalazioni di operazioni sospette alle Autorità nazionali competenti. Non ritenendo però sufficienti tali misure, il legislatore ha auspica che le *Financial Intelligence Unit* (FIU) potranno richiedere ai *provider* tutte le informazioni che consentano di associare gli indirizzi della valuta virtuale alla reale identità del proprietario della stessa[210]. A detto strumento si associa l'ulteriore possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate. A tal fine, il novellato art. 65 della direttiva 2015/843 delega la Commissione a presentare proposte legislative per *«istituire e mantenere una banca dati centrale in cui siano registrate le identità degli utenti e gli indirizzi dei portafogli e a cui possano accedere le FIU, e i moduli di autodichiarazione per gli utenti delle valute virtuali»*.

Deve infine ricordarsi come pochi mesi dopo la pubblicazione della direttiva in esame, il Parlamento europeo abbia approvato due risoluzioni legislative[211] aventi ad oggetto la disciplina vigente sui controlli in materia di denaro contante in entrata ed in uscita dai Paesi europei e l'armonizzazione delle fattispecie penali di contrasto al riciclaggio. In particolare la risoluzione n. 0339 si prefigge l'obiettivo di sollecitare l'utilizzo della competenza dell'Unione in materia penale per stabilire *minimum rules* relative alla definizione dei reati e delle sanzioni. L'attuale clima di fermento legislativo lascia presupporre che il legislatore dell'Unione interverrà nuovamente per rafforzare le strategie di prevenzione e repressione del riciclaggio, in modo da stare al passo con le sfide lanciate dal progresso tecnologico e dall'evoluzione dei fenomeni criminosi.

3.5. La responsabilità degli intermediari professionisti per concorso in riciclaggio.

[209] Con il D. Lgs. 4 ottobre 2019, n. 125 il legislatore italiano ha apportato modifiche ed integrazioni al D. Lgs. 25 maggio 2017, n. 90 in modo da rendere la normativa italiana aderente agli obblighi derivanti dalla quinta direttiva antiriciclaggio. Per quel che qui interessa, è stata introdotta la seguente definizione di prestatore di servizi di portafoglio digitale: *«ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali»* (art. 1, comma 2, lett. ff)-*bis* D. Lgs. 231/2007).

[210] Il *considerandum* n. 9 prevede che, per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria *«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»*.

[211] Si tratta delle risoluzioni legislative TA-PROV(2018) n. 0338 e n. 0339 del 12 settembre 2018 sulla proposta di direttiva del Parlamento europeo e del Consiglio sulla lotta al riciclaggio di denaro mediante il diritto penale.

Considerato che le operazioni di scambio e trasferimento di valuta virtuale sono spesso strumentalizzate per fini di riciclaggio, integrando la fattispecie tipica di cui, rispettivamente, agli artt. 648-*bis* e 648-*ter.*1 c.p., ci si chiede a quale titolo potranno essere chiamati a rispondere penalmente anche gli intermediari dei servizi.

Occorre precisare fin da subito che la posizione dei soggetti che convalidano le transazioni resta fuori dal campo d'indagine. Non si pongono infatti particolari questioni nell'escludere la responsabilità concorsuale dei partecipanti alla rete (*miners* o *contributors*)[212]che convalidano le transazioni in modo del tutto casuale[213] attraverso la soluzione di complessi problemi crittografici; il *miner* non può scegliere quali transazioni convalidare né prevedere *ex ante* quali transazioni saranno processate dai loro *computer.* Pertanto, anche nel caso in cui questi avesse stretto accordi per validare una o più transazioni illecite, sarebbe piuttosto improbabile che quest'ultime gli vengano poi attribuite. La responsabilità per riciclaggio dovrebbe dunque circoscriversi a quelle ipotesi – invero piuttosto rare – in cui il validatore disponga di una potenza di calcolo tale da monopolizzare l'intera fase di verifica.

Si dovrà piuttosto riflettere sulla posizione degli intermediari professionisti del mercato, che offrono servizi di scambio di valuta reale per criptomoneta (*exchange*) o di deposito/gestione di valori (*wallet provider*). A seguito dei recenti interventi di riforma l'attività svolta da questi soggetti è stata sottoposta a un particolare regime giuridico che, come vedremo, non è privo di effetti sul piano della responsabilità.

Nessun dubbio sul fatto che l'intermediario debba rispondere di concorso in riciclaggio (art. 648-*bis*, 110 c.p.) qualora abbia dolosamente agevolato la condotta del terzo non autore né concorrente nel reato presupposto. Per consolidata giurisprudenza di legittimità non occorre che il soggetto attivo del reato presupposto sia individuato o individuabile, in quanto il fondamento del riciclaggio è la provenienza del denaro o dell'utilità da un delitto anteriore, ancorché non accertato giudizialmente[214]. È dunque sufficiente che il delitto presupposto risulti – alla stregua degli elementi di fatto acquisiti ed interpretati secondo logica – almeno astrattamente configurabile. L'art. 648-*bis* c.p. non richiede particolari cointeressenze fra l'autore del delitto presupposto, il riciclatore e gli eventuali concorrenti nel reato, e neppure la necessaria conoscenza fra questi soggetti. Il reato potrà dunque perfezionarsi anche qualora i membri che compongono la filiera ignorino l'identità dei soggetti a monte e di quelli a valle: ciò

[212] Nelle *blockchain* pubbliche i *miners* mettono a disposizione dell'infrastruttura decentralizzata uno o più computer con elevata potenza di calcolo (*mining rigs*), contribuendo, mediante la risoluzione di complessi calcoli matematici finalizzati alla convalida di diverse transazioni, all'emissione di nuovo circolante virtuale; nelle *blockchain permissioned* parzialmente decentralizzate l'ammontare di valuta è tendenzialmente fisso, sicché la loro opera consiste nella sola convalida delle transazioni, remunerata attraverso i costi di transazione.

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

[214] Sul punto, *ex plurimis*, Cass. Pen., Sez. II, 07 gennaio 2011, n. 546; Sez. II, 16 aprile 2010 n. 18607;

che conta è che ciascuno di essi sia consapevole della provenienza illecita dei beni e che volontariamente si presti a sostituirli, trasferirli o compiere su di essi altre operazioni in modo da ostacolare l'identificazione della loro provenienza delittuosa[215].

Circa l'elemento oggettivo del concorso in riciclaggio non si ravvisano particolari criticità, essendo sufficiente l'aver prestato un contributo materiale o morale alla commissione del reato, secondo le regole ordinarie in materia di concorso di persone nel reato.

Decisamente più complesso stabilire a quale titolo dovrà rispondere l'*exchange* o il *wallet provider* che concorre con l'autore del delitto presupposto. L'introduzione dell'art. 648-*ter.1* c.p. ha sollevato non pochi dubbi sulla possibilità di ravvisare nel fatto dell'*extraneus* che fornisca un contributo morale o materiale un concorso in autoriciclaggio ovvero la più grave fattispecie di riciclaggio[216].

La questione, particolarmente discussa in dottrina, è stata recentemente risolta dalla Corte di Cassazione[217] che ha escluso che nel fatto dell'*extraneus* che ponga in essere la condotta tipica di autoriciclaggio ovvero contribuisca alla realizzazione della stessa da parte dell'*intraneus* sia ravvisabile un'ipotesi di concorso di persone nel reato *ex* art. 110 c.p. In tale ipotesi, dunque, mentre l'*intraneus* risponderà di autoriciclaggio, la condotta dell'*extraneus* non potrà che essere ricondotta alla più grave fattispecie riciclatoria prevista e punita dall'art. 648-*bis* c.p.[218]

Se sul piano oggettivo non si pongono dunque particolari problemi, giacché la condotta del *provider* si traduce in una agevolazione del fatto altrui, l'accertamento dell'elemento soggettivo dà luogo a criticità degne di nota[219]. Nel caso in cui il fornitore del servizio si rappresenti soltanto l'eventualità dell'origine delittuosa del denaro, si porrebbe il problema di una sua responsabilità a titolo di dolo indiretto. Sul punto la

---

[215] In altre parole, ciò che conta è che emerga l'esistenza di un delitto non colposo presupposto, ancorché delineato solo per sommi capi quanto alle esatte modalità di sua commissione, senza che sia necessario identificarne con precisione il soggetto passivo e, anzi, senza che sia indispensabile neppure l'accertamento dell'esatta tipologia del delitto presupposto, essendo sufficiente che sia raggiunta la prova logica della provenienza illecita delle utilità oggetto delle operazioni compiute (cfr. Cass. Pen., Sez. V, 21 maggio 2008 n. 36940; Sez. II, 07 gennaio 2011, n. 546).

[216] In dottrina, v. BRUNELLI D., *Autoriciclaggio: profili del concorso di persone*, in MEZZETTI E.-PIVA D., *Punire l'autoriciclaggio: come, quando e perché*, Torino, 2016, 19 ss.; GULLO A., *Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato*, in *Dir. Pen. Cont. – Riv. Trim*, 2018, 6, 262 ss.; CAVALLINI, TROYER, *Apocalittici o integrati? Il nuovo reato di auto riciclaggio*, cit., 104; BASILE E., *L'autoriciclaggio nel sistema penalistico di contrasto al* money laundering *e il nodo gordiano del concorso di persone*, in *Cass. Pen.*, 2017, 1277 ss.; DE FRANCESCO G., *Riciclaggio ed autoriciclaggio: dai rapporti tra le fattispecie ai problemi di concorso nel reato*, in *Dir. pen. proc*., 2017, 7, 944 ss.

[217] Cass. Pen., Sez. II, 17 gennaio 2018, n. 17235. La Corte definisce l'ambito applicativo delle fattispecie di riciclaggio e autoriciclaggio, muovendo dalla *ratio* sottesa all'introduzione dell'art. 648-*ter*. 1 c.p, richiamando alcune ipotesi codicistiche di diversificazione del titolo di reato tra i concorrenti (es. il rapporto tra evasione e procurata evasione).

[218] Per un commento critico v. GULLO., *Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato*, cit., 265.

[219] Ovviamente *nulla quaestio* nel caso in cui vi sia stato un previo accordo avente ad oggetto la conversione di denaro sporco, ipotesi in cui si configurerebbe una responsabilità a titolo di dolo diretto.

giurisprudenza[220] ritiene sufficiente la sussistenza del dolo eventuale, figura che, nel caso che ci occupa, potrebbe facilmente essere piegata verso schemi di accertamento presuntivo. Il rischio è infatti quello di ritenere l'intrinseca pericolosità dei valori virtuali un elemento sintomatico della consapevolezza dell'origine delittuosa dei fondi e dell'accettazione del rischio di concorrere con l'autore del reato presupposto.

Per rifuggire da automatismi applicativi l'imputazione del fatto a titolo di dolo eventuale dovrebbe seguire le cadenze delineate dalla più recente giurisprudenza di legittimità[221]. Non può tuttavia tacersi come il paradigma di accertamento dettato dalle Sezioni Unite in materia di ricettazione sia troppo rigoroso, poiché nessun fornitore del servizio acquisterebbe mai denaro nella consapevolezza – *idest* certezza soggettiva – della sua provenienza delittuosa[222].

Inoltre, il *provider* a cui sia ascrivibile una mera colpa non potrebbe rispondere eventualmente della contravvenzione di cui all'art. 712 c.p., posto che quest'ultima fattispecie si riferisce all'acquisto di *cose* che si abbia motivo di sospettare provengano da reato. Non potendo la valuta virtuale – per i motivi che abbiamo accennato in precedenza e che saranno ripresi più avanti[223] – essere considerata una cosa, viene meno la possibilità di applicare la fattispecie di incauto acquisto.

3.5.1. La responsabilità dell'*exchange provider* per concorso omissivo in riciclaggio. Rinvio.

Affrontando il tema della responsabilità omissiva del *provider* nella tenuta dei sistemi informatici decentralizzati, si era fatto cenno all'esistenza di una posizione di garanzia derivante dall'assoggettamento alla normativa antiriciclaggio[224]. Dagli

---

[220] Da ultimo v. Cass. Pen., sez. II, 5 giugno 2015, n. 27806, in *Guida al diritto*, 2015, 44, 78 ss. secondo cui la consapevolezza dell'agente in ordine alla provenienza dei beni da delitti «*può essere desunta da qualsiasi elemento e sussiste quando gli indizi in proposito siano così gravi e univoci da autorizzare la logica conclusione che i beni ricevuti per la sostituzione siano di derivazione delittuosa specifica, anche mediata*» e ciò anche perché, nel riciclaggio *«è sufficiente anche il dolo eventuale, che si configura quando l'agente si rappresenta la concreta possibilità, accettandone il rischio, della provenienza delittuosa dei beni ricevuti*» In argomento, ACCINNI, *Profili di rilevanza penale delle criptovalute,* cit., 27.

[221] Il riferimento è in particolare alla nota pronuncia delle Sezioni Unite sulla compatibilità del dolo eventuale con il delitto di ricettazione: Cass. Pen., Sez. Un., 26.11.2009, n. 12433, *Nocera* (*amplius,* a proposito degli *smart contract dual-use*, v. Cap. II, § 3.3). Pertanto, l'elemento volitivo del dolo eventuale dovrà resistere al sillogismo logico, secondo cui l'operatore che ha prestato il servizio avrebbe convertito o trasferito valute virtuale anche se avesse avuto la certezza della provenienza illecita della provvista (sono evidenti le ricadute pratiche di questo principio sull'attività svolta dai fornitori di servizi connessi all'utilizzo di valuta virtuale).

[222] Il fornitore di servizi che, nel dubbio sulla provenienza delittuosa del denaro, decida comunque di dar corso all'operazione dovrebbe dunque andare esente da pena, qualora non sia possibile superare la suddetta prova di resistenza. All'opposto, vi è il rischio di una dilatazione applicativa del dolo eventuale sulla base di indici rilevatori *in re ipsa* (ad esempio, l'accettazione per il cambio di valute che garantiscono un più alto grado di anonimato, l'assenza di controlli, la reiterazione delle operazioni di cambio da parte dello stesso utente etc.).

[223] Sulla nozione penalistica di cosa v. *infra,* § 5.2.

[224] *Supra,* Cap. II, § 6.6. al quale si rinvia per gli opportuni approfondimenti.

obblighi previsti dal Titolo II del D. Lgs. 231/2007 deriva, a nostro avviso, un potere/dovere impeditivo rilevante ai sensi dell'art. 40, comma 2, c.p. in capo al fornire di servizi di cambio (*exchange provider*) e al gestore di portafoglio elettronico (*wallet provider*). Non vi è infatti alcun dubbio sulla volontà del legislatore di responsabilizzare gli intermediari professionisti al preciso fine di prevenire lo sfruttamento della finanza virtuale a fini di riciclaggio, né sulla possibilità per costoro di attivarsi per bloccare i trasferimenti illeciti di fondi o le operazioni manifestamente illecite.

Ciò posto ci si potrebbe domandare, relativamente alla posizione dei fornitori di servizi di portafoglio, se l'obbligo giuridico di impedire l'evento possa derivare da una normativa comunitaria in attesa di recepimento. Le modifiche apportate dal D. Lgs. 90/2017 hanno infatti riguardato i soli cambiavalute virtuali, mentre si attende un intervento del legislatore per includere i *wallet provider* tra i destinatari degli obblighi antiriciclaggio. Non vi è dubbio sul fatto che la direttiva 2015/849/UE, come recentemente modificata, imponga agli Stati obblighi precisi e dettagliati per la protezione degli interessi finanziari dell'Unione. Da ciò non potrebbe tuttavia dedursi la natura *self-executing* della stessa poiché la giurisprudenza ammette la diretta applicabilità soltanto a favore dei cittadini, quando la normativa comunitaria attribuisca diritti soggettivi tutelabili davanti al giudice nazionale. Sarà dunque necessario un atto di recepimento interno perché possa affermarsi l'esistenza di un obbligo giuridico impeditivo.

3.5.2. Intestazione fittizia di *asset* virtuali e trasferimento fraudolento di valori. Incertezze applicative e aporie sistematiche.

L'art. 4 del D. Lgs. 1 marzo 2018, n. 21 sulla riserva di codice ha inserito all'art. 512-*bis* c.p., il delitto di trasferimento fraudolento di valori, già previsto all'art. 12-*quinquies* D.L. 306/1992 e trasfuso senza modifiche tra i delitti contro l'economia pubblica[225]. La disposizione punisce con la reclusione da due a sei anni *«chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre*

[225] In dottrina sul tema v. MUCCIARELLI F., *Commento all'art. 12 quinquies d.l. 8/6/1992 n. 306*, in *Legislazione penale*, 1993, 160; PALAZZI M., *I rapporti tra il delitto di autoriciclaggio e quello di trasferimento fraudolento di valori*, in MEZZETTI, PIVA (a cura di), *Punire l'autoriciclaggio*, cit., 55 ss.; DINACCI E., voce *Trasferimento fraudolento di valori*, in *Enciclopedia giuridica Treccani*, 2018, § 1 ss.; BALSAMO, A., DE AMICIS, G., *L'art. 12-quinquies della legge n. 356/1992 e la tutela del sistema economico contro le nuove strategie delle organizzazioni criminali: repressione penale "anticipata" e prospettive di collaborazione internazionale*, in *Cass. Pen.*, 2005, 5, 2075. Il delitto fu introdotto all'indomani delle stragi del 1992 sicché l'*intentio legis* era quella di contrastare in maniera più energica il fenomeno mafioso, impedendo l'accumulo di capitali illeciti. In realtà la fattispecie contiene un riferimento soltanto indiretto alla criminalità organizzata di tipo mafioso, dato dal richiamo alle leggi in materia di misure di prevenzione patrimoniali che, all'epoca, si applicavano esclusivamente agli «*indiziati di appartenere ad associazioni di tipo mafioso, alla camorra o ad altre associazioni*» (art. 1 della legge 31 maggio 1965, n. 575). Oggi il perimetro applicativo è ben più ampio e ricomprende anche a tutti i soggetti destinatari delle misure di prevenzione personale (sospettati di crimini economici e di delitti commessi con finalità di terrorismo, cfr. artt. 1, 4, 16, D. Lgs. 6 settembre 2011, n. 159).

utilità al fine di eludere le disposizioni di legge in materia di misure prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter del codice penale». Con l'incriminazione di tali condotte il legislatore anticipa la soglia di rilevanza penale di condotte prodromiche al riciclaggio e all'elusione delle misure di prevenzione patrimoniale, sanzionando la simulazione soggettiva come fatto dotato di autonomo disvalore penale e creando in tal modo una sorta di mescolanza tra prevenzione e repressione penale[226]. Senza scendere nel merito degli elementi costitutivi del reato, ci limiteremo qui a dar conto dei punti di contatto tra il trasferimento fraudolento di valori e i delitti commessi mediante l'utilizzo delle valute virtuali.

Emerge *prima facie* dalla lettura della disposizione come l'oggetto materiale del reato sia lo stesso degli artt. 648-*bis* ss. c.p.; ne deriva, alla stregua di quanto in precedenza osservato, che il reato potrà configurarsi anche mediante la fittizia intestazione di valori virtuali (che pacificamente rientrano nel concetto di "altra utilità"). La rilevanza penale di simili condotte appare coerente con la finalità perseguita dal legislatore con l'estensione della disciplina preventiva del riciclaggio agli intermediari professionisti sul mercato valutario virtuale; il sistema dei controlli cadrebbe di fatto nel vuoto se i criminali potessero liberamente servirsi di prestanome ripulire i capitali illeciti.

Emergono tuttavia alcune questioni critiche relative alla punibilità del terzo intestatario e dell'intermediario finanziario (fornitore di servizi di scambio o di portafoglio) che non abbia accertato la reale identità del cliente del servizio. L'art. 512-*bis* descrive una operazione negoziale di natura simulatoria che si perfeziona tra colui che realizza l'intestazione fittizia e un terzo che, consapevolmente, ne accetta il ruolo[227]; ci si è chiesti se il partecipe necessario sia assoggettabile alle norme in tema di concorso di persone nel reato (art. 110 ss. c.p.). La giurisprudenza di legittimità ha ritenuto punibile anche l'intestatario fittizio[228], posizione che non è andata esente da condivisibili critiche per violazione del principio di tassatività. Non meno controverso è il rapporto con le fattispecie di riciclaggio, specie alla luce dell'introduzione dell'art. 648-*ter*.1 c.p. La norma si apre con la clausola di salvaguardia *«salvo che il fatto costituisca più grave reato»* che esclude la punibilità *ex* art. 512-*bis* dell'autore e dei concorrenti nel delitto di riciclaggio. Più complesso il rapporto con l'autoriciclaggio giacché nelle ipotesi contemplate dal secondo comma dell'art. 648-*ter.1*, la cornice

[226] DINACCI, *Trasferimento fraudolento di valori*, cit., § 1

[227] Ciò è reso evidente dalla stessa lettera della legge che punisce chi *«attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro».* Secondo la dottrina maggioritaria si tratta di un reato plurisoggettivo improprio o a punibilità circoscritta. Il legislatore sanziona la condotta simulatoria senza replicare la sanzione per l'intestatario, forse per ragioni di politica criminale date dalle maggiori possibilità di rompere il sodalizio criminoso tra i due soggetti e di ottenere la collaborazione del terzo intestatario.

[228] *Ex plurimis*, Cass. Pen., Sez. I, 28 febbraio 2013, n. 14373

edittale non supera quella del trasferimento fraudolento di valori[229]. Si pensi al caso in cui l'autore del reato presupposto trasferisca sul conto virtuale intestato a un terzo, esercente un'impresa, valori virtuali derivanti dalla commissione, ad es., di una frode informatica con l'intesa che dopo un determinato lasso di tempo questi dovrà restituirli al mittente. A nostro avviso andrebbe esclusa l'ammissibilità di un concorso formale tra le due fattispecie, che presentano degli elementi strutturali profondamente diversi: da un lato si punisce la mera intestazione fittizia, dall'altro l'effettivo impiego in attività economiche. Nel caso esemplificato dunque si dovrà accertare se il trasferimento dei valori sul conto del terzo fosse preordinato all'impiego del capitale nell'impresa ovvero alla mera simulazione soggettiva: nel primo caso il soggetto risponderà per autoriciclaggio; nel secondo caso per trasferimento fraudolento di valori. Sembra dunque possibile ricostruire le due fattispecie in termini di progressione criminosa poiché la realizzazione del concreto ostacolo alla identificazione della provenienza illecita non richiesto nella condotta di intestazione fittizia. Non è dello stesso avviso la Corte di Cassazione che ha di recente riconosciuto l'ammissibilità del concorso tra intestazione fittizia ed autoriciclaggio dal momento che quest'ultimo *«non presuppone né implica che l'autore di essa ponga in essere anche il trasferimento fittizio ad un terzo dei cespiti rivenienti dal reato presupposto»*[230].

Emerge peraltro una *défaillance* legislativa nella determinazione dei limiti edittali poiché le condotte concretamente idonee a ostacolare l'identificazione della provenienza delittuosa del denaro (che ledono, *inter cetera*, la libera concorrenza del mercato) sono punite di meno rispetto alla pura e semplice intestazione fittizia. In entrambi i casi il terzo interposto potrà rispondere del più grave reato di riciclaggio di cui all'art. 648-*bis* c.p. ove siano integrati tutti gli elementi costitutivi. La punibilità a questo titolo non desta particolari problemi nel caso in cui l'autore del delitto presupposto sia punito *ex* art. 648-*ter*.1 c.p[231]. Decisamente più problematico la divisione dei titoli di responsabilità nel caso in cui il soggetto che effettua l'intestazione risponde *ex* art. 512-*bis*: in questo caso a fronte di una condotta dal disvalore omogeneo (trasferimento e ricezione di valori con patto di simulazione) l'intestatario potrà essere chiamato a rispondere di un reato con limiti edittali raddoppiati rispetto al trasferimento fraudolento di valori[232].

L'intestazione fittizia consiste nella creazione di una situazione di apparente signoria sulla cosa che può realizzarsi mediante qualunque espediente negoziale, purché vi sia alla base del regolamento contrattuale un patto simulato con cui le parti concordano circa la titolarità del bene (almeno in parte) in capo al dante causa. Nel

[229] Così recita il secondo comma: *«Si applica la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni».*

[230] Cass. Pen., Sez. II, 12 gennaio 2017, n. 3935, in *Cass. Pen.*, 2017, 5, 1956 ss.

[231] Si veda in tal senso la *querelle* giurisprudenziale sul concorso dell'*extraneus* in autoriciclaggio, *supra*, § 3.2.

[232] La pena base prevista dall'art. 648-*bis* va da quattro ai dodici anni, a fronte della reclusione da due a sei anni comminata dall'art. 512-bis.

caso dell'intestazione fraudolenta di valuta virtuale il mittente attribuisce al terzo fiduciario la disponibilità delle somme, perdendo ogni possibilità di controllo delle stesse; soltanto nel caso in cui il destinatario condivida le chiavi crittografiche private con il mittente si avrà una ipotesi di contitolarità di fatto. Per aversi intestazione fittizia è necessario che le unità di conto virtuale siano registrate su conti nominativi o su *account* privati di piattaforme di gestione o scambio; la precisazione non appare superflua, tenuto conto delle note caratteristiche di anonimato delle transazioni in valuta virtuale. Laddove l'operazione consista in un mero trasferimento di fondi *peer-to-peer* non vi è alcuna sfasatura tra *apparentia iuris* e volontà delle parti, poiché gli identificativi non compaiono se non in forma di indirizzi alfanumerici sulla *blockchain*. Diverso è il caso in cui i valori siano accreditati su conti accesi presso fornitori di servizi di portafoglio elettrico o piattaforme di scambio, soggetti obbligati *ex lege* a identificare la clientela ai sensi del D. Lgs. 90/2017 e della Direttiva 2018/843/UE. Con questi provvedimenti il legislatore ha inteso superare della barriera dell'anonimato sfruttando l'attività svolta dagli intermediari per imporre gli obblighi tipici della disciplina preventiva del riciclaggio. Ecco che l'intestazione fittizia dei valori diviene un espediente utile per eludere i controlli incrociati e la segnalazione delle operazioni sospette. L'intermediario finanziario, in quanto soggetto destinatario degli obblighi, dovrà assolvere con diligenza al compito di identificare i clienti del servizio. Risulta piuttosto arduo ipotizzare un concorso omissivo in trasferimento fraudolento di valori (artt. 110, 512-*bis* c.p.) da parte dell'intermediario che, essendo a conoscenza del carattere simulato dell'operazione, non abbia dato corso alle segnalazioni previste dagli artt. 17 ss. D. Lgs. 231/2007. A tal fine dovrà accertarsi l'esistenza di un dolo particolarmente intenso in capo al garante, non essendo sufficiente l'accettazione del rischio della provenienza delittuosa dei fondi o dell'intestazione di comodo dei capitali[233]. L'intermediario finanziario dovrà, in altre parole, essere consapevole dell'interposizione soggettiva nel momento di instaurazione del rapporto con l'intestatario fittizio e del fatto che l'apertura del conto è preordinata all'elusione delle misure di prevenzione o al compimento di fatti di riciclaggio. In quest'ultima ipotesi si ritiene che l'intermediario debba rispondere a titolo di dolo diretto nel più grave reato di riciclaggio commesso dal cliente in forza della clausola di riserva contenuta in apertura della fattispecie. Laddove invece sussista un mero *status* di dubbio sulla provenienza delittuosa dei fondi e sulla effettiva titolarità degli stessi, l'affermazione di responsabilità penale del concorrente dovrà seguire lo schema delineato dalla più recente giurisprudenza di legittimità[234].

[233] Il trasferimento fraudolento di valori è punito se commesso *«al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter»*. Una tale proiezione finalistica risulta, a nostro avviso, difficilmente compatibile con la componente volontaristica del dolo eventuale.

[234] La questione è stata esaminata in apertura del paragrafo a proposito del concorso dell'*exchange provider* in riciclaggio (v. *supra*, § 3.5).

3.6. Cenni sulla tutela penale secondaria e sull'apparato sanzionatorio amministrativo per le violazioni della disciplina preventiva del riciclaggio. L'introduzione di una ipotesi speciale di confisca.

La novella del 2017 ha apportato modifiche significative all'apparato sanzionatorio del D. Lgs. 231/2007, con l'intento di ricondurre nell'alveo del penalmente rilevante le sole violazioni caratterizzate da particolare gravità[235]. I primi commentatori[236] della riforma ritengono che la volontà del delegante sia stata attuata con la revisione delle fattispecie che compongono l'art. 55. I primi tre commi puniscono come delitto le condotte caratterizzate dall'elemento della fraudolenza, quali la falsificazione dei dati e delle informazioni in violazione degli obblighi di adeguata verifica, l'acquisizione di dati falsi e di informazioni non veritiere in violazione degli obblighi di conservazione, la comunicazione di dati falsi da parte del cliente[237]. È rimasta invece inalterata la contravvenzione prevista dal quarto comma, che punisce la violazione del divieto di comunicazione inerente alla segnalazione di operazioni sospette[238].

Il D. Lgs. 90/2017 ha inoltre depenalizzato le contravvenzioni di omessa e incompleta comunicazione (commi 7 e 8), la cui condotta è oggi confluita all'interno degli artt. 59 e 60. Così facendo il legislatore ha spostato il baricentro dell'appendice sanzionatoria, in linea con i criteri direttivi contenuti nella delega, verso l'illecito amministrativo[239]. Oltre ad avere aumentato il numero delle violazioni sanzionate in via amministrativa (artt. 56-64 D. Lgs. 231/2007), la riforma ha anche disciplinato in modo puntuale il procedimento sanzionatorio e i criteri per l'applicazione delle sanzioni.

Sebbene non strettamente connessa al tema oggetto della nostra trattazione, non potrebbe infine tacersi l'introduzione nel codice di una ipotesi di confisca speciale in caso di condanna o patteggiamento per i delitti di riciclaggio, reimpiego e

---

[235] La legge 12 agosto 2016 n. 170 (Legge di delegazione europea 2015) disponeva che *«al fine di garantire il rispetto dei principi di ne bis in idem sostanziale e di effettività, proporzionalità e dissuasività delle sanzioni irrogate per l'inosservanza delle disposizioni adottate in attuazione della direttiva (UE)2015/849»* il Governo dovesse apportare *«tutte le modifiche necessarie a: 1) limitare la previsione di fattispecie incriminatrici alle sole condotte di grave violazione degli obblighi di adeguata verifica e di conservazione dei documenti, perpetrate attraverso frode o falsificazione, e di violazione del divieto di comunicazione dell'avvenuta segnalazione […] 2) graduare l'entità e la tipologia delle sanzioni amministrative tenuto conto [omissis]»* (art. 15, lett. h).

[236] ACCINNI, *Profili di rilevanza penale delle "criptovalute",* cit. 24 ss.; BEVILACQUA F.C., *Le previsioni sanzionatorie della normativa antiriciclaggio,* in ALESSANDRI A. (a cura di), *Reati in materia economica,* Torino, 2017, 375 ss.

[237] La precedente formulazione dei primi tre commi dell'art. 55 assoggettava a pena anche la mera inosservanza degli obblighi previsti dal Titolo II del decreto; tali ipotesi sono state oggi depenalizzate e trasformate in illeciti amministrativi.

[238] Anche il delitto di uso indebito e falsificazione di carte di pagamento era rimasto inalterato. La fattispecie è confluita all'interno del codice penale (art. 493-*ter* c.p.) a seguito della riforma sulla riserva di codice di cui al D. Lgs. 21/2018.

[239] Quello della depenalizzazione dei reati c.d. di mera inosservanza è opzione che il legislatore ha recentemente intrapreso anche nella riforma dell'appendice sanzionatoria del D. Lgs. 196/2003 per le violazioni in materia di trattamento dei dati personali. Per approfondimenti v. D'AGOSTINO L., *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D. Lgs. 10 agosto 2018, n. 101,* in *Archivio penale*, 2019, 1, 2 ss.

autoriciclaggio. L'art. 648-*quater* c.p. aggiunto dall'art. 5, comma 4, del D. Lgs. 90/2017, prevede che per questi reati debba sempre essere ordinata la confisca dei beni che ne costituiscono il prodotto o il profitto, salvo che appartengano a persona estranea al reato, con la specificazione che, nel caso in cui non sia possibile procedere alla confisca diretta, il giudice sia tenuto a disporla anche nella forma "per equivalente". Quando la misura ablatoria ha come oggetto le valute virtuali emergono alcuni profili problematici relativi alla esecuzione della misura e al *quantum* di profitto confiscabile che ci riserviamo di esaminare nel prosieguo della trattazione[240].

3.7. Valute virtuali e riciclaggio. Uno sguardo all'ordinamento svizzero.

La piazza finanziaria svizzera rappresenta uno dei maggiori centri di interesse degli investitori internazionali, alla base del quale vi era la "ragione storica" della neutralità politica del Paese. Negli ultimi decenni sono tuttavia andate affermandosi altre ragioni, più strettamente connesse alla competitività del mercato elvetico: prelievo fiscale ridotto, solidità e segretezza bancaria, chiarezza del quadro normativo e prevedibilità delle decisioni giudiziarie, garanzie di alto ritorno economico dell'investimento.

Sono note le criticità nei rapporti transfrontalieri tra la Svizzera e gli Stati membri dell'Unione europea, non solo per quel che riguarda la lotta all'evasione fiscale, ma anche il contrasto a fenomeni di riciclaggio di denaro di provenienza illecita. La firma dell'accordo di Schengen sulla libera circolazione delle persone ha contribuito alla integrazione della Confederazione all'interno del mercato unico, mettendo in maggiore evidenza l'opportunità di introdurre limiti al segreto bancario[241]. Ferma la piena collaborazione con le autorità straniere in procedimenti per riciclaggio o frode fiscale, il *punctum pruriens* ha riguardato la semplice evasione fiscale sulla quale per anni Svizzera ed Unione europea hanno negoziato alla ricerca di una soluzione razionale. La questione è sorta a seguito del reiterato rifiuto delle autorità elvetiche di dar corso alle rogatorie internazionali per evasione fiscale che – a differenza dei reati tributari connotati da frode – è soggetta solo a sanzioni amministrative.

In tempi recenti il Governo italiano e il Consiglio federale svizzero hanno firmato un Protocollo di modifica della Convenzione sulle doppie imposizioni[242] che, nel disciplinare lo scambio di informazioni ai fini fiscali in base allo standard OCSE[243],

---

[240] *Infra*, in questo capitolo § 7 e, per i profili inerenti alla esecuzione della misura, Cap. V, § 7.

[241] Secondo la definizione fornita dal Dipartimento federale delle finanze elvetico, il segreto bancario consiste nella protezione della sfera privata dei clienti delle banche da interventi ingiustificati da parte dello Stato (*Der Schutz der Privatsphäre von in- und ausländischen Bankkunden gegenüber ungerechtfertigten Eingriffen des Staates*, cfr. https://efd.admin.ch).

[242] Cfr. Legge 4 maggio 2016, n. 69 di autorizzazione alla ratifica del *«Protocollo che modifica la Convenzione tra la Repubblica italiana e la Confederazione svizzera per evitare le doppie imposizioni e per regolare talune altre questioni in materia di imposte sul reddito e sul patrimonio, con Protocollo aggiuntivo, conclusa a Roma il 9 marzo 1976, così come modificata dal Protocollo del 28 aprile 1978, fatto a Milano il 23 febbraio 2015»*.

[243] In occasione del G20 tenutosi a Londra nel 2009 gli Stati confermarono a propria intenzione di stabilire una base comune di azione per favorire la trasparenza, lo scambio di informazioni e l'abolizione

pone fine al segreto bancario, facilitando la *voluntary disclosure* da parte dei cittadini italiani che hanno conti correnti in Svizzera e consentendo così all'Agenzia delle Entrate di ottenere informazioni su un singolo contribuente, a prescindere dal superamento delle soglie di punibilità penale.

Lo stretto legame intercorrente tra segreto bancario, evasione fiscale e ripulitura dei capitali illeciti è del resto confermato dalla introduzione di una procedura di *voluntary disclosure* con la stessa legge che ha introdotto nel codice penale il delitto di autoriciclaggio, in momento storico in cui già si avvertiva l'approssimarsi del tramonto del segreto bancario svizzero. La tecnica del *carrot-stick*, basata sulla non punibilità per i reati tributari e per i fatti di riciclaggio e reimpiego commessi precedentemente all'attivazione della procedura[244], ha permesso il rientro di oltre 16 miliardi di euro[245].

È curioso osservare che, di pari passo alla progressiva dismissione del segreto bancario, la Svizzera ha incentivato l'utilizzo dei valori virtuali, quasi a voler far rientrare dalla finestra ciò che oramai era uscito dalla porta. Non potendosi dar conto in questa sede, neppure cursoriamente, dell'ampio dibatto che ha accompagnato l'ingresso delle valute virtuali nel sistema finanziario svizzero, ci limiteremo qui ad esaminare gli aspetti più rilevanti per il contrasto al riciclaggio.

Analogamente al sistema italiano, la lotta al fenomeno poggia su due pilastri fondamentali: la repressione penale e la prevenzione amministrativa. Sul primo fronte, il riciclaggio di denaro figura tra i delitti contro l'amministrazione della giustizia; l'art. 305-*bis* del codice penale svizzero, introdotto dalla legge federale 23 marzo 1990, punisce con la reclusione sino a tre anni o con la multa chiunque compia *«un atto suscettibile di vanificare l'accertamento dell'origine, il ritrovamento o la confisca di valori patrimoniali sapendo o dovendo presumere che provengono da un crimine o da un delitto fiscale qualificato»*. Il secondo comma commina una pena più severa nel caso in cui il delitto ricorra in forma aggravata, ovverosia quando l'autore agisce come membro di un'organizzazione criminale o come membro di una banda costituitasi per esercitare sistematicamente il riciclaggio, oppure realizza una grossa cifra d'affari o un guadagno considerevole facendo mestiere del riciclaggio[246]. Può notarsi come il

---

del segreto bancario. Da allora sia in ambito OCSE che in ambito eurounitario si avviò un intenso dibattito per creare uno standard procedurale uniforme per lo scambio di informazioni. I lavori condussero all'emanazione della Direttiva 2014/107/UE che impone agli Stati membri di adottare il *Common Reporting Standard*, un documento approvato il 17 gennaio 2014 dal Comitato Affari Fiscali dell'OCSE che contiene lo standard globale per lo scambio automatico di informazioni in materia fiscale.

[244] L'art. 5-*quinquies* del decreto legge 28 giugno 1990, n. 167, introdotto dalla legge 15 dicembre 2014 n. 186 stabilisce, in favore del contribuente che collabora mediante la *disclosure* dei capitali detenuti all'estero, la non punibilità per i delitti di cui agli articoli 2, 3, 4, 5, 10-*bis* e 10-*ter* del decreto legislativo 10 marzo 2000, n.74; la non punibilità delle condotte previste dagli articoli 648-*bis* e 648-*ter* del codice penale, commesse in relazione ai delitti sopra indicati. È inoltre prevista la non punibilità, limitatamente alle attività oggetto di collaborazione volontaria, delle condotte di autoriciclaggio commesse in relazione ai reati tributari sino alla data del 30 settembre 2015.

[245] I risultati, reperibili sul sito internet nel Ministero delle Finanze https://finanze.it, evidenziano come oltre il 70% della base imponibile emersa fosse detenuta in Svizzera.

[246] Il reato è punibile anche se commesso all'estero, purché abbia rilevanza penale anche nel luogo in cui è stato compiuto.

trattamento sanzionatorio sia piuttosto mite, se paragonato alla cornice edittale prevista dall'art. 648-*bis* c.p.; è questo un *cliché* ricorrente nel sistema penale svizzero, storicamente caratterizzato da pene detentive che, pur essendo brevi, assolvono egregiamente alla funzione generalpreventiva in virtù della certezza della loro applicazione.

Il presidio penale è rafforzato dalla previsione, al successivo art. 305-*ter*, del delitto di «Carente diligenza in operazioni finanziarie e diritto di comunicazioni», descritto come il fatto di chi *«a titolo professionale, accetta, prende in custodia, aiuta a collocare o a trasferire valori patrimoniali altrui senza accertarsi, con la diligenza richiesta dalle circostanze, dell'identità dell'avente economicamente diritto»*[247]. Trattasi di un reato punito a titolo di colpa la cui struttura, osservata con le lenti del penalista italiano, risulta dalla combinazione di elementi tipici del riciclaggio e della contravvenzione di incauto acquisto (art. 712 c.p.); la disposizione è posta a chiusura del sistema dei delitti di 'consolidamento' contro l'amministrazione della giustizia.

Sul fronte preventivo la legge federale antiriciclaggio[248] impone agli intermediari finanziari il rispetto di precisi obblighi di diligenza e di segnalazione[249]. Il controllo sull'osservanza di tali doveri è attribuito all'Autorità federale di vigilanza sui mercati finanziari (FINMA) e coadiuvata dalle società di audit concessionarie[250]. Anche le società operanti in settori limitrofi a quello bancario (c.d. parabancario) sono soggette alla LRD, a condizione che accettino in deposito o custodiscano a titolo professionale

[247] Il secondo comma precisa che gli operatori professionali hanno il diritto di segnalare all'Ufficio federale di polizia gli indizi che permettono di sospettare che i valori patrimoniali provengono da delitto. La previsione di una espressa causa di giustificazione non è affatto superflua poiché la violazione del segreto bancario da parte degli operatori del settore integra di per sé reato ai sensi dell'art. 47 della legge federale sulle banche e le casse di risparmio del 1934.

[248] Legge federale del 10 ottobre 1997 relativa alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo (Legge sul riciclaggio di denaro, LRD).

[249] Gli obblighi antiriciclaggio previsti dalla LRD possono essere così riassunti: (i) l'intermediario finanziario non può accettare valori patrimoniali che sono palesemente frutto di reati o di atti illeciti; (ii) deve identificare la controparte contrattuale e determinare l'identità degli aventi economicamente diritto sui valori patrimoniali depositati o trasferiti; (iii) nel caso in cui una operazione sia sospetta o si abbia motivo di ritenere che i valori patrimoniali provengono da delitto, si trovano nelle disponibilità di un'organizzazione criminale o sono funzionali al finanziamento del terrorismo, l'intermediario finanziario deve richiedere al cliente maggiori informazioni sul rapporto economico o sulla causa del trasferimento dei valori; (iv) le transazioni ad elevato rischio, superiori a una determinata soglia o dirette verso paesi *off-shore* devono essere debitamente registrate, e su di esse vanno effettuati accertamenti più approfonditi; (v) le transazioni effettuate e i relativi accertamenti devono essere debitamente documentati; (vi) gli intermediari finanziari devono adottare gli opportuni provvedimenti organizzativi interni atti ad evitare attività di riciclaggio di denaro e di finanziamento del terrorismo (tra cui controlli di audit, l'emanazione di direttive interne e la formazione del personale); (vii) se per una relazione d'affari sussiste un sospetto di riciclaggio, l'intermediario finanziario deve sporgere denuncia presso l'Ufficio di comunicazione in materia di riciclaggio di denaro (MROS) facente capo al Dipartimento federale di giustizia e polizia (DFGP). Sul punto v. la Scheda informativa FINMA, *Lotta contro il riciclaggio di denaro: gli intermediari finanziari devono ottemperare agli obblighi di diligenza*, in https://finma.ch

[250] In caso di inottemperanza alle disposizioni dalla Legge sul riciclaggio di denaro, la FINMA può imporre agli intermediari finanziari di attivarsi per ripristinare la legalità. In presenza di casi particolarmente gravi, l'Autorità può disporre accertamenti e adottare ogni provvedimento opportuno, tra cui anche la confisca dei proventi delittuosi.

valori patrimoniali appartenenti a terzi, ovvero che forniscano aiuto al fine di investire o trasferire tali valori[251].

Passando al tema che più interessa l'oggetto della presente trattazione, in recenti comunicati[252] la FINMA ha mostrato grande interesse per il settore *fintech*, in particolare per quel che riguarda la diligenza degli operatori che offrono servizi di pagamento a distanza. Una circolare del 2016[253] ha dettato una disciplina *ad hoc* per l'identificazione degli utenti di servizi finanziari tramite canali digitali la cui osservanza rende l'intermediario finanziario *compliant* con le disposizioni antiriciclaggio.

Sebbene la legge svizzera sui mercati finanziari non regoli l'emissione, lo scambio e l'offerta al pubblico delle valute virtuali, l'Autorità ha chiarito che, a seconda del modello di *business* prescelto, potrebbe essere necessaria una specifica autorizzazione. Nelle linee guida di recente adozione[254] la FINMA ha inoltre sottolineato come la circolazione di detti valori accresca sensibilmente il rischio di riciclaggio e di finanziamento del terrorismo, motivo per cui gli intermediari professionisti del mercato saranno tenuti a osservare le disposizioni delle LRD. Nel dettaglio, rientrano nel campo di applicazione della legge l'offerta di servizi di custodia e pagamento in valute virtuali (*wallet provider*) e la gestione di piattaforme di compravendita (*trading*): gli operatori dovranno dunque registrarsi presso un organismo di autodisciplina o assoggettarsi direttamente al controllo della FINMA, al pari degli intermediari finanziari.

La vigilanza sul mercato *fintech* contribuisce a rendere il sistema finanziario virtuale credibile e più sicuro. Da questa prospettiva la posizione espressa dall'Autorità appare condivisibile, tanto più in considerazione del rilevante numero di imprese *blockchain* aventi sede legale in Svizzera. L'assoggettamento alla normativa

---

[251] Rientrano in questa categoria, ad esempio, le società di credito e di *leasing*, i gestori di circuiti di pagamento, i cambiavalute.

[252] I comunicati sono disponibili al seguente link https://finma.ch/it/autorizzazione/fintech/

[253] Circolare FINMA n. 7/2019 relativa alla «Video identificazione e identificazione online – Obblighi di diligenza all'avvio di relazioni d'affari attraverso i canali digitali», con cui l'Autorità ha chiarito l'estensione degli obblighi antiriciclaggio nel contesto della fornitura di servizi finanziari per via digitale. La circolare equipara la video identificazione all'identificazione *de visu*, purché siano soddisfatti i requisiti di seguito indicati: (i) l'identificazione avviene per mezzo di una comunicazione audiovisiva tramessa in tempo reale, vale a dire in diretta, tra la controparte e l'intermediario finanziario (tale scopo, l'intermediario finanziario impiega supporti tecnici idonei, in grado di garantire una trasmissione sicura dei dati, nonché la lettura e la decifratura delle informazioni nella zona leggibile dalla macchina sul documento d'identità); (ii) la qualità dell'immagine e dell'audio devono essere adeguate al fine di permettere un'identificazione inconfutabile; (iii) l'intermediario finanziario può impiegare supporti tecnici per compensare condizioni di illuminazione difficili, in particolare durante l'esecuzione delle fotografie richieste nell'ambito dell'identificazione; (iv) la registrazione audio va effettuata per l'intera durata del colloquio; (v) durante la trasmissione video, l'intermediario finanziario effettua delle fotografie del cliente, come pure di tutte le pagine rilevanti del documento d'identità, e verifica che le fotografie scattate durante la trasmissione video corrispondano alla fotografia che figura sul documento d'identità.

[254] *Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offering* (ICO), 16 febbraio 2018, ibidem, § 3.6. Il documento è noto anche per aver fornito una classificazione dei *token* virtuali in base alla funzione economica, a partire dalla quale l'Autorità individua le norme di legge astrattamente applicabili.

antiriciclaggio non è tuttavia sufficiente a garantire la tutela degli investitori, poiché, in mancanza di un intervento del legislatore, rimane preclusa ogni possibilità di applicare agli operatori professionali la disciplina in materia di prospetto e offerta a distanza.

Un ultimo importante traguardo è stato raggiunto il 21 settembre 2018 allorché l'Associazione Svizzera dei Banchieri[255] ha pubblicato una guida pratica, destinata ai suoi membri, concernente l'apertura di conti aziendali per le imprese *blockchain*, iniziativa fortemente sostenuta dalla FINMA in virtù di un rapporto di leale collaborazione tra *fintech* e sistema bancario tradizionale[256].

Nonostante gli sforzi profusi dall'Autorità per mitigare il rischio di riciclaggio, occorre dare atto della presenza sul territorio di ATM per la conversione di denaro contante in valuta virtuale costituisce una "valvola di sfogo" che permette ai criminali di evitare il passaggio per gli intermediari del mercato. In questo modo la fase più delicata dell'intero *iter* di ripulitura del denaro – il *placement* – sfugge a ogni possibilità di controllo statale.

3.8. Considerazioni finali.

La regolazione del mercato delle valute virtuali rappresenta un'autentica sfida per i legislatori nazionali, chiamati oggi a confrontarsi con un fenomeno vastissimo e tecnicamente assai complesso[257]. Le scelte di politica normativa dovrebbero essere dirette alla dissoluzione del legame che avvince l'uso delle criptovalute ai più disparati fenomeni criminosi, primo tra tutti il riciclaggio.

Giunti a conclusione dell'indagine sulle nuove frontiere del *cyberlaundering* "via cripto", si ritiene di poter condividere l'opinione di quella parte della dottrina[258] che ha denunciato la necessità di un ulteriore rafforzamento degli strumenti di contrasto, da compiersi non tanto sul piano della tipizzazione di nuove delle fattispecie criminose[259], quanto piuttosto sul terreno della prevenzione e della cooperazione investigativa.

A tal riguardo, non pare potersi dubitare dell'esistenza di una solida base normativa per combattere il fenomeno a livello transnazionale. Non solo la recente Direttiva

[255] Si veda la *Guide pratique de l'ASB pour l'ouverture de comptes d'entreprises pour des sociétés blockchain*, 21 settembre 2018, pubblicata dalla SwissBankIng con il patrocinio della FINMA, https://www.finma.ch

[256] Il sistema bancario elvetico si era mostrato inizialmente scettico dinanzi alla diffusione dei valori virtuali, tanto da impedire l'apertura di conti correnti a nome di società operanti in questo settore. Ciò incideva negativamente sulla competitività del mercato finanziario svizzero, opponendo una resistenza all'ingresso di capitali e investimenti esteri per la compravendita di asset virtuali.

[257] L'aumento vertiginoso del coefficiente di capitalizzazione di questo mercato rende l'intervento regolatorio non più differibile, al fine di garantire una adeguata tutela dell'interesse pubblico alla tracciabilità e alla sicurezza delle transazioni di natura finanziaria.

[258] PICOTTI, *Profili penali del cyberlaundering*, cit., 614

[259] Il legislatore ha forse ecceduto nell'opera di tipizzazione, inserendo nel codice più fattispecie suscettibili di creare problemi di coordinamento. Sul punto v. PICOTTI, *Profili penali del cyberlaundering*, ibidem.

2017/1371/UE obbliga gli stati a punire il riciclaggio che lede gli interessi finanziari dell'Unione (art. 4)[260], ma, guardando più in generale al diritto internazionale, si può notare la presenza di alcune disposizioni pattizie di sicura rilevanza. Benché non espressamente nominato nella Convenzione di Budapest, il *cyberlaundering* rientra tra i delitti commessi, in tutto o in parte, tramite un sistema informatico, per i quali le autorità investigative potranno servirsi degli strumenti di cooperazione previsti dalla Sezione II[261]. Si è inoltre correttamente osservato[262] come il riciclaggio digitale sia un buon candidato per l'inclusione tra i reati transnazionali di cui all'art. 3 della Convenzione di Palermo del 2000 contro la criminalità organizzata[263], che rende attivabili tutti gli strumenti di cooperazione ed assistenza internazionali, anche ai fini della confisca dei proventi del delitto (art. 12) [264].

Rinviando all'ultimo capitolo l'analisi degli strumenti d'indagine e delle forme di collaborazione processuale, ci limiteremo qui a individuare alcuni nuovi possibili ambiti di intervento in chiave di prevenzione.

Se condotto in modo razionale, nel rispetto della duttilità che caratterizza la moneta *peer to peer*, l'intervento statale non produrrà alcun "effetto collaterale", anzi ne sortirà di positivi, rafforzando la stabilità dei prezzi delle valute virtuali e la fiducia che gli utilizzatori ripongono in esse. Il timore che una regolamentazione ancorata su un modello pubblicistico di controllo dell'attività degli intermediari – ricalcata sulla disciplina bancaria e finanziaria – possa imbrigliare eccessivamente il meccanismo di condivisione tra utenti alla base della *distributed ledger technology*, frustrando i vantaggi della disintermediazione e dell'assenza di una Autorità centrale, appare privo di fondamento. Oltre a non esservi alcuna ragione per sottoporre detti soggetti a una disciplina differenziata rispetto a quella degli altri operatori del settore, risulta piuttosto evidente come il passaggio per gli intermediari sia l'unico punto di emersione delle attività illecite commesse mediante i valori virtuali. Se alla *longa manus* dello Stato sfuggisse il controllo sugli unici "portali" di comunicazione tra l'economia reale e la finanza virtuale, aumenterebbe non solo l'enorme cifra nera della *underground economy ma* anche il grado di desensibilizzazione dei criminali nel compimento di reati economici *online*.

---

[260] La direttiva, relativa «alla lotta contro la frode che lede gli interessi finanziari dell'Unione europea mediante il diritto penale», prevede una lista di reati a quali il Regolamento 2017/1939/UE fa riferimento nel determinare la competenza dell'*European Public Prosecutor Office* (EPPO). Per un primo commento, v. BASILE E., *Brevi note sulla nuova Direttiva PIF. Luci ed ombre del processo di integrazione europea in materia penale*, in *Diritto penale contemporaneo*, 12 dicembre 2017.

[261] Cfr. art. 14, par. 2, lett. b) della Convenzione di Budapest sul *cybercrime*.

[262] PICOTTI, *Profili penali del cyberlaundering*, cit., 616

[263] L'art. 6 della Convenzione di Palermo obbliga gli Stati firmatari a punire il riciclaggio di denaro, considerato uno dei crimini finanziari transnazionali per eccellenza.

[264] In dottrina sul tema v. MICHELINI G., POLIMENI G., *Il fenomeno del crimine transnazionale e la Convenzione della Nazioni Unite contro il crimine organizzato transnazionale*, in ROSI E. (a cura di), *Criminalità organizzata transnazionale e sistema penale italiano: la Convenzione ONU di Palermo*, Milano, 2007; di recente ACCILI SABATINI M. A., BALSAMO A., Verso un nuovo ruolo della convenzione di Palermo nel contrasto alla criminalità transnazionale, in *Diritto Penale Contemporaneo – Rivista trimestrale*, 2018, 1, 113 ss.

De lege lata, non può che accogliersi con favore la tempestività con cui il legislatore italiano è intervenuto sulla materia, ponendo le basi per una razionale regolazione dell'attività dei prestatori di servizi connessi all'utilizzo delle valute virtuali. Con l'emanazione della V direttiva antiriciclaggio si è avviato l*'iter* di armonizzazione del quadro di disciplina a livello dell'Unione, decisamente necessario in un settore caratterizzato dalla endemica transnazionalità dei flussi finanziari. In tal senso non può che guardarsi con favore la scelta del legislatore nazionale di colmare il "vuoto" del mancato assoggettamento dei *wallet provider*[265] alla disciplina antiriciclaggio.

Appare invece meno condivisibile la "frettosa" ed indiscriminata estensione della disciplina antiriciclaggio a tutti i prestatori di servizi connessi all'utilizzo delle valute virtuali, attuata mediante la soppressione dell'inciso *«limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso»* contenuto nell'art. 3, comma 5, lett. i) D. Lgs. 231/2007. In tal modo vengono assoggettati agli obblighi *de quibus* anche soggetti che svolgono attività non a rischio di riciclaggio (si pensi ad esempio al soggetto che offre buoni sconto "tokenizzati").

De iure condendo, si auspica comunque che le disposizioni normative possano rimanere condensate all'interno di un organico testo di legge sui profili finanziari, amministrativi e penali dell'offerta a pubblico e lo scambio di valori virtuali. Il legislatore dovrebbe inoltre favorire – sulla scia di quanto si è verificato nell'ambito della protezione dei dati personali – la condivisione di buone prassi e strumenti di regolazione flessibile (linee guida, strumenti di audit, autoregolazione societaria), valorizzando il modello del partenariato pubblico-privato (PPP) per un efficace contrasto al *cyberlaundering*. Un buon *input* di partenza potrebbe esser dato dalla costituzione di gruppo italiano di cooperazione tra forze dell'ordine e settore privato finalizzato allo scambio di informazioni e alla creazione di standard AML (*Anti Money-Laundering*) e KYC (*Know-Your-Costumer*). Così facendo, si replicherebbe a livello domestico quanto già compiuto da Europol con l'istituzione della Blockchain Alliance[266], un tavolo di lavoro riunisce *exchange provider* e alcune società che offrono di servizi di *blockchain forensics* in aperto dialogo con le istituzioni e le autorità investigative.

Rimane tuttavia sullo sfondo il dilemma dell'utilizzo della criptomoneta per transazioni illecite *peer-to-peer* su piattaforme di tipo pubblico, realizzate al di fuori di ogni possibilità di controllo da parte dei fornitori di servizi. Ne è consapevole il legislatore dell'Unione Europea che, nei *consideranda* alla direttiva 2018/843/UE, ricorda come le misure ivi previste non siano in grado di risolvere *in toto* il problema dell'anonimato *«poiché gli utenti possono effettuare operazioni anche senza ricorrere*

[265] Alla lacuna ha posto rimedio il D. Lgs. 125/2019 che, come accennato in precedenza (v. supra, § 3.4.) ha esteso l'ambito soggettivo di applicazione della normativa antiriciclaggio anche ai prestatori di servizi di portafoglio digitale.

[266] Sul tema della *partnership* tra settore pubblico e settore privato v. anche Cap. V, § 2.1.

a tali prestatori» e quindi *«gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato»*[267].

4. Il contrasto al finanziamento del terrorismo tra prevenzione e repressione. Cenni all'evoluzione normativa.

I presidi approntati dal legislatore mirano altresì a prevenire l'uso del sistema finanziario a scopo di finanziamento del terrorismo; è questa una finalità strettamente connessa a quella della lotta al riciclaggio[268], quasi che le due manifestazioni criminose fossero un *idem* sostanziale. Esiste, invero, una certa convergenza tra le attività delle associazioni terroristiche e il crimine economico che si traduce nell'organizzazione di risorse umane e materiali per l'esercizio di una attività imprenditoriale al fine di autofinanziare il compimento di delitti con finalità di terrorismo[269]. La strategia normativa di prevenzione del riciclaggio e quella di contrasto al finanziamento del terrorismo poggiano sulla comune base della responsabilizzazione degli intermediari finanziari; non sarà pertanto necessario tornare sui lineamenti della disciplina già oggetto d'esame nei paragrafi precedenti. Si dovranno invece esaminare nel dettaglio le questioni relative all'utilizzo delle valute virtuali come mezzo per il finanziamento di attività terroristiche, gettando uno sguardo alle ultime novità legislative e alle prospettive di evoluzione del fenomeno.

Tra le linee di azione politica e normativa, un ruolo di assoluto protagonista va riconosciuto alla creazione di strumenti coercitivi in grado di stigmatizzare il reperimento di fondi per la sopravvivenza delle associazioni terroristiche. È questa una materia assai vasta, al cui interno vanno ricomprese non soltanto fattispecie e sanzioni proprie del diritto penale, ma anche misure di carattere amministrativo (o forse parapenale) come il congelamento dei beni e la confisca di prevenzione.

Volendo ripercorrere per sommi capi, e senza pretesa alcuna di esaustività, l'evoluzione del quadro normativo, occorre partire dalla Convenzione di New York del 1999 a cui si deve il merito di aver creato una base normativa comune di contrasto al

---

[267] Considerando n. 9 alla Direttiva 2018/843/UE, nel quale il legislatore afferma altresì che *«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»*.

[268] In argomento, CUÈLLAR M.F., *The Tenuous Relationship between the Fight against Money Laundering and the Disruption of Criminal Finance*, in *The Journal of Criminal Law and Criminology*, 2003, vol. 93, 2, 311 ss.

[269] Sul tema in generale v. ROSSI A., *Prevenzione del riciclaggio e finanziamento del terrorismo: finalità e novità normative,* in *Dir. pen. e proc.*, 2018, 1, 25 ss.; DONINI M., *Il diritto penale di fronte a "nemico",* in *Cass. Pen*., 2006, 737 ss; PALAZZO F., *Contrasto al terrorismo, diritto penale del nemico e principi fondamentali,* in *Quest. Giust.,* 2006, 674 ss. La letteratura più recente ha messo in evidenza lo stretto legame tra la criminalità organizzata e criminalità economica, che si muoverebbero su percorsi integrati mediante una sempre maggiore razionalizzazione ed organizzazione. Cfr., in particolare, SAVONA E.U., *Economia e criminalità,* in *Enciclopedia delle scienze sociali*., vol. IX, Roma, 2001, 97 ss.

finanziamento del terrorismo[270]. Quello stesso anno il Consiglio di Sicurezza delle Nazioni Unite adottò la Risoluzione n. 1267/1999 con cui fu introdotta una procedura di congelamento di fondi diretta contro gli individui inseriti nella c.d. *black-list*, la prima di una lunga fila di risoluzioni adottate a partire dal 2001. A livello comunitario una prima presa di posizione vi fu con il Regolamento CE n. 2580/2001, adottato in via d'urgenza dopo i fatti dell'11 settembre, cui fecero seguito numerosi altri atti normativi[271].

Per far fronte all'emergenza terroristica il legislatore italiano intervenne dapprima con il decreto legge 12 ottobre 2001, n. 369, e, successivamente, con il decreto legge 27 luglio 2005, n. 144. A quest'ultimo si deve l'introduzione all'interno del codice penale di una definizione di "condotte con finalità di terrorismo" e di nuove fattispecie di reato (artt. 270-*quater* ss.), oltre all'estensione ai soggetti inseriti in particolari elenchi delle misure di prevenzione previste per la criminalità organizzata. Fu però con il D. Lgs. 109/2007, emanato in attuazione della terza direttiva antiriciclaggio 2005/60/CE[272], che la materia trovò una compiuta disciplina. Il decreto delegato introdusse una precisa definizione di finanziamento del terrorismo, inteso come *«qualsiasi attività diretta, con qualsiasi mezzo, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi o di risorse economiche, in qualunque modo realizzati, destinati ad essere, in tutto o in parte, utilizzati al fine di compiere uno o più delitti con finalità di terrorismo o in ogni caso diretti a favorire il compimento di uno o più delitti con finalità di terrorismo previsti dal codice penale, e ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione dei delitti anzidetti»* (art. 1, comma 1, lett. a), dettando specifiche disposizioni per la segnalazione delle operazioni sospette[273] e il c.d. congelamento[274] dei beni appartenenti ai presunti terroristi. Con l'emanazione del

[270] Il finanziamento del terrorismo è definito come una attività caratterizzata da punto di vista oggettivo dal fornire fondi, con qualsiasi mezzo, direttamente o indirettamente, legalmente o illegalmente, e dal punto di vista soggettivo, dalla consapevolezza che tali fondi saranno usati per svolgere azioni illecite, capaci di causare la morte o gravi lesioni fisiche ad un civile, o a qualsiasi altra persona che non ha parte attiva in situazioni di conflitto armato, con la finalità di intimidire un popolazione, o obbligare un governo o un'organizzazione internazionale a compiere o ad astenersi dal compiere qualcosa (cfr. art. 2 della Convenzione). L'Italia è tra i Paesi firmatari del trattato, ratificato e reso esecutivo con la legge 14 gennaio 2003, n. 7.

[271] Risoluzione 2002/402/PESC; Regolamento 2002/881/CE; Decisione Quadro 2002/475/GAI; Direttiva 2005/60/CE; Decisione Quadro 2008/919/GAI.

[272] D. Lgs. 22 giugno 2007, n. 109 recante «Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE», adottato in base alla delega contenuta nella legge 25 gennaio 2006, n. 29 (legge comunitaria 2005).

[273] All'epoca non era ancora stato varato il D. Lgs. 231/2007, per cui le disposizioni concernenti gli obblighi di comunicazione e segnalazione facevano ancora riferimento al decreto legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197 (c.d. legge antiriciclaggio).

[274] Il congelamento di fondi indica (art. 1, comma 1, lett. e) il *«divieto di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificare il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso degli stessi, compresa la gestione di portafoglio»*. La locuzione "fondi" ha una portata

Codice antimafia l'applicazione delle misure patrimoniali di prevenzione ai soggetti inseriti nella lista del Comitato per le sanzioni delle Nazioni Unite[275] è stata sottoposta a un regime amministrativo particolarmente rigoroso, tanto da suscitare seri dubbi sul rispetto del principio di legalità[276].

Le più recenti modifiche alla normativa di pubblica sicurezza hanno esteso i poteri delle autorità nazionali allo scopo di rendere più efficaci e snelli i controlli prodromici all'applicazione delle misure di prevenzione. Il rigido meccanismo delle *black list* si era infatti rivelato farraginoso, tanto da aver suggerito l'istituzione di una c.d. lista nazionale. L'art. 4-*bis* del D. Lgs. 109/2007, introdotto dal più volte citato D. Lgs. 90/2017, attribuisce al Ministro dell'Economia e delle Finanze su proposta del Comitato di sicurezza finanziaria, il potere di congelare beni e risorse economiche di soggetti che pongano in essere una o più condotte con finalità di terrorismo, ovvero che svolgano attività in grado di minacciare la pace e la sicurezza internazionale. L'esigenza di tale previsione nasce innanzitutto dalla necessità di dotare l'Italia di uno strumento autonomo e flessibile di prevenzione del finanziamento delle condotte suddette attivabile a livello nazionale con il supporto delle diverse autorità competenti che intervengono nel Comitato di Sicurezza Finanziaria[277]. Il tema sarà esaminato limitatamente alle ipotesi in cui la misura abbia a oggetto valori virtuali; si vedrà in particolare come l'ablazione di questi ultimi sollevi problematiche di non poco conto in punto di individuazione dei valori e di sottrazione della disponibilità degli stessi alla persona sospettata o indiziata[278].

Novità importanti si registrano anche sul fronte repressivo. A distanza di poco più di un anno dal precedente intervento[279], il legislatore italiano ha rimesso mano al codice penale[280] aggiungendo alla già nutrita costellazione di fattispecie incriminatrici i delitti

---

assai ampia e indica *«attività ed utilità finanziarie di qualsiasi natura»* anche possedute per interposta persona, sia essa fisica o giuridica (lett. f).

[275] L'art. 16, comma 1, lett. b) dispone che le misure di prevenzione patrimoniale si applichino anche *«alle persone fisiche e giuridiche segnalate al Comitato per le sanzioni delle Nazioni Unite, o ad altro organismo internazionale competente per disporre il congelamento di fondi o di risorse economiche, quando vi sono fondati elementi per ritenere che i fondi o le risorse possano essere dispersi, occultati o utilizzati per il finanziamento di organizzazioni o attività terroristiche, anche internazionali»*.

[276] Con rifermento, in particolare, alla violazione del principio di legalità v. Corte Cost. sentt. 24-25/2019; Cass. Pen., Sez. Un. 27 aprile 2017, n. 40076; Corte EDU, 27 febbraio 2017, De Tommaso c. Italia.

[277] Il successivo art. 4-*ter* prevede la competenza del Comitato di Sicurezza Finanziaria per la formulazione di proposte di designazione nazionale di individui ed entità alle autorità competenti delle Nazioni Unite e dell'Unione Europea.

[278] La questione sarà approfondita nella parte dedicata all'esecuzione delle misure cautelari (v. *infra*, Cap. V, § 7).

[279] D.L. 18 febbraio 2015, n. 7, convertito in L. 17 aprile 2015, n. 43, con cui furono apportante le seguenti modifiche al codice penale: aggiunta di un secondo comma all'art. 270-*quater* c.p., cha esteso la punibilità anche al soggetto arruolato; introduzione del reato di organizzazione di trasferimenti per finalità di terrorismo (art. 270-*quater*.1 c.p.); inserimento della condotta di auto-addestramento tra quelle punite dall'art. 270-*quinquies* e di una circostanza aggravante collegata all'utilizzo di strumenti informatici o telematici.

[280] Legge 28 luglio 2016 n. 153 (Norme per il contrasto al terrorismo, ratifica ed esecuzione degli obblighi internazionali in materia). La legge fu adottata sulla spinta della necessità di conformare l'ordinamento interno agli obblighi assunti in sede internazionale con la Convenzione del Consiglio

di finanziamento di condotte con finalità di terrorismo (art. 270-*quinquies*.1 c.p.)[281], sottrazione di beni o denaro sottoposti a sequestro (art. 270-*quinquies*.2 c.p.) e atti di terrorismo nucleare (art. 280-*ter* c.p.), prevedendo altresì una nuova ipotesi di confisca obbligatoria, diretta e per equivalente, per tutti i reati commessi con finalità di terrorismo (art. 270-*septies* c.p.). Il legislatore ha così sperimento un "paradigma anticipatorio del tutto inedito", che attribuisce rilevanza agli preparatori al compimento di azioni terroristiche[282].

Di lì a poco fu emanata la Direttiva 2017/541/UE che, con l'intento di armonizzare gli ordinamenti penali nazionali *in subjecta materia*, ha imposto nuovi obblighi di incriminazione a carico degli Stati, non previsti dalli decisioni quadro 2002/475/GAI e 2008/919/GAI, di condotte teleologicamente orientate alla commissione di atti terroristici tra cui la ricezione di addestramento a fini terroristici; l'organizzazione di viaggi a fini terroristici e il finanziamento di attività terroristiche[283]. Il legislatore italiano ha evidentemente ritenuto che il sistema penale fosse già conforme alle disposizioni della direttiva, tant'è che la legge 20 novembre 2017, n. 167 ha dato attuazione alla sola parte relativa al termine di conservazione dei dati del traffico telematico, non intervenendo su alcuna disposizione incriminatrice.

4.1. *Virtual currencies and terrorist financing*. Note a margine del recente studio condotto dal Parlamento Europeo.

Di pari passo con l'evoluzione delle interazioni economiche e la creazione di nuove forme di circolazione della ricchezza, le associazioni terroristiche hanno messo a punto espedienti sempre più sottili per il procacciamento delle risorse strumentali alla propria attività. Nel rapporto del FATF sul finanziamento dello Stato Islamico[284] si individuano

d'Europa per la prevenzione del terrorismo, stipulata a Varsavia il 16 maggio 2005; la Convenzione internazionale per la soppressione di atti di terrorismo nucleare, fatta a New York il 14 settembre 2005; il Protocollo di Emendamento alla Convenzione europea per la repressione del terrorismo, firmata a Strasburgo il 15 maggio 2003; la Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento al terrorismo, stipulato a Varsavia il 16 maggio 2005 e il Protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, fatto a Riga il 22 ottobre 2015. Sul tema v. ARAGONA V., *Il contrasto al finanziamento del terrorismo*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2017, 1, 101 ss.

[281] Occorre comunque precisare che, prima dell'introduzione dell'art. 270-*quinquies*.1, le condotte di finanziamento potevano già assumere rilevanza *ex* art. 270-*bis* (associazione con finalità di terrorismo) o 270-*ter* (assistenza agli associati) c.p. Degli elementi costitutivi del reato si dirà poco oltre, allorché ci occuperemo del finanziamento del terrorismo mediante valute virtuali (v. *infra*, § 4.2).

[282] Secondo BARTOLI R., *Legislazione e prassi in tema di contrasto al terrorismo internazionale: un nuovo paradigma emergenziale?*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2017, 3, 233 si tratta di un paradigma a tutela talmente anticipata che si pone in contrasto non tanto con i principi di garanzia elaborati per il diritto penale della "normalità", ma addirittura con gli stessi principi elaborati per il diritto penale dell'emergenza "tradizionale".

[283] Per approfondimenti v. SANTINI S., *L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2017, 7-8, 13 ss.

[284] Ci si riferisce al rapporto del Financial Action Task Force, *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant*, del febbraio 2015, http://fatf-gafi.org/

due principali forme di finanziamento: un *canale indiretto*, che passa per le donazioni di sostenitori istituzionali (Stati, ma anche attori non statali) e privati (petrolieri, associazioni di beneficienza, *crowdfunding* popolare) accresce l'enorme flusso economico derivante da strumenti di *finanziamento diretto* come la gestione di attività economiche e di traffici internazionali, la richiesta di fondi ad altri gruppi terroristici connessi o collegati, la commissione di gravi delitti contro il patrimonio (estorsioni, saccheggi, indebita imposizione fiscale etc.).

Lo studio si concentra anche sulle forme di *fundraising* che sfruttano le tecnologie informatiche[285], soffermandosi in particolare sul proselitismo mediante social *network* e sulla possibilità di utilizzare il *web* come mezzo di propaganda per campagne di *crowfunding* generico (richiesta di contributi da destinare al complesso di attività del gruppo terroristico) o specifico (raccolta di fondi per finanziare il compimento di uno specifico atto o per condurre a termine un determinato piano). In questo modo la proposta di finanziamento è in grado di raggiungere un numero indeterminato di destinatari, agevolando la raccolta di fondi da "simpatizzanti" residenti in tutto il modo tra cui i *foreign fighters* residenti in Occidente.

In un tale contesto, non era difficile ipotizzare che la crescente dematerializzazione della moneta avrebbe offerto uno strumento formidabile per il finanziamento del terrorismo[286]. Nel maggio del 2018 il Dipartimento per le politiche interne e costituzionali del Parlamento europeo ha presentato alla Commissione Speciale uno studio sulle congiunture tra valori virtuali e finanziamento del terrorismo[287] dal quale emergono dati di significativa importanza.

Nel documento si afferma che, sebbene allo stato non vi siano molti esempi conosciuti – complice anche l'enorme cifra nera che caratterizza del fenomeno – il rischio di un impiego sistematico della finanza virtuale per finanziare le organizzazioni terroristiche si presenta decisamente elevato. Si parla di una concreta possibilità di utilizzo per il compimento di tre distinte tipologie di operazioni, talvolta collegate tra loro[288]. La forma più elementare di finanziamento consiste nel "rastrellamento" di oblazioni e offerte da parte degli affiliati all'associazione, che partecipano a *chatroom* e gruppi di discussione su social media o su programmi di messaggistica istantanea criptata[289]. A tal fine il promotore della raccolta potrebbe anche servirsi di uno *smart contract* programmato per eseguire automaticamente la prestazione una volta raggiunto l'ammontare sperato, dissimulando la causa illecita con intestazioni fittizie (raccolta di fondi per la ristrutturazione di un luogo di culto o per il risanamento ambientale di un territorio); ciò permette di promuovere pubblicamente la proposta dopo aver informato gli associati del vero obiettivo della campagna di *crowdfunding*.

---

[285] *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant*, cit., 24

[286] Cfr. ARAGONA, *Il contrasto al finanziamento del terrorismo*, cit., 100

[287] KEATINGE T., CARLISLE D., KEEN F., *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, Bruxelles, 2018, in https://europarl.europa.eu

[288] KEATINGE, CARLISLE, KEEN, *Virtual currencies and terrorist financing*, cit., 9

[289] In tal caso il portavoce della raccolta di fondi non dovrà fare altro che comunicare ai partecipanti uno o più indirizzi di destinazione delle somme e la tipologia di valuta accettata per la donazione

Una seconda tipologia di finanziamento "via crypto" si ha con il trasferimento di fondi a livello internazionale *peer-to-peer* tra gli appartenenti alle reti terroristiche. Si tratta, in buona sostanza, di una evoluzione del tradizionale *money transfer* che permette di risolvere tutte le criticità legate al passaggio per gli intermediari finanziari; in questo modo le risorse possono essere trasferite in tempi rapidissimi, a costi ridotti, al riparo da ogni ingerenza statuale e senza necessità di dover contare sulla disponibilità di terzi fiduciari.

A vertice della piramide è collocato l'utilizzo delle valute virtuali per la compravendita di beni sulla parte oscura della rete (*darknet*). I traffici illeciti rappresentano una forma di finanziamento diretto per ottenere valuta virtuale in cambio della vendita di beni acquisiti illecitamente, ma anche un canale preferenziale per procurare all'associazione la disponibilità di quanto necessario per la realizzazione di atti terroristici (armi, munizioni, esplosivi, falsi documenti di identità, sostanze psicotrope).

Lo studio si sofferma anche sui fattori in grado di accrescere la propensione delle cellule terroristiche a servirsi del circuito finanziario virtuale, tra cui la proliferazione delle *privacy altcoin* totalente anonime, la crescita delle competenze tecnico-informatiche dei terroristi, il sempre più stretto legame tra da questi ultimi e la criminalità organizzata.

Scendendo nel dettaglio, viene posto in evidenza come la valutazione dei rischi non possa essere condotta in modo generico, dovendo piuttosto essere declinata *case by case* in base alle peculiarità del singolo gruppo criminale. Il terrorismo è un fenomeno poliedrico e complesso, che non si presta ad essere descritto in termini unitari e comprende una vasta la gamma di ideologie, motivazioni, comportamenti, obiettivi. Altrettanto può dirsi a proposito della struttura organizzativa, che varia da forme elementari fino a fisionomie decisamente articolate. Alla prima categoria appartengono i c.d. *lupi solitari* che, pur non avendo legami formali con un gruppo terroristico centrale, organizzano in modo autonomo attentati o altri atti dimostrativi; in posizione intermedia si collocano le piccole cellule terroristiche che, a seconda dei casi, presentano legami più o meno intensi con il gruppo principale; vi sono infine le grandi organizzazioni terroristiche che operano al di fuori del controllo statale (ad. es. al-Qaeda), occupando talvolta intere porzioni del territorio (come l'ISIS nel Califfato).

Considerando tutte queste sfumature, lo studio passa ad esaminare più da vicino quale sia la propensione di ciascuna di queste formule organizzative a fare uso del circolante virtuale come mezzo di finanziamento. Partendo dalle organizzazioni di più modeste dimensioni (attori solitari o piccoli gruppi localizzati), i dati più recenti dimostrerebbero come la criptomoneta non offra vantaggi sostanziali o benefici ulteriori rispetto ai circuiti finanziari convenzionali. Non dovendo questi nuclei terroristici movimentare grosse somme di denaro o raccogliere capitali in massa, anche un semplice prelievo o bonifico bancario può essere sufficiente all'acquisto di tutti gli allestimenti necessari alla commissione di delitti.

Alcuni fatti di cronaca recente lasciano tuttavia intendere come le associazioni terroristiche localizzate abbiano iniziato a manifestare interesse per i trasferimenti in valuta virtuale. Al riguardo viene richiamato il caso del giovane Ali Shukri Amin che nel giugno del 2015 fu condannato dai giudici del Virginia per aver fornito supporto allo Stato Islamico tramite campagne ideologiche sui *social media*. Durante l'interrogatorio l'imputato aveva confessato di utilizzare Twitter per fornire istruzioni su come la rete Bitcoin potrebbe essere utilizzata per l'invio di contributo in favore dell'ISIS[290].

Ben più evidenti le potenzialità che questi strumenti offrono ai grandi gruppi terroristici come mezzo di finanziamento diretto o indiretto. A tal riguardo viene richiamata la propaganda svolta *online* da alcuni gruppi vicini ad al-Qaeda secondo la piena conformità di Bitcoin – e, in generale, della criptomoneta – ai principi della *Sharia* islamica aprirebbe un ampio ventaglio di possibilità per il raggiungimento degli scopi dell'organizzazione. Per assicurare il totale anonimato e favorire la dispersione dei flussi finanziari lungo la *blockchain*, i gruppi terroristici si avvalgono dei servizi di *mixing*. Al riguardo viene citato il ritrovamento nel luglio del 2014 di forum su "Bitcoin e solidarietà per una lotta violenta" nel quale l'autore richiedeva espressamente ai mujaheddin di utilizzare servizi come DarkWallet per effettuare donazioni all'Isis[291].

Gli esempi dimostrano come il finanziamento del terrorismo "via crypto", pur non essendo la principale forma di sostentamento dei gruppi criminali, dipinga uno scenario concreto e tutt'altro che futuribile. Non sarebbe pertanto ultroneo esprimere una certa preoccupazione per l'impotenza degli Stati dinanzi all'espansione dell'economia disintermediata. Ad essa fa riferimento la ricerca più volte citata nel denunciare l'assenza di dati a supporto dell'utilizzo di *blockchain* private da parte dei gruppi terroristici. Pare che nessun trasferimento di fondi sia effettuato con *token* di sistemi centralizzati, perché farebbe venir meno i vantaggi offerti dall'assenza di intermediari.

Non manca tuttavia l'opinione contraria di chi, ottimisticamente, ritiene che il finanziamento dei gruppi terroristici "via cripto" abbia una dimensione decisamente ridotta[292]. Con riferimento al terrorismo di matrice islamica si rappresenta una certa resistenza nel superare i tradizionali mezzi di finanziamento come la *hawala* (trasferimento di valori per il tramite di intermediari) ormai radicati nella "cultura" degli appartenenti alle associazioni sovversive. L'apertura verso queste nuove forme di

---

[290] *Virtual currencies and terrorist financing*, cit., 28; United States Department of Justice, *Virginia Teen Pleads Guilty to Providing Material Support to ISIS*, in *Justice News*, 11 June, 2015, https://www.justice.gov

[291] Si riporta testualmente il contenuto dell'avviso: *«DarkWallet's beta release will be published within the next coming months, the mujahideen Dawlatul Islam would simply need to set up a wallet and post their addresses online. Then, Muslims from across the globe could simply copy the wallet address, login to their [wallets], purchase whatever amount of bitcoin they wish to send, and send them over»*. Cfr. *Virtual currencies and terrorist financing*, cit., 32; HIGGINS S., ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide, 7 July 2014, https://coindesk.com

[292] Si richiama lo studio pubblicato dal Center for New American Security dal titolo «*Terrorist use of virtual currencies. Containing the potential threat*, in *Center for a New American Security»*, in https://cnas.org, citato da STURZO, *Bitcoin e riciclaggio 2.0.*, cit., 32.

finanziamento sembrerebbe inoltre ostacolata dalla scarsa diffusione dei valori virtuali come mezzo di pagamento e dalla difficoltà nel preservare l'anonimato nella fase di conversione per valuta avente corso legale.

Nell'impossibilità di effettuare stime precise, non potrebbero tuttavia negarsi le prospettive di uno rapido sviluppo del fenomeno che, verosimilmente, andrà di pari passo con la crescita della capitalizzazione del mercato valutario virtuale e con l'affermazione della criptomoneta come mezzo di scambio.

4.2. Valute virtuali e finanziamento di condotte con finalità di terrorismo (art. 270-*quinquies*.1 c.p.).

L'art. 270-*quinquies.*1 di recente introduzione punisce chi, alternativamente, raccoglie, eroga o mette a disposizione denaro o beni destinati ad essere in tutto o in parte utilizzati per il compimento di condotte con finalità di terrorismo.

Con il predicato "raccogliere" si intende un'attività, per quanto episodica, consiste nell'accantonamento di disponibilità economiche; per "erogazione" la corresponsione a terzi, in modo continuativo o meno, una somma di denaro o beni; la "messa a disposizione" consiste, infine, nel destinare o riservare una somma di denaro o beni in modo che siano reperibili al destinatario[293].

La norma non richiede che i fondi raccolti, erogati o messi a disposizione siano successivamente utilizzati; trattasi dunque di reato di pericolo presunto, morfologia compatibile con la volontà legislativa di anticipare la punibilità anche agli atti meramente preparatori.

La presenza di una clausola di salvaguardia in apertura della fattispecie[294] esclude il concorso tra il reato in esame e i delitti di associazione con finalità di terrorismo e di organizzazione, finanziamento o propaganda di viaggi all'estero per finalità di terrorismo. Nei casi in cui non venga raggiunta la prova dell'inserimento del soggetto nell'organizzazione terroristica, la condotta di finanziamento potrà essere punita in via residuale ai sensi dell'art. 270-*quinquies.*1[295]. La questione merita un approfondimento specie per quel che riguarda l'esclusione dal novero dei possibili autori del delitto dei partecipanti all'associazione *ex* art. 270-*bis* c.p.[296]. Ciò è tanto più vero per quei gruppi terroristici che operano mediante campagne di propaganda ad ampia diffusione, rispetto ai quali la giurisprudenza più recente ha sensibilmente esteso la soglia di

[293] ARAGONA, *Il contrasto al finanziamento del terrorismo*, cit., 100; BARTOLI, *Legislazione e prassi in tema di contrasto al terrorismo internazionale*, cit., 251.
[294] Che testualmente recita «*al di fuori dei casi di cui agli articoli 270*-bis *e 270*-quater.1».
[295] Quanto, invece, al rapporto tra la nuova fattispecie e i singoli reati finanziati, resta impregiudicata la possibilità che il finanziatore possa rispondere a titolo di concorso nelle singole condotte di terrorismo sovvenzionate. Tuttavia, in tal caso, non sarà sufficiente la generica consapevolezza del finanziatore di contribuire a condotte con finalità di terrorismo, essendo necessario dimostrare la consapevolezza dell'agente di concorrere alla realizzazione dello specifico fatto di reato reso possibile dal finanziamento.
[296] Il delitto in esame punisce coloro che – privi di *affectio societatis* e dunque estranei all'associazione – forniscono il supporto economico necessario alla realizzazione dei fini della stessa, senza tuttavia prendervi parte.

partecipazione a tutte le condotte dalle quali possa evincersi una adesione psicologica ai fini dell'organizzazione terroristica[297].

Alla luce di un simile orientamento giurisprudenziale non potrebbe *a priori* escludersi che anche il mero trasferimento di valute virtuali da parte di soggetti "radicalizzati" al fine di favorirne l'operato sovversivo del gruppo terroristico, possa assumere rilevanza come partecipazione all'associazione[298]. Sembra quindi che il titolo di responsabilità per il soggetto finanziatore dipenderà dal *modus operandi* dell'organizzazione e dalla prova del dolo di partecipazione.

Oggetto materiale della condotta sono i "beni" o il "denaro"; ciò pone un ostacolo significativo all'applicazione della fattispecie a condotte di finanziamento che si realizzino per il tramite di valori virtuali. Circa l'impossibilità di ricondurre la criptomoneta al denaro in senso tecnico-giuridico abbiamo già detto *funditus* in precedenza[299], mettendo in evidenza come anche la sussunzione nel concetto penalistico di "bene" si scontri con ostacoli di tutto spessore. Questo aspetto sarà approfondito poco oltre a proposito dell'impossibilità di ricondurre alla fattispecie del furto la indebita sottrazione della valuta virtuale (*rectius*, delle chiavi crittografiche)[300]. È sufficiente qui ribadire come ogni forzatura ermeneutica potrebbe facilmente

---

[297] La giurisprudenza più recente ha ampliato le maglie applicative della condotta di partecipazione ad associazione con finalità di terrorismo in modo da consentire una efficace repressione dei nuclei terroristici 'a cellula' o 'a rete', in grado di operare a distanza attraverso elementari organizzazioni di uomini e mezzi, facendovi rientrare anche l'operato di coloro che, per la totale autonomia organizzativa, sono stati giornalisticamente definiti lupi solitari. Il riferimento è alla giurisprudenza che si è occupata – e con frequenza sempre maggiore continua ad occuparsi – di terrorismo di matrice jihadista. Le più recenti pronunce di legittimità sulla configurabilità del reato di cui all'art. 270-*bis*, comma 2, c.p. hanno evocato principi estremamente elastici, la cui concreta applicazione tende ad anticipare sensibilmente la "soglia di partecipazione" all'associazione terroristica, ritenendo sufficienti, ad esempio, anche mere condotte di propaganda, proselitismo, o arruolamento, purché supportate dall'adesione psicologica al programma criminoso dell'associazione medesima. Si vedano, *ex plurimis*, Cass. Pen., sez. VI, 12 luglio 2012 n. 46308 in *Guid. Dir.*, 2013, 7, 66; Cass. Pen., sez. V, 08 ottobre 2015, n. 2651; Ass. Milano, sent. 25 maggio 2016, in *Diritto penale contemporaneo*, 21 ottobre 2016, con nota di ALBANESE D., *Partecipazione all'associazione con finalità di terrorismo 'Stato Islamico': una pronuncia di condanna della Corte d'Assise di Milano*. In dottrina v. anche FASANI F., *Un nuovo intervento di contrasto al terrorismo internazionale*, in *Dir. Pen. Proc*., 2016, 12, 1555 ss.; ID., *I martiri invisibili. Quale ruolo per il diritto penale nella lotta al terrorismo Islamico?* in *Criminalia*, 2015, 485 ss.; MASARONE V., *La responsabilità delle persone giuridiche in rapporto ai delitti di terrorismo tra obblighi internazionali e normativa interna di attuazione*, in *Crit. Dir.* 2014, 3, pp. 225 ss.; D'AGOSTINO L., *I margini applicativi della condotta di partecipazione all'associazione terroristica: adesione psicologica e contributo causale all'esecuzione del programma criminoso*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2017, 1, 81 ss.

[298] Si ritiene che la condotta di partecipazione debba compendiarsi in relazione alle singolarità organizzative dell'associazione criminale, che, nel caso del fondamentalismo islamico, raggiunge una conformazione assai diffusa e disarticolata. La nascita del terrorismo individuale di matrice islamista, improntato ad un modello orizzontale, e quindi caratterizzato dalla frammentazione estrema del fattore umano, delinea nuove forme di partecipazione e mette evidentemente a dura prova le categorie pensate e costruite per le comuni associazioni per delinquere. Un fenomeno così disarticolato, in cui ogni individuo può da sé attuare il programma dell'organizzazione terroristica, non può che porre delle difficoltà nell'individuazione del momento a partire dal quale possa dirsi che un soggetto partecipa alla stessa, ai sensi dell'art. 270-*bis*, comma 2, c.p.

[299] Si veda *supra*, § 1.5.

[300] *Amplius*, § 5.2.

scontrarsi con il divieto di analogia *in malam partem*[301]*;* sarebbe pertanto opportuno estendere l'oggetto materiale del reato anche alle "altre utilità" in linea con la tecnica descrittiva utilizzata nelle fattispecie di riciclaggio.

4.3. La criptomoneta come mezzo di scambio per l'acquisto di beni intrinsecamente illeciti sul *dark web*. Mercati neri virtuali e dintorni.

Si parla di web profondo per indicare l'insieme delle risorse del World Wide Web non indicizzate dai comuni motori di ricerca. Per spiegare la mole di dati presente in questa parte della rete si ricorre spesso alla metafora dell'*iceberg*: il *surface web* rappresenta una parte minimale della massa di informazioni, mentre la parte sostanziale si trova sotto il livello delle acque, invisibile all'occhio dei navigatori. Nel *deep web* si trovano contenuti raggiungibili mediante un normale *browser* a coloro che conoscano l'indirizzo della pagina o dispongano delle credenziali di autenticazione; in esso confluisce l'intera massa di informazioni che riservate che si ha interesse a rendere accessibile da remoto[302].

Da esso si distingue un terzo livello, definito *dark web* – o più propriamente *dark net*, visto che non si utilizza il consueto protocollo web di comunicazione – un contenitore di dati resi intenzionalmente invisibili e non accessibili dai comuni motori di ricerca, ma accessibili tramite *browser* per la navigazione "sottomarina" come Tor[303]. Il termine *dark* mette in evidenza non soltanto le caratteristiche di oscurità delle informazioni, ma anche l'attitudine all'impiego per attività criminali. D'altro canto, però, la possibilità di trasmettere informazioni in maniera anonima dà luogo a un canale di comunicazione sicuro per i dissidenti di stati totalitari, offrendo uno strumento per l'esercizio dei diritti civili e dalla libertà nella manifestazione del pensiero. La navigazione nel *dark web* non costituisce di per sé reato, anzi potrebbe essere animata da fini, oltre leciti, assolutamente comprensibili (tutela della *privacy* e lotta alla datificazione a alla massiva profilazione per finalità commerciali)[304]; a ciò di

[301] *Contra*, STURZO, *Bitcoin e riciclaggio 2.0.*, cit., 32, la quale ritiene ammissibile l'inquadramento della valuta virtuale tanto nel *genus* del "bene" quanto in quello delle "altre utilità". Al riguardo si argomenta che l'espresso riferimento ai beni o denaro «in qualunque modo realizzati» – contenuto nell'art. 270-*quinquies.*1 c.p. – include nel perimetro del penalmente rilevante il finanziamento mediante l'utilizzo di valuta virtuale, potendosi ritenere quest'ultima "un bene in qualunque modo realizzato".

[302] Si pensi ai *cloud* e alle banche dati *online* per la registrazione di documenti scientifici, cartelle cliniche, atti governativi o aziendali etc. Secondo alcune stime il *deep web* sarebbe centinaia di volte più grande del web di superficie, ma si tratta di statistiche difficilmente dimostrabili.

[303] L'accesso alle *dark net* avviene tramite *software* particolari che fanno da ponte tra Internet e la rete oscura. Uno dei più famosi è Tor che, oltre a fornire accesso all'omonima rete, garantisce l'anonimato all'utente, permettendogli di navigare anche sul normale World Wide Web da uno dei nodi della rete Tor, mediante un indirizzo IP nascosto (*rectius*, riflesso su un altro nodo della rete).

[304] Deve pertanto distinguersi l'utilizzo per fini illeciti (siti contenenti materiale pedopornografico, *online criminal markets* per il commercio illegale di droghe e armi, siti sottoposti a censure governative, siti per la committenza di reati informatici su richiesta), da quello assolutamente legittimo (informazioni e contenuti nascosti intenzionalmente per ragioni di *privacy* degli utenti, al fine di evitare il tracciamento mediante *cookies* e la profilazione mediante *big data*).

accompagna la diffusa tendenza a profittare dello schermo dell'anonimato per il compimento di fatti penalmente rilevanti (es. reati del narcotraffico, vendita di armi, istigazione a delinquere, arruolamento per finalità di terrorismo, riciclaggio, ricettazione, diffusione di codici di accesso a sistemi informatici etc.). Esistono dunque numerose congiunture tra *darknet* e criminalità informatica sulle quali non ci si potrà soffermare se non cursoriamente e con specifico riferimento al fenomeno dei mercati neri virtuali. Il *trading* sul mercato nero ha raggiunto dimensioni allarmanti, non solo per l'enorme quantità di denaro (*rectius*, di criptovaluta) in esso circolante, ma anche per il numero di annunci inseriti, che rendono chiaramente l'idea di un fenomeno diffuso, sistemico e ben strutturato.

La pessima fama della parte oscura del *web* è sostanzialmente dovuta all'evidenza, ormai acquisita, dell'elevato numero delle attività illecite che ivi si svolgono. Le statistiche finora edite evidenziavano una progressiva crescita del fenomeno, dovuta alla diffusione della informatizzazione nel tessuto sociale: un vero e proprio spostamento di intere porzioni di criminalità dal mondo reale a quello virtuale. In tal senso, i dati del penultimo rapporto *Internet Organised Crime Threat Assessment*[305] dell'EC3 di Europol evidenziavano un rapporto di diretta proporzionalità tra l'aumento di capitalizzazione del mercato delle valute virtuali e il dilagare sulla parte oscura della rete di *criminal markets*[306] per la compravendita di beni intrinsecamente illeciti.

Con la chiusura dei tre maggiori *marketplaces* (AlphaBay, RAMP, Hansa) il commercio di beni illegali ha subito un forte contrazione[307]. Secondo l'European Cybercrime Center nel 2018 vi sono stati netti segnali di miglioramento[308], sebbene il

[305] IOCTA 2017, a cura dell'*Internet Cybercrime Centre* (EC3) costituito presso Europol. Il documento è disponibile su https://europol.europa.eu

[306] Si tratta di veri e propri "supermercati" virtuali per lo scambio di beni intrinsecamente illeciti. Basti pensare che AlphaBay alla data del sequestro aveva oltre 200.000 clienti e 40.000 venditori, oltre 250.000 inserzioni per la compravendita di sostanze stupefacenti, più di 100.000 annunci di oggetti rubati e di documenti di identità contraffatti, svariate migliaia di offerte per l'acquisto di beni contraffatti, di strumenti di hacking o di programmi finalizzati alla commissione di reati informatici; altrettanto numerose inserzioni per l'acquisto di armi da fuoco e di esplosivi. L'*European Cybercrime Centre* stima che, dalla sua creazione nel 2014, sono state effettuate transazioni per un equivalente, in criptovalute, di quasi un miliardo di dollari. Non di certo inferiore il volume di affari di *SilkRoad*, il più grande *hidden market* al mondo, che l'FBI a definitivamente chiuso nel novembre 2014. Circa un anno dopo il suo creatore, Ross Ulbricht, è stato condannato all'ergastolo per i reati di associazione per delinquere, frode informatica, distribuzione di false identità, riciclaggio di denaro, traffico di droga, traffico di droga su internet e cospirazione per il traffico di stupefacenti.

[307] In questi mercati neri era possibile l'acquisto di ogni genere di bene o servizi illeciti, perfino di quelli più rari. Alcuni annunci sponsorizzavano, ad esempio, la vendita di vulnerabilità dei sistemi operativi più diffusi (IOS, Android, Windows), di guide tecniche per la creazione di virus informatici o di armi artigianali, di carte di credito clonate etc. Il pagamento era inizialmente consentito soltanto in Bitcoin (BTC), successivamente, con la diffusione e la crescita della capitalizzazione di altri valori virtuali, i venditori hanno iniziato ad accettare anche altre valute virtuali tra cui Monero (XMR), Litecoin (LTC), Bitcoin Cash (BCH) etc.

[308] Così, testualmente, il rapporto IOCTA 2018, *ibidem*, 10 *«The Darknet market ecosystem is extremely unstable. While law enforcement shut down three major marketplaces in 2017, at least nine more closed either spontaneously or as a result of their administrators absconding with the market's stored funds».* Pur nel quadro di un giudizio positivo sull'andamento del fenomeno, il rapporto mette comunque in

tramonto della "grande distribuzione" abbia condotto alla diffusione dei rivenditori "al dettaglio" e di piccolo "mercati rionali": *«the almost inevitable closure of large, global Darknet marketplaces has led to an increase in the number of smaller vendor shops and secondary markets catering to specific language groups or nationalities»*.

La frammentazione della filiera distributiva è una chiara dimostrazione della duttilità del crimine informatico dinanzi all'affinamento delle strategie di contrasto. Come in un sistema di vasi comunicanti l'ostruzione di un tubo porta a un innalzamento proporzionale del livello di fluido, così nel mercato nero la chiusura di una piazza centrale di scambio favorisce l'incontro tra domanda e offerta "per vie traverse". Un esempio è dato dall'oscuramento del sito webstresser.org, sul quale venivano offerti servizi a pagamento di Distrituted Denial of Service (DDoS) sulla parte visibile della rete così da renderle fruibili per un numero maggiore di utenti.

Ancor più recente la notizia del sequestro di Wall Street Market e Silkkitie[309]. L'operazione si è conclusa con successo grazie al coordinamento investigativo tra Ufficio europeo di polizia e le Autorità nazionali. A tal fine Europol ha istituito un *team* specializzato nel contrasto alla criminalità sul *dark web* al quale è attribuito il compito di condividere le informazioni, offrire supporto operativo per condurre indagini sulla parte oscura della rete, organizzare iniziative di formazione e campagne di sensibilizzazione.

L'incentivo all'utilizzo delle valute virtuali come mezzo di pagamento per gli acquisti sui mercati neri deriva chiaramente dalle garanzie di anonimato che esse offrono: la criptomoneta rappresenta il *medium* per eccellenza per la compravendita di beni illegali. Sul versante investigativo ciò comporta serie difficoltà nell'individuazione degli autori di una transazione illecita. Per far fronte a queste difficoltà sono state elaborate alcune innovative tecniche di indagine basate sull'osservazione delle evidenze disponibili sul registro pubblico delle transazioni e sulle informazioni reperibili in rete, al fine di delineare un profilo dei possibili cyber-criminali[310]. Con il termine *Open Source Intelligence* si indica l'attività di raccolta d'informazioni mediante la consultazione di fonti di pubblico accesso. Le pagine del *dark web*, sebbene non indicizzate dai comuni motori di ricerca, possono rivelarsi una preziosa sorgente di informazioni se consultate mediante software di *web crawling* in grado di filtrare i risultati e di restituire agli inquirenti indici di risultati in cui compare

---

evidenza come la commercializzazione di beni o servizi illegali nella parte oscura del *web* rimanga una assoluta priorità per Europol.

[309] La notizia è stata diffusa da Europol con la conferenza stampa del 3 maggio 2019, v. https://europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces. Wall Street era il secondo mercato nero virtuale per dimensioni, in cui si faceva commercio di droghe (tra cui cocaina, eroina, cannabis e anfetamine), dati rubati, documenti falsi e software malevoli. Esso conteneva oltre 63.000 offerte di vendita, più di 1.150.000 conti clienti e oltre 5.400 venditori registrati. Per il pagamento gli utenti del mercato *online* utilizzavano Bitcoin e Monero. Dalla conferenza stampa risulta che i gestori del mercato abbiano ricevuto commissioni per il 2-6% del prezzo di vendita di ciascun articolo. Il secondo, noto come il Valhalla Marketplace, era il più famoso mercato nero della Finlandia, conosciuto a livello internazionale. Dopo la chiusura del sito molti commercianti finlandesi hanno trasferito le proprie attività su altri siti illegali, fra cui appunto Wall Street.

[310] Sono questi temi che saranno approfonditi nel prosieguo (*infra*, Cap. V, § 5).

la chiave di ricerca utilizzata. In questo modo è possibile andare alla scoperta dei siti contenenti parole inserite nella *black-list*, aggregare i risultati per monitorare l'attività dei criminali e cercare di portarli allo scoperto grazie a lunghe operazioni sotto copertura[311].

In conclusione, appare doveroso osservare come l'attuale dimensione del commercio illegale in rete costituisca una sorta di riedizione contemporanea del mercato nero reale che, progressivamente, ha perso clientela.

Le ragioni dell'espansione del commercio illegale nella parte oscura della rete vanno ricercate in più fattori. Se da un lato la possibilità di ordinare a distanza, senza necessità di un incontro fisico con il distributore, desensibilizza gli utenti e accresce la propensione al *trading* illegale, dall'altro è certamente l'anonimato garantito dai *browser* di navigazione e dall'impiego delle valute virtuali a offrire la spinta criminogena decisiva. Il commercio nella parte oscura del web presenta degli indiscutibili vantaggi per i cyber-criminali, per eliminare i quali occorre una solida cooperazione tra autorità investigative a livello internazionale.

Ma il fronte investigativo non è l'unico su cui insistere. Anche la regolazione in materia di valute virtuali (antiriciclaggio, prevenzione del terrorismo, controllo sull'esercizio dell'attività di cambiavalute) è in grado di sortire effetti positivi nella lotta al *trading* illecito sul *dark web*, favorendo l'emersione di capitali illeciti e la progressiva caduta della barriera dell'anonimato.

5. La valuta virtuale come oggetto (im)materiale del reato. Furto e indebita sottrazione di chiavi crittografiche.

La trattazione svolta nei paragrafi precedenti si è concentrata sui principali utilizzi della criptomoneta come *strumento del reato*. Mutando la prospettiva dell'indagine, si affronterà ora la questione della tutela penale della valuta virtuale come bene giuridico suscettibile di valutazione economica. L'attenzione andrà rivolta, in particolare, ai reati configurabili nei casi di indebita sottrazione di valuta virtuale: trattasi manifestazioni criminose del tutto inedite, non previste né prevedibili all'epoca in cui fu scritto il codice penale.

Anzitutto, una breve premessa sulla meritevolezza di tutela della *virtual property* appare indispensabile. Per quanto si tratti di una forma di ricchezza artificiale, priva di valore intrinseco, del tutto dematerializzata, e per molti versi inconsistente, non potrebbe non considerarsi, dalla prospettiva del diritto penale, l'esistenza di un *valore di mercato* delle unità di conto virtuale. A differenza delle comuni informazioni digitali, duplicabili *ad infinitum* e fruibili da un numero tendenzialmente illimitato di

[311] Il patrimonio informativo disponibile *open source* si rivela talvolta essenziale per iniziare una investigazione nei confronti di possibili sospettati. Queste tecniche si fondono con quelle, ancora più innovative, di *blockchain forensics* che consentono di tracciare il flusso delle transazioni sospette e di tentare di risalire alle identità degli utilizzatori di valute virtuali.

persone, le valute virtuali sono dati univoci, inalterabili e disponibili al solo possessore delle chiavi crittografiche. Già questo sembra sufficiente a far ritenere tali rappresentazioni digitali dei beni immateriali suscettibili di valutazione economica, pur senza considerare la circostanza – non trascurabile – della idoneità delle stesse a fungere da veicolo per l'incorporazione e la circolazione dei diritti. Rimane invece fuori dal perimetro classificatorio l'esistenza di un mercato a valle della creazione dell'informazione[312], che, pur dando riprova del requisito di economicità del bene, non ne costituisce un elemento essenziale. Occorre infatti attribuire rilievo giuridico alla *scarsità digitale* dell'informazione in sé, a prescindere dall'attuale esistenza di operatori economici disposti a pagare un corrispettivo in denaro pur di ottenerla.

A tal fine non potrebbe non considerarsi la latitudine del concetto civilistico di patrimonio dal quale deriva l'ampiezza della relativa tutela penale[313]. La dottrina più autorevole sostiene che il patrimonio sia il complesso delle attività e delle passività che si riferiscono a una persona[314], l'insieme dei rapporti giuridici economicamente valutabili che le fanno capo, avente ad oggetto cose o ad altre entità valutabili in denaro. Sia che si tratti di diritti soggettivi o di rapporti di fatto, di *res* corporali o immateriali, il valore delle singole cose è determinato dall'interesse del soggetto a soddisfare, tramite esse, i propri bisogni; tale interesse concorrerà ad individuare le componenti del patrimonio meritevoli di tutela penale secondo la teoria c.d. funzionale del bene giuridico. Che la valuta virtuale costituisca un cespite patrimoniale nel senso sopra descritto non pare revocabile in dubbio. Pur essendo un oggetto incorporale (come un'opera dell'ingegno o un credito), essa è funzionale al soddisfacimento di un interesse di chi la possiede: trattasi di una informazione limitata e non duplicabile, che può essere trasferita in modo sicuro con prerogative di esclusività, suscettibile di essere apprezzata e scambiata sul mercato, il cui possesso permette l'accesso ai servizi di un sistema di registri distribuiti.

Ecco che la marcata componente patrimonialistica, ancorché immateriale, che caratterizza questi valori rende evidente che al diritto penale competerà assicurare una tutela paritetica rispetto alle oggettività tutelate dal titolo XIII del libro II del codice.

---

[312] Si intende per mercato lo scambio delle rappresentazioni digitali di valore, ovverosia l'esistenza di operatori economici disposti ad acquistare tali valori per denaro a un determinato livello di prezzo.

[313] L'opinione più diffusa è che il concetto delineato dai cultori del diritto privato sia valido anche per il diritto penale, con l'importante precisazione che il patrimonio in senso penalistico comprende anche le cose che hanno per il soggetto un valore di affezione. In tal senso v. ANTOLISEI F., *Manuale di diritto penale – Parte speciale*, vol. I, Milano, 2016, 377 ss., il quale ritiene che la dibattuta questione sulla natura giuridica o economica del patrimonio, considerato come oggetto della tutela penale, vada risolta nel primo senso. Del resto sono le stesse esigenze alla base del diritto penale che non consentono di accogliere una definizione di patrimonio che si limiti al complesso dei rapporti giuridici solo se economicamente valutabili. Per questo è stata proposta una nozione di patrimonio inteso come «complesso dei rapporti giuridici facenti capo ad una persona aventi per oggetto cose dotate di funzione strumentale a soddisfare bisogni materiali o spirituali» (v. CARMONA A., *I reati contro il patrimonio*, in FIORELLA A. (a cura di), *Questioni fondamentali della parte speciale del diritto penale*, Torino, 2016, 7).

[314] Cfr. FIANDACA G., MUSCO E., *Diritto penale – Parte speciale*, vol. II, Bologna, 2015, 3 ss.; MEZZETTI E., *Reati contro il patrimonio*, Milano, 2013, 4 ss.; ANTOLISEI, *Manuale di diritto penale*, ibidem.

Del resto, la cronistoria dei più recenti cyber-attacchi[315] ha dimostrato che i valori virtuali sono utilità ad elevato rischio di aggressione; non è tuttavia chiara la qualificazione giuridica delle condotte di indebita sottrazione, astrattamente riconducibili alle fattispecie di furto (art. 624 c.p.) e di frode informatica commessa con indebito utilizzo dell'identità digitale altrui (art. 640-*ter*, comma 3, c.p.). Si potrebbe del resto discutere sulla configurabilità del delitto di appropriazione indebita (art. 646 c.p.), qualora le condotte di cui sopra siano realizzate dal soggetto che, a qualunque titolo, possieda le chiavi crittografiche (si pensi, ad. es., a fornitore di servizi di portafoglio). Per sciogliere questi dubbi l'interprete dovrà percorrere un terreno reso particolarmente scivoloso dalla sfuggente natura giuridica delle valute virtuali, che, come vedremo, solleva problematiche di non poco conto sul piano della tassatività penale.

5.1. Tra proprietà e possesso. *Dominium* crittografico, signoria di fatto e atti dispositivi in *blockchain*.

Nel ricondurre i valori virtuali all'alveo dei rapporti patrimoniali attivi il punto di partenza è dato dall'attitudine della *blockchain* ad attribuire valore economico a informazioni digitali univoche e non duplicabili. Laddove un soggetto sia l'unico a conoscere le chiavi di accesso e a poter disporre di una data informazione, si crea un terreno fertile affinché quella rappresentazione digitale acquisti valore economico. In tal senso, non sarebbe peregrino affermare che la tecnologia a registro distribuito ha dato vita alla "rappresentazione informatica della scarsità", permettendo parimenti di trasferire ovunque, in modo rapido e affidabile, unità di conto aventi valore economico. La *blockchain* rivoluziona così i connotati materiali e spazio-temporali dei trasferimenti di ricchezza tra individui, tanto da aver fatto parlare la dottrina[316] di una nuova istituzione del diritto di proprietà, in grado di reggersi indipendentemente e al di fuori della presenza statuale. La tenuta di una infrastruttura decentralizzata *fa del codice legge*, assicurando il rispetto dell'esclusività del potere di disposizione deli valori e rendendo a tutti conoscibile la situazione proprietaria e la circolazione delle unità di conto. Né potrebbe negarsi valore giuridico a tali rappresentazioni digitali di valore,

[315] Possiamo citare ad esempio il *crac* della popolare piattaforma di scambio giapponese Mt. Gox, bersagliata da ripetuti attacchi informatici che hanno comportato la perdita di 744.408 Bitcoin, equivalenti – al tasso di cambio allora in vigore – ad oltre 350 milioni di dollari, costati al fondatore, Mark Karpeles, anche un procedimento per bancarotta e l'applicazione di una misura cautelare custodiale. Più di recente si ricorda la vicenda che ha interessato l'*exchange* Bitfinex, che a causa di un attacco informatico ha perduto oltre 200.000 Bitcoin, equivalenti allora a circa 72 milioni di dollari statunitensi. Per la cronaca nazionale, ricordiamo la procedura fallimentare a carico della piattaforma fiorentina BitGrail, scaturita dalla sottrazione da parti di ignoti di oltre 17 milioni di Nanovalute (XBR), equivalenti ad oltre 120 milioni di Euro.

[316] Cfr, ISHMAEV G., *Blockchain technology as an institution of property*, in *Metaphilosophy*, 2017, vol. 48, 5, 665, richiamato da PISELLI R., *Autonomia negoziale, potere e blockchain. La rivoluzione del contratto*, in NUZZO A. (a cura di), *Blockchain e autonomia privata. Fondamenti giuridici*, Roma, 2019, 27.

poiché l'assetto proprietario si legittimerebbe dal basso in base all'*opinio iuris* dei consociati (modello c.d. *bottom-up*, basato dalla fiducia nel sistema) senza il necessario passaggio per il riconoscimento statale (modello c.d. *top-down*, attualmente dominante a livello globale).

Per un corretto approccio alle problematiche relative alla tutela penale, appare indispensabile una precisazione sul contenuto e sui limiti del diritto di proprietà sugli *asset* virtuali.

Qualsiasi transazione sulla catena dei blocchi è individuata da un codice identificativo alfanumerico che definisce un indirizzo cui sono ricollegate le unità di conto virtuale. Il più delle volte l'indirizzo viene rilasciato nel momento in cui un utente decide di dotarsi di un portafoglio virtuale (*e-wallet*), che, *mutatis mutandis*, può essere paragonato a un IBAN bancario. Per effettuare un ordine di pagamento in valuta virtuale la transazione viene sottoscritta digitalmente con la chiave privata di criptazione, generata in automatico al momento dell'apertura del conto/portafoglio e ivi custodita. Quel che importa mettere in evidenza è il particolare funzionamento del sistema: le unità virtuali non fuoriescono mai dai registri informatici, rimanendo memorizzati in *blockchain* sottoforma di indirizzi-valore. Il che vuol dire che il deposito della valuta nel *wallet* si traduce in una mera finzione, poiché oggetto di custodia non è altro che la coppia di chiavi crittografiche per permette di smobilizzare l'ammontare di criptomoneta associata a quell'indirizzo. Ecco che la proprietà del *token* si risolve nel possesso della chiave privata, giacché soltanto tramite di essa è possibile disporre dell'informazione registrata in *blockchain*[317].

Una simile situazione possessoria, che potremmo definire *titolarità* del dato informatico, presenta dei connotati profondamente diversi rispetto al diritto di proprietà. Le facoltà e i poteri che spettano al *dominus* subiscono qui una forte contrazione; il titolare dei *token* non può, ad esempio, distruggere la ricchezza o "tirarla fuori" dall'infrastruttura per destinarla a indirizzi di altri sistemi[318]. Ci si è chiesti, pertanto, in che termini sia possibile descrivere il rapporto giuridico che lega il possessore delle chiavi crittografiche agli asset virtuali. [319]. Trattandosi di un interrogativo dalla evidente impronta civilistica, impossibile da sciogliere in questa sede con la dovizia di dettagli che meriterebbe, possiamo limitarci a una precisazione di carattere terminologico. Si è preferito l'utilizzo dei sostantivi "titolarità" o

[317] Il meccanismo delle chiavi asimmetriche esclude dal potere di disposizione dei *token* chi non è a conoscenza della chiave privata. Perfino il proprietario, una volta smarrite le chiavi, è destinato a non poter più recuperare l'ammontare di valuta virtuale associata all'indirizzo del quale ha smarrito la chiave. Ciò rende del resto assai complicata l'esecuzione di misure come il sequestro o la confisca poiché, come vedremo, è sufficiente che il soggetto abbia una copia di *back-up* delle chiavi per riacquisire il possesso degli averi sottratti dall'autorità (v. *infra*, Cap. V, § 7).

[318] Nella prassi commerciale si riscontra la presenza si termini e condizioni accettati dall'utente con cui si fa espresso riferimento all'assenza di diritti economici o funzionalità particolari del *token* al di fuori del sistema.

[319] Sostiene PISELLI, *Autonomia negoziale, potere e blockchain*, cit., che la relazione tra il *token* e chi conosce la chiave privata in termini di proprietà non possa gettare alcuna luce sulla relazione che si instaura tra il soggetto e il bene e sul nucleo di facoltà spettanti a quest'ultimo.

"detenzione della chiave di criptazione" per evitare fraintendimenti con termini quali "proprietà" o "possesso" che, avendo un significato giuridico ben preciso, rischierebbero di essere fuorvianti.

Il *dominium* sull'informazione non si estrinseca dunque in un'attività corrispondente all'esercizio della proprietà o di altro diritto reale. Il titolare può soltanto esercitare un pieno potere dispositivo sul *token* all'interno del sistema informatico che lo contiene[320].

Si va in tal modo verso un nuovo concetto di proprietà, sganciata dal requisito della materialità di un bene, lontano da modello dello *ius utendi ac abutendi* di romanistica memoria, sempre più limitato, in cui il nucleo del diritto è rappresentato dall'appartenenza al sistema e dalla signoria sul potere dispositivo dell'informazione.

5.2. L'applicabilità della fattispecie comune di furto tra equilibrismi interpretativi ed esigenze di tassatività.

La premessa sul contenuto e sui limiti del diritto "di proprietà" sui valori virtuali ci permette di affrontare con maggiore consapevolezza la questione di fondo: il presidio penale contro le condotte di indebita sottrazione.

Una tesi senza dubbio affascinante è quella di punire tali condotte allo stesso modo di quelle aventi ad oggetto il denaro o la valuta avente corso legale, sussumendole nella fattispecie di furto[321]. L'oggetto materiale della condotta andrebbe ravvisato non nella valuta virtuale in sé – ovverosia il dato informatico registrato in *blockchain*, che rimane nel sistema – bensì nelle chiavi crittografiche private. Si è già detto come esse siano dati informatici *sui generis* poiché, una volta "spese" per firmare l'*input* di una transazione, privano definitivamente il proprietario della disponibilità della valuta. Ragionando secondo lo schema tipico dell'art. 624 c.p. può ritenersi che la sottrazione della suddetta chiave dia luogo a uno spossessamento e alla costituzione di una nuova situazione possessoria in capo al ladro.

A favore di questa soluzione si potrebbe inoltre sostenere che l'apprensione di valori da un portafoglio virtuale è del tutto assimilabile al prelievo non autorizzato di somme da un conto corrente. Una recente sentenza di merito ha ritenuto che la condotta dell'impiegato di banca, che attraverso movimentazioni fittizie effettui spostamenti o prelievi di denaro dai conti correnti dei clienti, sottraendolo alla loro disponibilità, integri gli estremi del reato di furto, aggravato dal mezzo fraudolento, e non quello di frode informatica[322].

320

321 Il reato punisce, come noto, chi s'impossessa della cosa mobile altrui sottraendola a chi la detiene, al fine di trarne profitto (art. 624 c.p.).

322 App. Taranto, 07 luglio 2014 n. 223, in *Guida dir.*, 2015, 7, 80 ss. Secondo il collegio, ai fini della configurabilità della fattispecie di cui all'articolo 640-*ter* c.p. non è sufficiente che le operazioni di spostamento del denaro siano effettuate attraverso sistemi informatici. Tale reato si configura soltanto quando l'agente interviene su un sistema informatico, alterandone il funzionamento o manipolando dati, informazioni o programmi senza l'autorizzazione dal titolare del sistema.

La tesi presta tuttavia il fianco a numerose critiche. Sul piano della tipicità, sembra piuttosto arduo sostenere che i valori virtuali possano essere considerati una cosa mobile ai sensi dell'art. 624 c.p. Se nel linguaggio comune essa indica ogni oggetto del mondo esteriore diverso dall'uomo, per il diritto *«sono "cose" tutti gli oggetti corporali e quelle altre entità naturali che hanno valore economico e sono suscettibili di appropriazione»*[323]. Il richiamo agli oggetti corporali (*res quae tangi possunt*) e alle entità naturali (*omnia in rerum natura*) dà ragione del tradizionale connotato materialistico delle cose in senso tecnico-giuridico nel quale certamente non può rientrare l'informazione digitale espressa in logica binaria (valuta virtuale o chiave privata di criptazione). La stessa dottrina sostiene però che la nozione giuridica di cosa vada intesa in senso "storicamente relativo" in modo da assumere una ampiezza tanto maggiore a seconda sulle crescenti capacità tecnologiche dell'uomo di utilizzo delle risorse naturali. Si spiega in tal modo la previsione del capoverso dell'art. 624 secondo cui agli effetti della legge penale è considerata cosa mobile *«anche l'energia elettrica e ogni altra energia che abbia un valore economico»*[324], disposizione su cui la giurisprudenza ha fatto leva per farvi rientrare anche le onde elettromagnetiche generate da elettrodotti[325] e il segnale telefonico[326].

Ci si domanda allora se tra le energie che abbiano un valore economico possano includersi anche i dati informatici alla base del funzionamento dei valori virtuali. Pur seguendo un approccio ermeneutico evolutivo, è opportuno delimitare il concetto di "energia" di cui al secondo comma dell'art. 624 c.p. alle sole forme di fruizione dell'energia che siano suscettibili di impossessamento. La più recente giurisprudenza in tema di reati contro il patrimonio ha affermato che per "cosa mobile" deve intendersi *«qualsiasi entità di cui sia possibile la fisica detenzione, sottrazione, impossessamento*

[323] Così ANTOLISEI, *Manuale di diritto penale*, cit., 381.

[324] Il codice civile del 1942 ha esteso il principio a tutto il campo del diritto civile, inserendo una disposizione ad hoc in apertura del libro III. Cfr. Art. 814 c.c. secondo cui *«si considerano beni mobili le energie naturali che hanno valore economico»*

[325] Da ultimo Cass. Pen., Sez. III, 13 maggio 2008, n. 36845 in *Cass. Pen.*, 2009, 3, 944 ss., con nota di SCARCELLA A., *L'inquinamento elettromagnetico tra getto pericoloso di cose e principio di tassatività* in malam partem *in materia penale: un difficile compromesso per affermare la rilevanza penale del fatto*. Il Collegio ribadisce l'orientamento giurisprudenziale prevalente secondo cui nell'espressione "getto di cose" di cui all'art. 674 c.p. rientri mediante una semplice interpretazione estensiva, anche la creazione, l'emissione e la propagazione di onde elettromagnetiche. Nulla infatti osta a che il termine cosa, già di per sé ampiamente generico ed idoneo ad esprimere una pluralità di significati, *«comprenda anche le energie, che sono pacificamente dotate, al pari delle* res quae tangi possunt*, di fisicità e di materialità e che dunque, sia per la loro attitudine ad essere misurate, percepite ed utilizzate sia per la loro individualità fisica, ben possono essere considerate cose»*.

[326] Un orientamento in passato dominante in giurisprudenza riteneva che l'utilizzo del telefono d'ufficio per ragioni private da parte del pubblico funzionario integrasse gli estremi del reato di peculato comune. Cfr. Cass. Pen., Sez. VI, 15 gennaio 2003, n. 10671 secondo cui l'oggetto della condotta appropriativa sarebbe rappresentato dall'energia occorrente per le conversazioni la quale, possedendo valore economico, può costituire oggetto materiale del peculato in virtù della sua equiparazione alla "cosa mobile", con conseguente definitiva appropriazione, da parte del pubblico funzionario, degli impulsi elettrici,

od appropriazione e che possa essere trasportata da un luogo ad un altro»[327], precisando che vi rientrano le sole energie *«che vengono captate dall'uomo, mediante l'apprestamento di mezzi idonei»*; deve dunque trattarsi di *«una forza della natura misurabile in denaro, per cui deve esservi sia un soggetto che la controlla, sia un soggetto disposto normalmente a versare un corrispettivo per averla in godimento»*[328]. Sulla scorta di queste considerazioni si tende ad escludere che i beni immateriali personali (vita, onore, prestigio, etc.) o patrimoniali (opere dell'ingegno, *software*, dati informatici invenzioni industriali, *know-how*, ditta, insegna, marchio) siano annoverabili tra le cose.

Dal punto di vista tecnico-informatico la valuta virtuale è un segmento di dati informatici, una stringa di bit registrata su un sistema di registri distribuiti, la cui registrazione avviene attraverso una pluralità di impulsi elettronici. Il valore economico di questi ultimi – si badi bene – non dipende dal *quantum* di energia trasmessa, ma dalla rappresentazione digitale che è alla base della sua creazione: informazioni che acquisiscono valore in virtù di una convenzione sociale, non suscettibili di sfruttamento economico come "energia".

La valuta virtuale non può tecnicamente essere oggetto di sottrazione, poiché manca il requisito della previa detenzione da parte del titolare[329]. Questi non esercita alcun potere di fatto sul *token*, ma soltanto un potere dispositivo attraverso l'utilizzo delle chiavi crittografiche[330]. Circoscritto il campo di indagine alle condotte di indebita sottrazione della chiave crittografica privata, i termini della questione rimangono pressoché invariati. Le moderne tecniche di crittografia consentono di risolvere il problema della genuinità e della provenienza delle comunicazioni informatiche, assicurando l'immodificabilità del contenuto e la certezza dell'autore del messaggio. Il meccanismo è basato sulla cifratura dei dati e dei documenti informatici per mezzo di impronte alfanumeriche delle quali una parte delle quali è resa pubblica agli utenti del servizio, mentre l'altra è conosciuta dal solo soggetto a cui l'informazione si riferisce. La *private key* consiste in una sequenza di caratteri, di formato differente a seconda

[327] Così, Cass. Pen., 11 maggio 2010, n. 20647 in *Guida al diritto* 2010, fasc. 38, 90 ss. con cui i giudici di legittimità hanno ritenuto che oggetto materiale del reato di appropriazione indebita non possa essere il bene immateriale, come la proprietà industriale o le opere dell'ingegno, che, semmai, possono essere oggetto di appropriazione con riferimento ai documenti intesi nella loro cartacea fisicità che detti beni immateriali contengano e riportino.

[328] In questo senso Cass. Pen., Sez. Un., 2 maggio 2013, n. 19054, § 4.3, in *Diritto penale contemporaneo*, 12 maggio 2013, con nota di BENUSSI C., *Il pubblico funzionario che fa uso del cellulare di servizio per fini privati risponde di peculato d'uso.*

[329] Il previo possesso del bene-energia da parte del proprietario è ritenuto dalle Sezioni Unite uno degli indicatori fondamentali per delineare i confini della nozione penalistica di cosa in relazione alle forme di energia "a propagazione" (onde elettromagnetiche, impulsi elettronici, segnali di rete etc.). Nel caso di specie il Collegio ha ritenuto che il segnale telefonico non sia suscettibile di appropriazione, escludendo così la configurabilità del peculato.

[330] Nessuno potrebbe mai appropriarsi l'informazione, eccetto il proprietario di una infrastruttura centralizzata. Nel qual caso si ritiene configurabile il delitto di appropriazione indebita (art. 646 c.p.) qualora questi decida, ad esempio, di scollegare i *server* dalla rete senza giustificato motivo impedendo agli utenti di utilizzare i valori virtuali.

della tecnica di cifratura utilizzata, che giuridicamente costituisce un "dato informatico"[331].

Il dibattuto sulla riconducibilità di quest'ultimo alla nozione penalistica di "cosa" risale all'epoca precedente all'introduzione del delitto di danneggiamento di informazioni dati e programmi informatici (art. 635-*bis* c.p.)[332], in cui si era posto il dubbio sull'applicazione della fattispecie di danneggiamento comune alla cancellazione di informazioni dalla memoria del *computer*. Da più parti si era paventato il rischio di una analogia *in malam partem*[333] rispetto a quei danneggiamenti logici che non avessero reso realmente inservibile l'elaboratore. La dottrina più attenta[334] proponeva di distinguere la specifica aggressione all'integrità del *software* dalle ipotetiche conseguenze che essa è in grado di produrre sull'utilizzabilità dell'*hardware*, contestando l'assimilazione giurisprudenziale tra la cancellazione di un dato e la "manomissione di dischi" anche se operata attraverso semplici alterazioni magnetiche.

Tali condotte difficilmente integrano un danneggiamento o una manomissione del supporto materiale o dell'impianto in cui avviene la elaborazione di dati[335]. Specialmente nella fase di trasmissione appariva ancor più evidente l'irriducibilità al concetto di "cosa", essendo il *software*, e più in generale, il dato informatico, estraneo alla nozione di "energia"[336]. Essa postula l'idea di consumabilità, diminuzione o trasformazione a cui corrisponde – nella descrizione tipica del furto – un depauperamento del soggetto passivo come conseguenza dell'utilizzazione e godimento della stessa da parte del ladro. La sottrazione delle chiavi crittografiche – che, come vedremo, può avvenire in diversi modi – non modifica neppure in parte l'*ubi consistam* del dato informatico. La perdita della disponibilità economica si ha soltanto con l'utilizzo della chiave per effettuare una transazione verso un nuovo indirizzo; fino

---

[331] Il legislatore codicistico si riferisce ai dati informatici in numerose disposizioni (artt. 615-*quinquies*, 635-*bis*; 640-*ter c*.p.) senza tuttavia fornirne una definizione. In mancanza di una nozione giuridica si può far riferimento all'accezione comune del termine inteso come *«informazione elementare codificabile o codificata»*. Cfr. Enciclopedia online Treccani, voce *Dato informatico*, in https://treccani.it

[332] Il reato consistente nel fatto di *«chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui ovvero programmi, informazioni o dati altrui»*, fu introdotto dalla legge 23 dicembre 1993 n. 547 e poi successivamente modificato dalla legge 18 marzo 2008 n. 48.

[333] In dottrina per tutti v. PECORELLA, C., *Il diritto penale dell'informatica*, Padova, 2006, 195 ss. La giurisprudenza maggioritaria era tuttavia di diverso avviso. Una nota pronuncia delle Sezioni Unite sulla successione di leggi penali nel tempo (Cass. Pen., 09 ottobre 1996, n. 1282 in *Cass. Pen.*, 1997, 2428 ss.) aveva infatti ribadito che la condotta consistente nella cancellazione di dati dalla memoria di un *computer* integrasse un'ipotesi di danneggiamento ai sensi dell'art. 635 in quanto, mediante la distruzione di un bene immateriale, si produceva l'effetto di rendere inservibile l'elaboratore. Veniva dunque affermato che tra il delitto di cui all'art. 635 e l'analoga speciale fattispecie criminosa prevista dall'art. 635-*bis* esistesse un rapporto di successione meramente modificativa.

[334] Tra cui PICOTTI L., *La rilevanza penale degli atti di «sabotaggio» ad impianti di elaborazione dati*, in *Diritto dell'informazione e dell'informatica*, 1986, 3 969 ss. il quale denunciava il pericolo di cadere facilmente nell'elusione del principio di tassatività di fronte alle nuove manifestazioni della criminalità informatica.

[335] Si poneva comunque il problema di garantire una tutela del dato informatico in quanto tale, come bene immateriale a rischio di cancellazione o soppressione, indipendentemente dalla perdurante integrità ed idoneità funzionale dell'*hardware* e dalla memorizzazione sui supporti magnetici.

[336] PICOTTI., *La rilevanza penale degli atti di «sabotaggio»*, cit., 974

a quel momento il soggetto passivo può rientrare in possesso delle somme, qualora disponga di una copia di *back-up* della stringa di codice[337]. L'effettivo "impossessamento" si configura soltanto al momento dell'intervento senza diritto sui dati registrati in *blockchain*, attività assolutamente necessaria per sottrarre definitivamente la ricchezza al controllo dell'avente diritto[338].

In conclusione, riteniamo che la sussunzione dell'indebita sottrazione di valuta virtuale nella fattispecie di furto si scontri contro due ostacoli significativi: uno di carattere normativo, l'altro di ordine logico.

Per far fronte all'impossibilità di ricondurre le rappresentazioni digitali di valore nel concetto penalistico di "cosa", anche se riferito all'energia, sarebbe sufficiente una specifica previsione legislativa in tal senso. L'intervento del legislatore non farebbe tuttavia venir meno le difficoltà applicative dello schema tipico del furto (sottrazione/impossessamento) il cui corretto funzionamento postula l'esistenza di rapporto di signoria sul bene di una sfera di controllo dominicale che, a nostro avviso, mal si concilia con queste nuove forme di *smart property*. Se spetta al legislatore farsi carico delle emergenti esigenze di tutela della ricchezza virtuale, appare comunque doveroso predisporre un presidio penale che sia coerente rispetto al funzionamento dei nuovi ritrovati tecnologici.

5.2.1. Portafogli elettronici e indebita sottrazione di valuta virtuale. Chiarimenti in ordine ai reati configurabili tra accesso abusivo a sistema informatico e frode informatica aggravata.

La sussunzione nella fattispecie di frode informatica (art. 640-*ter* c.p.) permette di ricondurre il fenomeno in esame allo schema commissivo tipico dei reati informatici, eliminando alla radice ogni criticità applicativa.

Si possono distinguere tante forme di realizzazione dell'indebita sottrazione di valuta virtuale quante sono le modalità di conservazione delle chiavi crittografiche. Il portafoglio elettronico (*e-wallet*) è quel programma o dispositivo in cui sono memorizzate le chiavi pubbliche (*currency address*) e le chiavi private; ne esistono varie tipologie, ciascuna dotata di proprie specifiche tecniche[339], da cui derivano

[337] La sottrazione della valuta virtuale è possibile anche senza che la vittima sia privata della disponibilità della chiave crittografica privata, facendo un semplice "duplicato" delle informazioni, ottenuto il quale il ladro potrà controllare l'indirizzo e disporre un ordine di pagamento in proprio favore.

[338] Il tema sarà approfondito in relazione alle particolari modalità operative delle misure di ablazione patrimoniale (sequestro e confisca) aventi a oggetto valori virtuali (v. *infra,* Cap. V, § 7).

[339] Tra le tipologie più diffuse possono annoverarsi: il *desktop wallet*, una volta installato nel computer permette all'utente di archiviare le chiavi private e di inviare/ricevere valuta virtuale; il *mobile wallet*, applicazione installata su uno smartphone con le stesse funzionalità del precedente; il *web wallet*, un portafoglio *online* gestito da un fornitore di servizi e accessibile tramite la rete Internet; l' hardware wallet, un device elettronico in cui vengono archiviate le chiavi crittografiche per garantire la massima sicurezza; il *paper wallet*, semplice foglio di carta contenente un codice QR o una stringa di caratteri identificativa delle chiavi pubbliche e private. In argomento v. DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 101.

differenti livelli di sicurezza. Gli utenti utilizzano solitamente *desktop* o *web wallet* per i pagamenti ordinari, mentre quelli su supporti *hardware* esterni sono preferiti per la conservazione nel lungo periodo.

Quale che sia concreto utilizzata, può notarsi come l'appropriazione della ricchezza si realizza all'esito di due azioni ontologicamente e cronologicamente distinte: l'introduzione abusiva nel sistema informatico in cui si trova il portafoglio elettronico, per ottenere copia delle chiavi private; e l'intervento senza diritto su dati e informazioni al fine di sottrarre alla vittima la disponibilità dei valori virtuali. Quanto alla prima condotta, appare pienamente configurabile il reato di accesso abusivo *ex* art. 615-*ter* c.p. indipendentemente dalle modalità commissive del fatto[340]. Il presidio penale si estende ai soli sistemi protetti da misure di sicurezza, presupposto assolutamente ricorrente nel caso in esame, in cui gli applicativi *web* di più ampia diffusione[341] richiedono di *default* una password per accedere all'area riservata di gestione del conto. Alcuni fatti di cronaca cui abbiamo fatto riferimento[342] dimostrano come quella appena descritta sia la tipologia di attacco preferita dai criminali informatici che, sfruttando le vulnerabilità nei sistemi di sicurezza dei più noti *exchange*, sono spesso riusciti ad ottenere l'accesso ai conti di un nutrito numero di conti.

L'introduzione abusiva e l'esfiltrazione delle chiavi private rappresentano la prima fase di un più ampio disegno criminoso, che culmina con l'utilizzo dei codici per movimentare le somme verso un nuovo indirizzo di conto controllato dal reo. Tale condotta integra appieno gli estremi della frode informatica, ben potendosi ravvisare nella spendita delle chiavi per trasferire valori sulla *blockchain* un intervento senza diritto sulle valute virtuali, *rectius* sui dati informatici che le compongono[343].

Questa soluzione ermeneutica appare sicuramente più persuasiva della prima, presentando anche il pregio di poter essere applicata a tutte condotte astrattamente ipotizzabili. Si pensi ad esempio all'appropriazione di una quantità di criptomoneta i cui estremi di accesso (indirizzo e chiave privata di criptazione) sono custoditi in un *paper wallet*, vale a dire un comune foglio di carta. La condotta "furtiva" consisterà in questo caso nel semplice utilizzo dei codici appuntati per trasferire le valute ad un altro indirizzo, azione di per sé sufficiente ad integrare un intervento senza diritto sui dati informatici[344].

---

[340] Potrà infatti trattarsi di tanto di un'azione compiuta da remoto quanto di un fatto realizzato nel luogo in cui si trova il sistema informatico.

[341] Il richiamo è ai *web wallet* e agli *hot storage* messi a disposizione da piattaforme di scambio. Questi *provider*, come si è visto, svolgono anche le funzioni di prestatori di servizi di portafoglio elettronico.

[342] Cfr. *supra*, § 5 a proposito degli attacchi che hanno colpito Mt. Gox e Bitfinex, causando danni per centinaia di milioni di dollari.

[343] L'oggetto materiale della condotta è descritto con riferimento ai «dati, informazioni o programmi contenuti in un sistema informatico», nozione che non lascia alcun dubbio sull'applicazione nel caso in esame.

[344] Per "intervento senza diritto" si intende ogni azione che produca una qualche modifica ai regolari processi dell'elaboratore. L'espressione "senza diritto" può assumere due differenti significati, indicando l'assenza del consenso del titolare dei dati, informazioni e programmi contenuti nel sistema informatico, oppure una modalità di azione non consentita da norme giuridiche, né da altre fonti.

Riteniamo che le condotte *de quibus* debbano essere punita con la pena più severa di cui al terzo comma dell'art. 640-*ter* c.p., che prevede l'aggravante del furto o dell'indebito utilizzo dell'identità digitale[345]. Vi è infatti motivo di credere che la crittografia asimmetrica a doppia chiave utilizzata dai moderni circuiti di pagamento – in valuta virtuale, ma anche e soprattutto in denaro – assolva precipuamente alla funzione di identificare il soggetto che emette l'ordine di pagamento.

All'interno di una infrastruttura tecnologica, la chiave privata assume quindi le caratteristiche di un documento di riconoscimento, sicché l'utilizzo indebito da parte di soggetti terzi non autorizzati si traduce in una appropriazione dell'identità digitale del legittimo possessore. L'affermazione richiede un rapido *excursus* sulla tutela penale dell'identità digitale e sulle diverse forme che essa può assumere.

L'identità nel mondo digitale viene intesa quale bene-valore, costituito dalla proiezione sociale dell'individuo nella rete. Essa può assumere connotazioni personalistiche[346], ma anche meramente informatiche. Alcuni parlano di *identità digitale imposta*[347] per descrivere l'insieme di dati informatici gestiti da enti terzi, quali istituzioni pubbliche o società private, utilizzati essenzialmente per fini commerciali o istituzionali[348]. Questa particolare forma di identità/autenticazione può essere considerata una evoluzione dell'identità digitale in senso personalistico: si tratta della c.d. *identità informatica,* vale a dire l'insieme delle informazioni che danno luogo a un apposito sistema di autenticazione, che si attua tramite una parola chiave, la c.d. *password*, oppure attraverso caratteristiche biologiche (*fingerprint*, *face detection* etc). A tale accezione sembra essersi ispirato il legislatore nell'introdurre tra le disposizioni definitorie del D. Lgs. 82/2005 (Codice dell'amministrazione digitale) una nozione di

[345] Il decreto legge 14 agosto 2013, n. 93 (art. 9, co. I, lett. a) convertito con modificazione con legge 15 ottobre 2013, n. 119 ha introdotto, all'interno dell'art. 640-*ter* c.p., una nuova circostanza aggravante ad effetto speciale del delitto di frode informatica: *«La pena è della reclusione da due a sei anni e della multa da euro seicento a euro tremila se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti».* La formulazione testuale della disposizione presta il fianco a diverse critiche. Il riferimento al "furto" non allude alla fattispecie di cui all'art. 624 c.p. essendo l'identità qualcosa di incorporale che non può costituire oggetto di sottrazione e impossessamento. Appare evidente il tentativo del legislatore di "materializzare" l'identità personale in rete come se fosse riferita i dati personali, attraverso i quali il soggetto proietta sé stesso nel mondo digitale. Con l'espressione furto d'identità il legislatore ha probabilmente inteso richiamare la definizione fornita dall'art. 30-*bis* del D. Lgs. 13 agosto 2010, n. 141, intendendo tale l'*impersonificazione totale* (occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto) e l'*impersonificazione parziale* (occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto).

[346] Alcuni parlano di *identità digitale progettata* per scrivere quella creata da ciascun individuo, che ne determina autonomamente il contenuto (*nickname* e personalità frutto della fantasia) e di *identità digitale ibrida* deriva dalle connessioni sociali alle quali un individuo partecipa via web (es. profilo personale sui *social network*). Cfr. CLARKE R., *The Digital Persona and its Application to Data Surveillance*, in *The information Society*, 1994 10, 77 ss.; RESTA G., *L'identità digitale e l'identità personale*, in *Diritto dell'informazione e dell'informatica*, 2007, 3 511 ss.

[347] ROSENDAAL A., *Digital personae and profiles as representations of individuals*, in BEZZI M., DUQUENOY P., FISCHER-HÜBNER S. (a cura di), *Privacy and identity management for life*, Tilburg, 2010, 226 ss.

[348] Si pensi, ad esempio, al Sistema pubblico di identificazione (SPID).

identità digitale come *«rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale»*[349]. Il riferimento all'indeterminato concetto di "attributi identificativi" e la verifica attraverso "dati raccolti e registrati in forma digitale" sembrerebbe includere nel perimetro definitorio tutte le procedure informatiche attraverso cui è possibile l'autenticazione di un soggetto previamente identificato.

Per delineare correttamente il campo di applicazione della circostanza aggravante in esame, si dovrà leggere il terzo comma dell'art. 640-*ter* c.p. in combinato disposto con l'art. 30-*bis* del D. Lgs. 141/2010 che parla di "impersonificazione totale e parziale" come espediente che si realizza *«mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto»*.

Risulta tutt'altro che agevole tracciare una linea di demarcazione tra "furto"' e "utilizzo indebito". Avvalorando la disgiunzione "o" utilizzata dal legislatore, sembra possibile tracciare un *discrimen* tra le due condotte tale per cui, se nel secondo manca la apprensione di dati identitari, nel primo si realizza la perdita di disponibilità da parte del legittimo titolare delle credenziali di autenticazione. Applicando il principio al caso oggetto d'esame si avrà che, laddove l'acquisizione della chiave privata sia stata realizzata tramite la mera "duplicazione" (che non sottrae alla vittima la possibilità di utilizzare i propri dati) il successivo impiego darà luogo a un indebito utilizzo dell'identità digitale; nel diverso caso in cui l'esfiltrazione dei dati abbia spogliato la vittima delle credenziali di autenticazione, ricorrerà invece una ipotesi di furto di identità digitale[350].

Occorre infine dar conto dell'indeterminatezza della definizione legislativa di identità digitale. Intendendo la stessa come rappresentazione informatica della corrispondenza tra un "utente" e informazione di autenticazione (art. 1, lett. u-*quater* cit.), sembra che il legislatore non abbia ritenuto necessaria la previa identificazione della persona fisica a cui il profilo informatico si riferisce. Ciò potrebbe produrre delle conseguenze significative per l'estensione della circostanza aggravante alle ipotesi di indebita sottrazione di valuta virtuale. Il raggio applicativo dell'aggravante andrebbe difatti a includere tutte quelle frodi informatiche commesse su dati, programmi e informazioni che individuino univocamente l'utente di una piattaforma, sebbene lo stesso non sia stato nominativamente individuato.

La possibilità di sussumere le condotte di indebita sottrazione di valuta virtuale nell'art. 640-*ter* c.p. segna, a nostro avviso, un punto importante in favore della scelta del legislatore del 1993 di garantire una tutela ampia del patrimonio contro le possibili forme di abuso dei sistemi informatici. La previsione di un reato di evento, caratterizzato da una condotta generalmente descritta in termini di alterazione del funzionamento o intervento senza diritto sui dati, rende il paradigma punitivo sufficientemente elastico, di modo che possa adattarsi alla mutevolezza delle ipotesi di

[349] Art. 1 lett. u-*quater* del D. Lgs. 82/2005 come modificato dal D.lgs. 13 dicembre 2017 n. 217.

[350] Il trattamento sanzionatorio rimane peraltro invariato, dal momento che norma accomuna *quoad poenam* il furto e l'indebito utilizzo dell'identità digitale.

attacco informatico e alla rapidità dell'evoluzione tecnologica. Così è stato per la tutela penale delle componenti patrimoniali "virtualizzate" per la quale non sembra necessario un nuovo intervento da parte del legislatore.

5.2.2 L'appropriazione indebita di chiavi crittografiche da parte del fornitore di servizi di portafoglio digitale.

Date tali premesse, risulta piuttosto agevole escludere la configurabilità del delitto di appropriazione indebita nell'ipotesi in cui il fatto sia commesso dal gestore del servizio di portafoglio digitale. Questi come noto, è il soggetto che *«fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali»* (art. 1, n. 2, lett. Direttiva 2018/843/UE; art. 1, comma 2, lett. ff-*bis*) D. Lgs. 231/2007).

Se ragionassimo secondo gli schemi tradizionali della sistematica dei delitti contro il patrimonio, affermeremmo che coloro che custodiscono le chiavi crittografiche ne hanno pure il "possesso". Secondo la dottrina maggioritaria tale istituto, ricostruito in chiave penalistica, consiste nell'esercizio di un potere di fatto al di fuori della sfera di sorveglianza di chi abbia sulla cosa un potere giuridico maggiore[351]. La presenza attuale di un tale potere permette di distinguere le condotte di appropriazione di tipo furtivo – nella quali la vittima è spogliata del possesso – da quelle connotate da abuso del titolo di legittimazione[352]. Sennonché, l'applicazione dell'art. 646 c.p. si scontra contro il dato letterale che descrive l'oggetto materiale dell'appropriazione indebita con riferimento al *«denaro o la cosa mobile altrui»*. Circa l'impossibilità di ricondurre la chiave di criptazione al concetto di cosa mobile si è già approfonditamente detto nel corso del paragrafo. Non pare del resto necessario doversi soffermare oltre sulla nozione di denaro, essendo già stato chiarito in corso d'opera[353] come esso si riferisca alla sola moneta avente corso legale.

Al di là dei limiti testuali, le difficoltà applicative derivano anche dalla particolare evanescenza del possesso in relazione ai valori virtuali. Le perplessità maggiori sorgono con riferimento all'esercizio della signoria sul bene al di fuori del controllo del *dominus*[354]. L'accesso all'area personale (*account*) nella quale sono registrati gli indirizzi di portafoglio è di esclusiva pertinenza dell'utente, sicché neppure il gestore potrebbe accedervi senza prima aver ottenuto i necessari permessi. Il *provider* del servizio si limita a mettere a disposizione uno spazio di archiviazione e una interfaccia grafica, accompagnati da particolari prerogative di sicurezza, senza alcuna "salvaguardia" attiva dei valori virtuali; la definizione fornita dal legislatore europeo

[351] Così ANTOLISEI, *Manuale di diritto penale,* cit., 299

[352] . La distinzione permette anche di spiegare la presenza del delitto di appropriazione indebita (art. 646 c.p.) tra i delitti contro il patrimonio commessi mediante frode.

[353] *Amplius,* in questo capitolo, § 1.5.

[354] L'utente del servizio potrebbe aver ottenuto un duplicato informatico delle chiavi, circostanza di per sé sufficiente a far ritenere la sua situazione possessoria ancora in essere.

risulta, da questo punto di vista, piuttosto imprecisa. Ad ogni modo, importa rilevare come l'eventuale appropriazione dei valori *invito domino* non sarebbe realizzata al di fuori della sfera di controllo dell'utente, che è l'unico a poter accedere alla propria area privata e a poterlo fare in ogni momento, anche, da remoto[355]. Sul piano logico si impone una distinzione tra la proprietà del *server* sul quale sono registrate le informazioni e la disponibilità delle stesse, poiché l'appartenenza giuridica del contenitore non si estende al contenuto[356].

Venuta meno la suggestiva tesi dell'appropriazione indebita, la condotta del *provider* andrà ricondotta alle fattispecie già esaminate: potrà dunque essere ritenuto responsabile di accesso abusivo a sistema informatico e di frode informatica unite dal vincolo della continuazione *ex* art. 81, comma 2, c.p.

Non osta all'applicazione dell'art. 615-*ter* la circostanza che l'accesso sia effettuato da proprietario del sistema, dovendosi per converso attribuire rilevanza al dissenso implicito del titolare dello *ius excludendi alios*, vale a dire l'utente, a che terzi non autorizzati facciano ingresso nel proprio domicilio informatico protetto da misure di sicurezza. Né varrebbe ad escludere l'integrazione del reato la circostanza che il *provider,* in quanto operatore di sistema, sia astrattamente legittimato all'accesso; la giurisprudenza di legittimità[357] ammette, ormai pacificamente, la configurabilità del reato a carico del soggetto che, pur essendo abilitato, violi le condizioni e i limiti imposti dal titolare del diritto di esclusione[358], utilizzando le credenziali per ragioni ontologicamente diverse rispetto a quelle per le quali l'utilizzo gli è consentito. Il possesso della qualifica di *system operator* renderà anzi punibile il fatto in modo più severo ai sensi del secondo comma dell'articolo.

Quanto al secondo titolo di responsabilità, risulta fin troppo evidente come l'azione del *provider* costituisca un intervento senza diritto sui dati dell'utente. Anche questo reato potrà ricorrere in forma aggravata – *ex* art. 61 n. 11 c.p. – per abuso della prestazione d'opera da parte del *provider*[359]. In entrambi i casi l'aggravamento di pena appare ben giustificato dal maggior disvalore della condotta posta in essere da chi avrebbe il dovere di salvaguardare i dati informatici altrui contro possibili abusi.

---

[355] Esemplificando, sarebbe come se il custode di un complesso residenziale, munito di *passpartout* per far fronte a eventuali emergenze, in assenza dei proprietari facesse ingresso nelle pertinenze di una abitazione per appropriarsi di una autovettura. Sarebbe piuttosto arduo negare la responsabilità di costui a titolo di furto in abitazione, facendo leva sulla asserita esistenza di una signoria di fatto sul bene.

[356] Potremmo addurre l'esempio del banchiere che, mediante scasso di una cassetta di sicurezza, si appropriasse il contenuto. Quest'ultimo dovrebbe rispondere di furto, e non si appropriazione indebita.

[357] Il contrasto interpretativo che era insorto sulla configurabilità del reato di cui all'art. 615-*ter* c.p. in caso di abuso del titolo di legittimazione è stato risolto da Cass. Pen., Sez. Un. 27 ottobre 2011, n. 4694, Casani, con cui la Corte di Cassazione ha affermato principi che, pur con alcuni adeguamenti successivi, formano oggi il diritto vivente.

[358] Non si deve infatti incorrere nell'errore di confondere il titolare del sistema con il titolare dello *ius excludendi* figure soggettive che, se spesso sono rappresentati dallo stesso soggetto, in molti casi potrebbero anche non coincidere.

[359] L'abuso della relazione di prestazione d'opera è configurabile in presenza di rapporti giuridici, anche fondati sulla fiducia, che a qualunque titolo comportino un vero e proprio "obbligo" per il fiduciario.

5.3. Una ipotesi residuale di applicazione dell'art. 624 c.p.? Il *mining* abusivo tra furto, frode informatica e truffa comune.

L'aumento del prezzo dei valori virtuali rende progressivamente più conveniente prendere parte al processo di *mining*, attività che garantisce una ottima remunerazione del capitale investito per l'acquisto degli apparecchi e dell'energia elettrica[360]. La potenza computazionale necessaria a vincere la "gara" di calcolo – perlomeno nel sistema Bitcoin – è cresciuta significativamente negli ultimi anni. Se ciò, da un lato, limita le possibilità di accesso al mercato, riservandolo ai soli operatori disposti a sostenere un ingente investimento o a consorziarsi con altri, dall'altro accresce la propensione verso forme di sfruttamento abusivo della potenza di calcolo di sistemi informatici e telematici altrui.

Con l'espressione *mining* abusivo, sorto in conseguenza dell'apprezzamento della criptomoneta e della corrispondente maggiore difficoltà di "estrazione" dei valori, si indica quel particolare fenomeno consistente nello sfruttamento dell'energia computazionale di terze parti al fine di validare transazioni senza il consenso del titolare del sistema informatico. L'indebita sottrazione delle risorse è attuata mediante artifici volti a dissimulare la presenza, all'interno del sistema, di un *software* deputato a processare le transazioni per conto dell'autore del programma; possono distinguersi due diverse forme di *mining* abusivo, in base all'espediente in concreto utilizzato.

La più importante, che potremmo definire *"malware mining"*, sfrutta espedienti di ingegneria sociale per indurre la vittima a installare sul proprio dispositivo un *software* apparentemente innocuo. Una volta entrato in funzione il programma viene eseguito in *background* per prendere parte al processo di "estrazione" di valuta virtuale, iniziando così a "prosciugare" le risorse di rete e la potenza di calcolo del *device* infettato. Le funzionalità del *malware* sono controllate da remoto dagli ideatori del programma ai quali spetteranno tutti i vantaggi economici dell'attività "mineraria".

Il *mining* abusivo assume di solito dimensioni assai estese e si inserisce in un *iter criminis* complesso, caratterizzato da più azioni, commesse anche in tempi diversi, in esecuzione di un medesimo disegno criminoso. L'attacco richiede una fase preparatoria molto lunga, che può durare talvolta mesi o addirittura anni, e culmina con la creazione di una *Botnet*, vale a dire una rete di computer "zombie" controllata dall'*hacker* che l'ha istituita (detto *botmaster*)[361]. Per raggiungere una potenza di calcolo sufficiente a

[360] Vi è chiaramente un rapporto di proporzionalità diretta tra l'aumento del prezzo di scambio dei valori virtuali e la remunerazione del capitale investito. Secondo alcuni l'aumento dei costi di produzione rappresenta uno dei "driver tecnici" che determinano l'andamento del prezzo di Bitcoin. La difficoltà nell'ottenere l'*hash* di transazione cresce in difficoltà nel tempo, facendo aumentare la potenza computazionale necessaria per risolvere l'equazione matematica alla base della costruzione della catena dei blocchi; ciò a sua volta aumenta il costo delle attrezzature e la spesa in elettricità. È quindi dato ipotizzare che, in alcune fase del suo sviluppo, le maggiori spese di estrazioni abbiano contribuito all'aumento esponenziale del prezzo.

[361] Le *botnet* sono un veicolo per la commissione di reati informatici, rispetto ai quali la costruzione di una rete di devices zombie è spesso funzionale. Grazie ad esse i *botmaster* possono commettere diverse tipologie di illecito (spam, attacchi di *denial-of-service*, mining abusivo) o perfino vendere sul mercato

prender parte al processo di *mining* l'attaccante dovrà avere il controllo di migliaia dispositivi simultaneamente attivi. Per questo motivo il programma viene diffuso in rete, in modo gratuito, utilizzando nomi e loghi di applicazioni di uso comune, e attivato soltanto quando avrà raggiunto un numero sufficiente di utenti[362].

Data la complessità dell'attacco informatico in esame, ci si domanda quali siano le conseguenze in punto di responsabilità penale. Invero, già la diffusione di virus su larga scala nel tentativo di 'accalappiare' il maggior numero possibile di 'zombie' è sussumibile nel fatto descritto dall'art. 615-*quinquies* c.p., che punisce, tra le altre, la condotta di diffusione di programmi informatici commessa allo scopo di alterazione il funzionamento di un sistema informatico[363].

Laddove il *botmaster* riesca ad assumere il controllo dei *devices*, lucrando i proventi del *mining* abusivo, risponderà anche di frode informatica *ex* art. 640-*ter* c.p. Non pare infatti revocabile in dubbio né l'evento della realizzazione di un ingiusto profitto, né quello della verificazione dell'altrui danno. Deve però darsi conto della differenza ontologica tra i due eventi naturalistici, in quanto il danno per la vittima è rappresentato dal maggior dispendio di energia e risorse computazionali, mentre il profitto del reo consiste della quantità di valuta virtuale indebitamente "minata" dai dispositivi infetti[364]. Se le funzionalità del programma-virus non sono state attivate il fatto sarà punibile a titolo di tentativo; la presenza di uno script maligno nel *software* diffuso in rete – unita alla possibilità tecnica di attivazione a distanza – appare di per sé sufficiente a integrare i presupposti della idoneità e della univocità degli atti a commettere la frode informatica.

Certamente più problematico è l'elemento dell'alterazione del funzionamento del sistema informatico. La giurisprudenza ritiene che l'alterazione possa essere ottenuta agendo sul *software*, cioè su programmi, dati, informazioni installati e memorizzati in un apparato con capacità di elaborazione, ovvero operando sull'*hardware*, cioè sulle parti elettroniche, meccaniche, magnetiche, ottiche che ne consentono il

---

la disponibilità temporanea della rete a chi fosse interessato ad utilizzarla per commettere reati (c.d. *crime-as-a-service*).

[362] I *botmaster* possono anche controllare i computer infetti tramite sofisticate reti *peer-to-peer*. In risposta agli sforzi effettuati per individuare ed eliminare i botnet tradizionali – costruite secondo il modello client-server – gli attaccanti hanno iniziato a servirsi delle reti *peer-to-peer* come alternativa per continuare a distribuire *malware*. Piuttosto che comunicare con un server centralizzato, i bot P2P si configurano sia come un *server* per eseguire comandi, sia come un *client* per riceverli: ciò rende estremamente difficile la loro rimozione.

[363] Più precisamente la disposizione punisce con la reclusione fino a due anni e con la multa sino a euro 10.329 «*chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici*».

[364] La circostanza che i due eventi si riferiscano a oggettività materiali distinte non è tuttavia di ostacolo all'applicazione della fattispecie. La disposizione non richiede un legame di diretta interdipendenza tra profitto e danno; sarebbe dunque un errore di immaginare profitto e danno come "due facce della stessa medaglia". Trattandosi di requisiti dotati di autonomia l'accertamento processuale dovrà estendersi ad entrambi, senza poter ritenere implicito il profitto nel verificarsi del danno.

funzionamento, in modo tale da far compiere operazioni diverse rispetto a quelle per le quali la macchina è stata programmata[365]. L'elemento oggettivo consiste dunque in una manipolazione dei dati contenuti nel sistema o delle sue componenti fisiche condotte che, a ben vedere, non appaiono necessarie nel caso in esame.

L'attacco informatico si realizza infatti mediante l'induzione in errore della vittima che artificiosamente acconsente all'installazione del *software* malevolo sul proprio dispositivo, senza che il funzionamento dell'elaboratore sia in alcun modo alterato o che sia necessario un intervento senza diritto sui dati o sulle informazioni ivi contenute. Non si potrebbe affermare, se non in modo surrettizio, che il *software* abbia "alterato" il funzionamento di un computer che, in realtà, esegue fedelmente le istruzioni impartite. Il disvalore della condotta si concentra nell'aver carpito con dolo il consenso della vittima facendo uso di espedienti a carattere dissimulatorio: ci si chiede, pertanto, se l'ipotesi di *mining* abusivo non vada piuttosto ricondotta alla fattispecie di truffa comune art. 640 c.p.

L'atto di disposizione patrimoniale della vittima viene qualificato dalla dottrina maggioritaria come elemento che, per quanto implicito, è nondimeno indispensabile per la configurabilità della truffa[366]. A conferma di ciò l'essenza di reato va individuata nella collaborazione artificiosa della vittima, eteroindotta mediante artifici o raggiri, che distingue le ipotesi di frode dagli illeciti c.d. ad aggressione unilaterale. Diversamente opinando la truffa diverrebbe una "fattispecie di rifugio", una clausola generale di tutela del patrimonio da tutte quelle forme di aggressione nelle quali il danno e il profitto seguano in modo automatico alla induzione in errore[367]. Quanto alla estensione concettuale dell'atto di disposizione patrimoniale, si ritiene che assuma rilievo ogni possibile schema negoziale tra cui l'esercizio di diritti di qualunque natura, l'assunzione di obbligazioni o oneri, o l'esecuzione di prestazioni o servizi, purché si tratti di atti aventi un contenuto patrimoniale dai quali dipenda tanto la verificazione di un danno patrimoniale per il disponente e quanto il vantaggio altrui.

In dottrina si è posta la questione del rapporto tra l'elemento dell'induzione in errore e l'atto di disposizione patrimoniale, con particolare riguardo alla necessità o meno della consapevolezza dell'atto dispositivo. Posto che l'errore deve essere la causa dell'atto dispositivo, alcuni autori hanno condivisibilmente inteso tale nesso in senso pregnante, richiedendo che il soggetto passivo abbia formato, come conseguenza della condotta fraudolenta dell'agente, il proprio convincimento in senso distorto rispetto alla realtà e, quindi, proprio sulla scorta di tale erroneo convincimento, abbia compiuto un

[365] Cass. Pen., Sez. II, 6 marzo 2013, n. 13475 secondo cui per alterazione del funzionamento del sistema informatico o telematico deve intendersi «ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei dati e, quindi, sia sull'*hardware* che sul *software*».

[366] Nella manualistica, cfr. MANTOVANI F., *Diritto penale – Parte speciale*, vol. II, Padova, 2018, 206 ss.; ANTOLISEI, *Manuale di diritto penale*, cit., 473; MEZZETTI, *Reati contro il patrimonio*, cit., 378.

[367] In questi termini, ZANNOTTI R, *La truffa*, Milano, 1993, 74.

atto "consapevole" nella propria sfera patrimoniale[368]. Sulla base di queste premesse, non si ritiene che la semplice manifestazione del consenso all'installazione di un programma informatico costituisca una disposizione patrimoniale nel senso sopra descritto. La vittima non è affatto consapevole di aver compiuto un atto dispositivo del proprio patrimonio attraverso un semplice clic all'installazione del programma. A ciò si aggiunga che la produzione dell'ingiusto vantaggio e del danno non derivano in via immediata dalla cooperazione della vittima (come, ad es. nel *phishing*), quanto piuttosto dalla attivazione e dal controllo del programma malevolo da parte dell'agente.

Una diversa e più convincente qualificazione giuridica del fatto potrebbe far leva sulla fattispecie comune di furto, aggravato dall'utilizzo del mezzo fraudolento (art. 625, n. 2, c.p.), che risulta applicabile senza particolari forzature ermeneutiche. Mediante lo sfruttamento delle risorse computazionali del dispositivo l'agente sottrae alla vittima una notevole quantità di energia elettrica, la quale giusta l'equiparazione contenuta nel secondo comma dell'art. 624, rientra tra le cose mobili suscettibili di appropriazione. La particolare modalità esecutiva del reato mette in evidenza come la sottrazione della *res* sia il frutto di una condotta di aggressione unilaterale "ad alto contenuto tecnologico", mentre l'induzione in errore della vittima rappresenta una nota di maggior disvalore di una condotta che, sul piano della tipicità, resta furtiva. Volendo esemplificare, si pensi al cd. "allaccio abusivo" realizzato tramite un cavo a marchio ENEL, che la giurisprudenza di merito ha considerato un'ipotesi di furto aggravato[369]; oppure all'utilizzo di un dispositivo per l'apertura della cassa di un distributore automatico, installato fraudolentemente dall'operatore che ne ha in carico la manutenzione. In entrambi i casi la vittima è indotta a credere che l'intervento (allaccio del cavo o installazione del dispositivo) non importino alcuna conseguenza patrimoniale per cui, mancando l'atto dispositivo, la condotta andrà ricondotta al perimetro applicativo del furto.

La qualificazione del *mining* abusivo come furto aggravato di energia elettrica rileva anche ai fini della consumazione del reato. La giurisprudenza più recente annovera questa particolare tipologia di furto tra i delitti a "consumazione prolungata" o a "condotta frazionata", caratterizzati dal fatto che l'azione si perpetua nel tempo, anche con eventuale soluzione di continuità, con la conseguenza che le plurime captazioni di energia, successive alla prima, costituiscono un *post factum* penalmente irrilevante. Dal punto di vista dell'elemento soggettivo l'autore sin dall'inizio si prospetta la commissione di un'azione durevole nel tempo, per cui le singole ed autonome azioni non sono autonomamente punite, ma vanno intese come singoli atti di un'unica azione furtiva che spostano in avanti la cessazione della consumazione fino

[368] PEDRAZZI C, *Inganno ed errore nei delitti contro il patrimonio*, Milano, 1955, 34 ss., richiamato, sia pur in senso parzialmente critico da ZANNOTTI *La truffa*, cit., 78.
[369] Tribunale Bari, Sez. II, sentenza 4 marzo 2011, n. 468

all'ultimo prelievo di energia, momento da quale inizierà a decorrere il termine prescrizionale[370].

In conclusione, deve darsi conto dell'esistenza di una ulteriore forma di *mining* abusivo, consistente nella mendace prospettazione di un alto rendimento economico derivante dalla volontaria messa a disposizione del dispositivo per il processo di *mining*. Tale condotta, che mutuando una terminologia anglosassone potremmo definire *deceptive mining*, si differenzia dalla precedente per la consapevolezza dell'utente di prendere parte al processo di validazione delle transazioni. Esistono diversi applicativi in rete che consentono di collegare il proprio dispositivo a uno o più *mining rigs*, al fine di accrescere la potenza computazionale necessaria alla risoluzione dei blocchi; in questo modo l'autore del *software* può "cumulare" la capacità di elaborazione dati di migliaia di dispositivi interconnessi, risparmiando sulla spesa per l'acquisto di *hardware* e energia elettrica[371].

In linea di principio non è dato dubitare della liceità di questi programmi, specie laddove l'utente sia messo al corrente del reale funzionamento del programma e del criterio di ripartizione dei profitti generati dall'attività di *mining*. Sennonché, alcune noti fatti di cronaca[372] hanno messo in luce l'esistenza di una totale asimmetria informativa tra professionisti e consumatori, poiché l'utente è mosso dall'aspettativa di un margine di guadagno netto proporzionato alla quantità di energia offerta o al numero di transazioni validate, mentre, nella maggior parte dei casi, gli viene attribuita soltanto una quantità risibile di criptomoneta del tutto slegata dagli esiti positivi del processo di *mining*. L'utente si trova inoltre nella totale inconsapevolezza dell'asservimento delle proprie energie computazionali agli elaboratori altrui, circostanza spesso taciuta in modo antidoveroso.

Si ritiene che il silenzio su questi elementi costituisca una condotta omissiva rilevante per l'integrazione della c.d. *truffa contrattuale*. Non essendo questa la sede opportuna per dar conto delle diverse opinioni espresse dalla dottrina, possiamo limitarci a richiamare il condivisibile orientamento giurisprudenziale secondo cui il silenzio antidoveroso va considerato a tutti gli effetti come un raggiro, tutte le volte in cui contribuisca a rappresentare alla vittima uno stato di fatto idoneo ad incidere sul

[370] In questo senso, Cass. Pen., Sez. IV, 15 novembre 2018, n.53456 che riafferma il principio secondo cui il termine di prescrizione del delitto di furto di energia elettrica decorre dall'ultima delle plurime captazioni di energia, che costituiscono i singoli atti di un'unica azione furtiva a consumazione prolungata

[371] Tali applicazioni hanno riscosso grande successo presso il pubblico, poiché permettono a chiunque, con un investimento davvero minimo, di prendere parte al processo di *mining*. Tra la fine del 2017 e l'inizio del 2018, periodo di massima espansione del mercato valutario virtuale, si contavano centinaia di applicazioni di questo tipo.

[372]Si veda il comunicato stampa Ansa del 20 febbraio 2018, intitolato «Bitcoin: nuova campagna di mining 'abusivo' frutta 3 milioni», in https://ansa.it; ancor più eclatante la notizia del *mining* abusivo effettuato mediante un *software* che ha infettato una centrale nucleare russa riportata dal quotidiano La Stampa, cfr. NEPORI A., *Fanno mining di Bitcoin col supercomputer: arrestati scienziati di una base nucleare russa*, 11 febbraio 2018, in https://lastampa.it. In argomento si vedano anche il libello informativo «Miner occulti su Google Play» pubblicato sul sito di Kaspersky Lab, 04 aprile 2018, https://kaspersky.it.

processo motivazionale, sì da indurla a prestare un consenso che altrimenti non avrebbe dato[373]. Può notarsi come a differenza delle ipotesi di *malware mining*, in questo caso il soggetto passivo è consapevole di compiere un atto di disposizione patrimoniale (nella specie fornitura di energia elettrica e di potenza di calcolo), indotto dalla mendace rappresentazione (anche in forma omissiva) circa le aspettative di guadagno e la funzionalità del *software*. In questo modo gli sviluppatori dell'applicativo potranno realizzare ingenti profitti sfruttando, a buon mercato, le risorse computazionali altrui[374].

Tale schema commissivo ricalca appieno quello tipico della truffa *ex* art. 640 c.p., risultando evidente come il depauperamento patrimoniale sia il frutto della cooperazione della vittima, indotta artificiosamente a compiere un atto dispositivo a tempo indeterminato[375] sulla base di informazioni contrattuali lacunose, imprecise o maliziosamente generiche.

5.4. Frode informatica e sottrazione indebita di valuta virtuale: gli obblighi di criminalizzazione contenuti nella Direttiva 2019/713/UE.

Con l'emanazione della direttiva 2019/713/UE si è compiuto un passo decisivo verso l'armonizzazione delle disposizioni penali di contrasto alle frodi nei mezzi di pagamento diversi dai contanti[376], elevando la valuta virtuale a oggetto meritevole di tutela penale[377]. Allo sguardo lungimirante del legislatore europeo non è sfuggito

[373] In tal caso la omessa comunicazione di informazioni non rileverebbe quale mera omissione, bensì in quanto momento di una più articolata condotta fraudolenta. L'orientamento prevalente in giurisprudenza ammette la configurabilità del delitto di truffa anche nella forma omissiva, limitandosi a richiedere la verifica della avvenuta violazione da parte del soggetto attivo di un obbligo giuridico di rivelare le circostanze taciute e stimando *tout court* tale comportamento di per sé idoneo a trarre dolosamente in errore. Nei casi di c.d. truffa contrattuale l'obbligo giuridico violato può essere contenuto anche in norme *extrapenali* a carattere generale (es. artt. 1173, 1377 c.c.), purché il silenzio maliziosamente serbato cada su circostanze essenziali per la conclusione del contratto, che il soggetto attivo avrebbe dovuto fare conoscere alla controparte contrattuale. Cfr. *ex multis*, Cass. Pen., Sez. II, 9 maggio 2018, n. 23079; Sez. II, 19 ottobre 2017, n. 52441; Sez. II, 19 marzo 2013, n. 28703.

[374] Sull'*eventus damni* è bene precisare che, coerentemente alla concezione economica di "danno", nel caso in esame esiste una netta sproporzione tra il valore patrimoniale delle due prestazioni, poiché a fronte di poche unità (o sottounità) di conto virtuale guadagnate dalle vittime, gli sviluppatori riescono ad ottenere ingenti profitti impiegando l'energia elettrica altrui. Vi è inoltre un filone minoritario della giurisprudenza che, partendo da una nozione "dematerializzata" del danno, ritiene sufficiente che il contraente sia addivenuto, a causa dello stato di errore, alla stipulazione del contratto che, senza la condotta truffaldina altrui, non avrebbe invece concluso, così prescindendo dalla effettiva diminuzione patrimoniale (Cass. Pen., Sez. II, 8 febbraio 2011, n. 21000).

[375] Per determinare il momento consumativo del reato sembra possibile anche qui ricorrere al paradigma dei reati a consumazione prolungata sulla base dell'orientamento giurisprudenziale citato pocanzi a proposito del furto di energia elettrica.

[376] Direttiva (UE) 2019/713 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio.

[377] La valuta virtuale è definita, analogamente alla nozione contenuta nella direttiva 2018/843/UE, come la «*rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e*

l'importante ruolo che i nuovi strumenti di pagamento rivestono nell'ambito dell'economia digitale, tale da rendere necessario l'intervento di misure minime ai sensi dell'art. 83, par. 1, TFUE[378].

Venendo alle novità introdotte dalla direttiva, si fa rientrare nel concetto di "mezzo di scambio digitale" anche la valuta virtuale (art. 2, lett. c) nella misura in cui venga comunemente utilizzata per effettuare pagamenti[379]. In tal modo il legislatore europeo ha invitato gli Stati membri a provvedere affinché il loro diritto nazionale *«preveda per le future valute virtuali emesse dalle rispettive banche centrali o altre autorità pubbliche lo stesso livello di protezione dai reati di frode di cui godono i mezzi di pagamento diversi dai contanti»*[380].

Per quel che qui interessa, gli Stati dovranno punire come reato l'utilizzazione fraudolenta di strumenti di pagamento diversi dai contanti che siano stati rubati o altrimenti illecitamente ottenuti ovvero oggetto di illecita appropriazione (art. 3). In relazione agli strumenti di pagamento immateriali, l'art. 5 pone, inoltre, un preciso obbligo di criminalizzazione delle seguenti condotte: (i) l'ottenimento illecito di uno strumento di pagamento immateriale, se tale ottenimento ha comportato la commissione di uno dei reati di cui agli articoli da 3 a 6 della direttiva 2013/40/UE[381], nonché l'appropriazione indebita dello stesso; (ii) la contraffazione o la falsificazione fraudolente di uno strumento di pagamento immateriale; (iii) la detenzione di uno strumento di pagamento immateriale ottenuto illecitamente, contraffatto o falsificato a fini di utilizzazione fraudolenta; (iv) il fatto di procurarsi o di mettere a disposizione, uno strumento di pagamento immateriale diverso dai contanti ottenuto illecitamente, contraffatto o falsificato a fini di utilizzazione fraudolenta. Sarà curioso osservare in che modo il legislatore nazionale darà attuazione ai nuovi obblighi di criminalizzazione. Sul punto possiamo limitarci a ribadire l'opportunità di una modifica alle disposizioni del codice penale considerando: l'inapplicabilità dell'art. 648 c.p. all'ipotesi *sub* (i) stante l'impossibilità di ricondurre la valuta virtuale a concetto penalistico di "cosa" e di "denaro"; la dubbia applicabilità dell'art. 493-*ter* c.p. all'ipotesi *sub* (ii), mancando in tal caso un "documento analogo che abiliti all'acquisto di beni o alla prestazione di servizi"; la mancanza di una fattispecie penale punisca la mera detenzione cui ricondurre la condotta descritta *sub* (iii); la dubbia applicabilità dell'art. 615-*quater* all'ipotesi *sub* (iv) che presuppone che la chiave crittografica di spendita della valuta virtuale rientri nel concetto di "mezzo idoneo all'accesso a un sistema informatico o telematico".

---

che può essere trasferita, memorizzata e scambiata elettronicamente» (v. *amplius*, in questo capitolo § 1).

[378] La direttiva stabilisce le norme minime relative alla definizione dei reati e delle sanzioni nelle materie di frode e di falsificazione di mezzi di pagamento diversi dai contanti (art. 1). Gli Stati membri dovranno conformarsi alle disposizioni contenute nella stessa entro il 31 maggio 2021.

[379] La precisazione è contenuta nel considerando n. 10 alla Direttiva.

[380] *Ibidem*

[381] Il riferimento è alle condotte di accesso abusivo ai sistemi di informazione (art. 3), interferenza illecita relativamente ai sistemi (art. 4), interferenza illecita relativamente ai dati (art. 5), intercettazione illecita (art. 6).

Per quel che riguarda, infine, le ipotesi di sottrazione indebita di valuta virtuale, il legislatore europeo propende per la qualificazione in termini di frode informatica prevedendo che gli Stati debbano adottare le misure necessarie affinché l'atto di effettuare o indurre un trasferimento di denaro, di valore monetario o di valuta virtuale, arrecando illecitamente a terzi una perdita patrimoniale allo scopo di procurare un ingiusto profitto *«sia punibile come reato, se commesso intenzionalmente […] ostacolando, senza diritto, il funzionamento di un sistema di informazione o interferendo con esso oppure introducendo, alterando, cancellando, trasmettendo o sopprimendo, senza diritto, dati informatici»*. Tale condotta sembra rientrare appieno del raggio d'azione dell'art. 640-*ter* c.p., circostanza che porta a ritenere superfluo – almeno in questo caso – un intervento del legislatore[382].

6. Valute virtuali e reati tributari nella nuova dimensione dell'economia.

L'aporia classificatoria che circonda l'universo delle valute virtuali avvolge anche i profili fiscali connessi al loro utilizzo, sollevando una densa nebulosa di criticità applicative. Nel corso della trattazione si è più volte fatto riferimento alla natura ibrida del circolante virtuale che talvolta viene in rilievo come mezzo di scambio con funzione monetaria, altre volte come *asset* immateriale, altre ancora come strumento finanziario[383].

Le difficoltà nell'inquadramento giuridico del fenomeno non potevano che ripercuotersi sulla qualificazione fiscale delle operazioni aventi ad oggetto i valori virtuali, ulteriormente complicata dalla connotazione parzialmente "soggettivistica" propria del diritto tributario[384]. Il campo d'indagine andrà dunque esteso considerando non solo la natura giuridica delle operazioni e dei valori ad esse strumentali, ma anche le caratteristiche soggettive delle parti interessate; uno stesso negozio potrà infatti integrare diversi presupposti d'imposta a seconda che sia posto in essere nell'esercizio dell'impresa, a titolo professionale, in via occasionale, oppure *uti privatus*.

Le questioni relative al trattamento fiscale della criptomoneta saranno affrontate con lo sguardo rivolto verso l'oggetto della nostra trattazione: la commissione di reati tributari mediante le operazioni di emissione, cambio e trasferimento di valuta virtuale.

Numerose sono le questioni meritevoli di approfondimento.

---

[382] La penale edittale prevista per la frode informatica (reclusione da sei mesi a tre anni) è peraltro conforme alle previsioni dell'art. 9 della Direttiva che obbliga gli Stati a punire la condotta di cui all'art. 6 con pena detentiva massima non inferiore a tre anni.

[383] *Amplius*, in questo capitolo, § 1.5

[384] Le categorie del diritto civile e commerciale assumono spesso un significato particolare per il diritto tributario, al quale importa tanto la funzione socio-economica del negozio quanto i soggetti che lo realizzano. Si faccia l'esempio al trasferimento della proprietà di una automobile usata, sottoposta a un regime fiscale del tutto differente a seconda che contratto di compravendita sia posto in essere *inter privatos* ovvero si inserisca nell'ambito di una attività d'impresa.

La pseudonimizzazione delle transazioni e le difficoltà nel tracciamento delle operazioni costituiscono, per gli utilizzatori del circolante virtuale, un forte incentivo per evadere le imposte sui redditi e sul valore aggiunto, aprendo orizzonti significativi in materia penaltributaria. Gli investimenti sul mercato virtuale producono spesso plusvalenze molto generose, tali da rendere possibile il superamento delle soglie di punibilità previste dagli artt. 3 ss. del D. Lgs. 10 marzo 2000, n. 74 laddove fossero considerate come redditi di capitale. Problematiche similari si pongono con riferimento al *mining* di valuta virtuale che, se da un lato appare come un mero servizio della società dell'informazione, dall'altro si inserisce nell'ambito di una attività economica organizzata a scopo di lucro.

Particolarmente delicata la questione relativa all'assoggettamento al regime IVA delle operazioni di *trading* valutario, rilevante per la configurabilità dei reati di omessa dichiarazione (art. 5) e omesso versamento (art. 10-*ter*). Entrambe le categorie di tributi (imposte dirette e sul valore aggiunto) sono inoltre interessate dall'utilizzo dei valori virtuali come mezzo fraudolento idoneo ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria. Rimane però il dubbio se l'omessa indicazione in dichiarazione delle attività conseguite in unità di conto virtuale (es. pagamenti in Bitcoin, scambio di valuta corrente in asset virtuali, plusvalenze di investimento) rilevi come dichiarazione infedele (art. 4) ovvero sia *ex se* idonea a rendere fraudolenta la dichiarazione (art. 3).

Non potrebbero infine non considerarsi le enormi potenzialità offerte dal sistema valutario virtuale per eludere le procedure di riscossione coattiva dei tributi. La gestione dei flussi finanziari mediante intermediari autorizzati assicura la piena trasparenza dei traffici giuridici, agevolando l'amministrazione finanziaria nel compito di ricostruire la base imponibile e assicurare il gettito fiscale. Per contro in una economia disintermediata il monitoraggio dei capitali diviene impossibile, poiché gli attori economici dispongono di un formidabile strumento per eludere i controlli fiscali e rendere inefficace la procedura di riscossione coattiva dei crediti erariali; si dovrà pertanto rivolgere l'attenzione anche al delitto di sottrazione fraudolenta al pagamento delle imposte (art. 11) e ai rischi innescati dalla progressiva virtualizzazione dei mezzi di scambio.

Di non minore importanza la regolazione dei flussi di denaro da e per l'estero rispetto alla quale si registrano significative novità. Con il D. Lgs. 90/2017 il legislatore ha infatti esteso il campo di applicazione della normativa sul monitoraggio fiscale per rafforzare l'azione di controllo ai fini fiscali per la prevenzione e la repressione dei fenomeni di illecito trasferimento e detenzione di attività economiche e finanziarie all'estero.

Per una compiuta analisi dei profili di rilevanza penale non potremo esimerci dal fornire alcune premesse sulla disciplina tributaria di riferimento. Trattandosi tuttavia di un panorama normativo complesso ed estremamente articolato, occorre precisare fin da ora che l'inquadramento non avrà alcuna pretesa di esaustività.

6.1. L'assoggettamento al regime IVA delle operazioni di cambio di valuta virtuale. I principi affermati dalla Corte di Giustizia UE.

L'introduzione dell'imposta sul valore aggiunto si deve agli impegni assunti dall'Italia con firma del Trattato istitutivo della Comunità Economica Europea del 1957, che si poneva tra i principali obiettivi quello della creazione di un mercato unico europeo a tutela della leale concorrenza e della libera circolazione delle persone e dei capitali[385]. Per adeguare l'ordinamento nazionale alla normativa comunitaria[386] fu approvata una legge delega per la riforma del settore tributario[387] in base alla quale fu approvato il D.P.R. 26.10.1972, n. 633 istitutivo dell'IVA. Il decreto rappresenta ancora oggi la principale fonte di disciplina dell'imposta sul valore aggiunto, sebbene sia stato soggetto a numerosi interventi di riforma.

Con l'emanazione della Direttiva 2006/112/CE la materia è stata completamente armonizzata a livello comunitario[388], dando vita a un "sistema comune dell'IVA" al quale la compravendita di beni e servizi ai fini del consumo all'interno dell'Unione europea è oggi sottoposta[389]. Considerato che il diritto derivato dell'Unione stabilisce gli elementi essenziali del tributo tra cui il presupposto e la base imponibile, l'aliquota minima, e le operazioni esenti, la Corte di Giustizia si è più volte pronunciata in via pregiudiziale sull'interpretazione delle disposizioni di armonizzazione.

In questo contesto si inserisce la nota sentenza del 22 ottobre 2015, *Skatteverket* contro *Hedqvist*, causa C-264/14 con cui la Corte di Lussemburgo ha affrontato il tema

---

[385] Si veda il contributo di TODINI C., voce *Imposta sul valore aggiunto*, in *Enciclopedia Treccani – Diritto online*, 2016, in https://treccani.it al quale si rimanda per una concisa esposizione degli elementi strutturali dell'imposta.

[386] Con la prima direttiva IVA (1967/227/CEE) furono stabiliti i principi generali dell'applicazione ai beni ed ai servizi un'imposta generale sul consumo. La seconda direttiva IVA, di contestuale emanazione (1967/228/CEE), disciplinava invece la struttura e le modalità applicative dell'imposta. Successivamente vi furono molte altre direttive in materia di IVA che introdussero obblighi sempre più stringenti per gli Stati, di pari passo con l'espansione delle competenze della Comunità europea. Oggi la politica fiscale nell'Unione europea opera su due fronti: la fiscalità diretta, che rimane di competenza esclusiva degli Stati membri, e la fiscalità indiretta, che interessa la libera circolazione delle merci e la libera prestazione dei servizi e che invece è oggetto di forte armonizzazione, in quanto la concorrenza tra gli Stati membri nell'ambito del mercato interno non deve essere falsata da disparità di aliquote e di regimi d'imposizione a livello della fiscalità indiretta.

[387] Legge 9 ottobre 1971, n. 825 (Delega legislativa al Governo della Repubblica per la riforma tributaria), detta anche "legge Visentini".

[388] Con l'emanazione della direttiva n. 112 il legislatore comunitario ha semplificato il quadro normativo, sostituendo la precedente direttiva 77/388/CEE del 17 maggio 1977 in materia di armonizzazione delle legislazioni degli Stati membri relative alle imposte sulla cifra di affari (cosiddetta "sesta direttiva IVA"), più volte modificata nel corso degli anni. La direttiva 2006/112/CE si compone di 414 articoli, raggruppati in 15 titoli e 12 allegati; la maggior parte dei cambiamenti rispetto al sistema precedente sono soltanto strutturali, al fine di rendere il testo più chiaro e comprensibile. Si veda, in argomento, il Dossier del Servizio Studi del Senato della Repubblica "*Principi dell'Iva comunitaria*", in https://camera.it

[389] Con le modifiche apportate al Trattato sul funzionamento dell'Unione europea la competenza dell'Unione in materia di IVA è regolata oggi all'art. 113 TFUE, che attribuisce al Consiglio, secondo la procedura legislativa speciale, l'adozione delle disposizioni che riguardano l'armonizzazione delle legislazioni relative alle imposte indirette sul consumo.

del trattamento ai fini IVA delle operazioni relative alle valute virtuali[390]. Prima di scendere nel merito della questione risolta dalla Corte, alcune precisazioni sui presupposti del tributo appaiono necessarie.

L'IVA è qualificata come una imposta generale sui consumi che grava – in ultima istanza, sulla base di un sofisticato meccanismo applicativo – su coloro che acquistano beni e servizi non per utilizzarli successivamente nella filiera produttiva o distributiva, ma come consumatori finali[391]. L'obbligo contributivo sorge dal compimento di atti a titolo oneroso che importino il trasferimento della proprietà ovvero costituzione o trasferimento di diritti reali di godimento sui beni di ogni genere[392], e dalle prestazioni di servizi verso corrispettivo, dipendenti da una serie di contratti o comunque da una serie di obbligazioni di fare, non fare e permettere, qualunque ne sia la fonte (art. 3 decreto Iva)[393]. Dal punto di vista soggettivo il tributo si riferisce a coloro che esercitano: un'attività oggettivamente considerata commerciale o agricola, indipendentemente dal fatto che sia o meno organizzata in forma d'impresa; un'attività che presenta i caratteri tipici dell'attività commerciale, disponendo di una organizzazione in forma d'impresa; una professione abituale, ancorché non esclusiva, di qualsiasi attività di lavoro autonomo da parte di persone fisiche o di società non commerciali.

Numerose sono tuttavia le operazioni considerate *ex lege* esenti che, pur presentando tutti i requisiti previsti per l'applicazione dell'imposta, per scelta di politica legislativa vengono sottratte dal pagamento del tributo. La giurisprudenza comunitaria ha tuttavia precisato che, essendo l'esenzione un istituto eccezionale, le

---

[390] La sentenza è ampiamente citata dalla dottrina che si è occupata dei profili fiscali delle valute virtuali Cfr. MAJORANA D., *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in *Corriere Tributario*, 2018, 8, 630 ss.; CAPACCIOLI S., *Regime impositivo delle monete virtuali: poche luci e molte ombre*, in *Il Fisco*, 2016, 37,3538 ss: DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 128; MAGLIOCCO A., *Bitcoin e tassazione*, in *Strumenti finanziari e fiscalità*, 2016, 1, 34 ss.; PALUMBO G., *Il trattamento tributario dei bitcoin*, in *Diritto e Pratica Tributaria*, 2016, 1, 2079 ss.; MAZZOCCHI S., *Esenti da IVA le operazioni di cambio nella valuta virtuale "bitcoin"*, in *iltributario.it*, 22 dicembre 2015; CLAPS P. – PIGNATELLI M., *L'acquisto e la vendita per conto terzi di "bitcoin" non sconta l'IVA ma rileva ai fini IRES ed IRAP*, in *Corriere Tributario*, 2016, 40, 3073 ss.; LUCEV R., BONCOMPAGNI F., *Criptovalute e profili di rischio penale nelle attività degli exchanger*, in *Giurisprudenza Penale Web*, 2018, 3.

[391] Il funzionamento del tributo si basa sugli istituti della rivalsa e della detrazione: mediante l'esercizio del diritto di detrazione che, in parallelo alla previsione dell'obbligo di rivalsa, il soggetto passivo del tributo attua quella traslazione dell'imposta a valle della catena di consumo, che vede il suo ultimo anello nel soggetto che, non rientrando formalmente tra i soggetti passivi del tributo, si vede addebitare l'imposta per traslazione economica, ma non può al contempo esercitare la detrazione. Cfr. TODINI, voce *Imposta sul valore aggiunto*, cit., § 2

[392] Gli elementi essenziali sono dunque costituiti dalla presenza di un atto dagli effetti giuridici traslativi o costitutivi e dalla sua onerosità.

[393] Il legislatore europeo definisce la prestazione di servizi, ancor più semplicemente, come *«ogni operazione che non costituisce una cessione di beni»* (art. 24, Direttiva 2002/112). Per semplificare possiamo affermare che in questa categoria rientrano tutte le prestazioni caratterizzate da un obbligo che non sia di dare, a fronte di un corrispettivo. Deve dunque esservi l'elemento della corrispettività, vale a dire una controprestazione, ossia un vantaggio economicamente valutabile per il prestatore, che giustifichi il servizio.

relative disposizioni nazionali devono essere interpretate restrittivamente previo accertamento del reale scopo economico della prestazione.

Venendo ai fatti all'origine della pronuncia sopra indicata, la Corte doveva valutare se l'attività esercitata da Hedqvist di cambiavalute virtuali – nella specie di Bitcoin per valuta corrente – costituisse attività di prestazione di servizi a titolo oneroso ai sensi dell'art. 2, par. 1, della Direttiva e, in tal caso, se rientrasse tra le ipotesi di esenzione[394]. L'amministrazione finanziaria svedese (*Skatteverket*) aveva ritenuto che le operazioni di cambio da e per valuta virtuale possano rientrare nell'ampio concetto di divise, banconote e monete qualificate operazioni esenti dalla direttiva.

La Corte di Giustizia afferma che le operazioni di cambio aventi ad oggetto Bitcoin rientrano tra le prestazioni di servizio a titolo oneroso ma, benché sia integrato il presupposto applicativo dell'imposta, l'esenzione di qui alla lett. e) dell'art. 135 risulta pienamente applicabile. L'estensore argomenta che, non avendo Bitcoin *«altre finalità oltre a quella di un mezzo di pagamento ed essendo questa moneta accettata a tal fine da alcuni operatori»*[395] l'esenzione risulta pienamente conforme alla *ratio* dell'istituto. Per contro, l'interpretazione secondo cui la norma disciplina *«le operazioni relative alle sole valute tradizionali si risolverebbe nel privarla di parte dei suoi effetti»*[396]. Viene così affermato il principio per cui le prestazioni di servizi consistenti nel cambio di valuta tradizionale in valuta virtuale, e viceversa – effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale viene rivenduta – costituiscono operazioni esenti da IVA.

6.1.1. Oltre la sentenza della Corte di Giustizia. Cenni sul regime IVA applicabile alle cessioni di beni, alla prestazione di servizi e all'attività di *mining*.

In sede di primo commento alla sentenza la dottrina ha subito precisato come le statuizioni della Corte riguardino soltanto l'attività di *exchange*, mentre l'esenzione non è applicabile laddove siano trasferiti Bitcoin a fronte della dazione di beni (diversi dal denaro) o la prestazione di servizi[397]. Risulta infatti chiaro che, laddove la valuta

[394] L'art. 135 prevede tra le ipotesi di esenzione anche le *«operazioni, compresa la negoziazione, relative a divise, banconote e monete con valore liberatorio»* (par. 1, lett. e). Nel caso di specie l'amministrazione finanziaria 2013 aveva affermato che l'assenza di una definizione di valuta all'interno della Direttiva IVA conduce alla conclusione che tale valuta sia da intendersi come mezzo di pagamento, non assimilabile dunque al concetto di valuta avente corso legale. Non era tuttavia dello stesso avviso la commissione tributaria (*Skatterättsnämnden*), chiamata a pronunciarsi in sede di parere preventivo, la quale riteneva che le operazioni di cambio dovessero essere soggette ad IVA poiché Bitcoin non è privo di "valore liberatorio" ai sensi della citata direttiva.

[395] Così si legge al § 48 della sentenza. Per un commento, PIASENTE M., *Esenzione IVA per i "bitcoin": la strada indicata dalla Corte UE interpretando la nozione "divise"*, in *Corriere Tributario*, 2016, 2, 141.

[396] *Ibidem*, § 51

[397] Cfr. PALUMBO, *Il trattamento tributario dei bitcoin*, cit., 2079; MAZZOCCHI, *Esenti da IVA le operazioni di cambio*, cit., 1 ss.

virtuale sia il corrispettivo per regolare i rapporti economici tra le parti, si rientrerebbe nel campo delle operazioni sottoposte ad IVA, mentre l'opposta interpretazione sarebbe non solo del tutto contraria rispetto alle finalità della direttiva ma anche evidentemente pericolosa sul versante dell'elusione fiscale.

Tra gli spazi lasciati aperti dalla sentenza in esame, vi è il tema della rilevanza ai fini IVA dell'attività *mining*. L'estrazione di valuta virtuale richiede una organizzazione strumentale di risorse materiali che non sarebbe affatto arduo ricondurre nel perimetro soggettivo di applicazione dell'imposta[398]. Manca tuttavia un rapporto sinallagmatico con una terza parte che fornisce il corrispettivo: la valuta virtuale non preesiste all'attività del *miner*, essendo generata dall'attività di convalida delle transazioni, sicché il relativo titolo di acquisto avviene a titolo originario. Se sotto questo profilo l'attività è da ritenersi non imponibile, più complesso è stabilire se l'esenzione si estende anche ai profitti generati dai costi di transazione (*transaction fees*). Molti sistemi *blockchain* adottano meccanismi di remunerazione non collegati alla creazione di nuova ricchezza, tali per cui chi prende parte al processo di validazione trattiene una percentuale (fissa o variabile che sia) come corrispettivo per l'opera prestata. Si instaura in questo caso un rapporto a titolo oneroso, riconducibile ad una attività economica, da ritenersi però esente ai sensi della lett. d) dell'art. 135 sopra citato[399] trattandosi di un'attività comunque avente ad oggetto "pagamenti". La tesi trova conforto nel principio di diritto affermato dalla Corte di Giustizia che valorizza, quantomeno ai fini IVA, la natura monetaria delle valute virtuali.

In conclusione, va affermata la rilevanza ai fini IVA di tutti i corrispettivi pagati in valuta virtuale, a qualunque titolo, come scambio di "cosa contro prezzo"; andranno invece esenti da imposta quelle operazioni strettamente collegate alla funzione monetaria tra cui il cambio di denaro, l'intermediazione nei pagamenti, la creazione di nuovo circolante.

6.2. La posizione dell'Agenzia delle Entrate sul regime fiscale applicabile alle cessioni e ai redditi derivanti da operazioni in valuta virtuale.

Rivolgendo ora lo sguardo verso il sistema giuridico italiano, deve anzitutto darsi atto dell'assenza di indicazioni normative sul trattamento fiscale delle operazioni aventi ad oggetto valori virtuali. La questione non ha tuttavia tardato a presentarsi all'attenzione dell'Agenzia delle Entrate più volte interrogata in sede di interpello.

[398] È questo un tema pressoché inesplorato dalla dottrina. Tra i pochi contributi v. SPAZIANTE F., *Le operazioni concernenti i "bitcoin": la declinazione pratica dei principi espressi nella sentenza Hedqvist,* in *Fiscalità e Commercio Internazionale,* 2016, 8, 29 il quale ritiene che l'attività di estrazione rientri a pieno titolo tra le ipotesi di esenzione.

[399] La norma considera esenti le operazioni «*relative ai depositi di fondi, ai conti correnti, ai pagamenti, ai giroconti, ai crediti, agli assegni e ad altri effetti commerciali*».

Partendo proprio dagli aspetti legati all'IVA l'amministrazione finanziaria[400] ha richiamato i principi espressi dalla Corte di Lussemburgo sottolineando che alle operazioni di cambio valuta si applica il regime di esenzione di cui all'art. 10, comma 1, n. 3), del D.P.R. 26 ottobre 1972, n. 633. In una successiva risoluzione[401] è stata affrontata una questione del regime applicabile in una operazione consistente nella restituzione dei *token* all'emittente per fruire dei beni e servizi dallo stesso erogati[402]. In risposta all'interpello l'Agenzia delle Entrate ritiene che gli *utility token* emessi dalla società istante fossero assimilabili ai *voucher*, quali strumenti che conferiscono al detentore il diritto a beneficiare di determinati beni o servizi, la cui emissione/cessione non assume rilevanza ai fini IVA, non configurandosi quale anticipazione della cessione/prestazione cui essi stessi danno diritto[403]. L'obbligo contributivo sorgerà al momento dell'utilizzo del *voucher*, ossia all'atto dell'acquisto del bene/servizio che lo stesso incorpora[404].

Ben più complessa è la questione relativa alla rilevanza ai fini IRES delle attività di compravendita di valute virtuali e di scambio tra valute virtuali e tradizionali e viceversa, nonché, ai fini IRPEF, delle operazioni poste in essere da persone fisiche al fuori dell'esercizio dell'impresa.

Quanto all'imposta sul reddito delle società, nella citata Risoluzione n. 72/E l'Agenzia ritiene che le componenti di reddito derivanti dalla attività di intermediazione nell'acquisto e vendita di Bitcoin[405] costituiscano base imponibile al netto dei relativi costi. La differenza tra il prezzo di acquisto sostenuto dalla società e i costi di acquisto cui si è impegnato il cliente, o tra il prezzo di vendita praticato dalla società e i ricavi di vendita garantiti al cliente, è imputabile ai ricavi (o ai costi) di esercizio dell'attività di intermediazione esercitata[406]. Sulla base di tali considerazioni,

---

[400] Risoluzione n. 72/E del 2 settembre 2016, *Interpello ai sensi dell'art. 11, legge 27 luglio 2000, n. 212.Trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali*, in https://agenziaentrate.gov.it

[401] Interpello n. 956-39/2018, Risposta n. 14, *Regime fiscale (IRES, IRAP ed IVA) relativo alla offerta di token digitali. Art. 11, comma 1, lettera a), legge 27 luglio 2000, n. 212*, in https://www.agenziaentrate.gov.it

[402] L'istante riteneva che il corrispettivo ricevuto in sede di ICO costituisse il pagamento anticipato per la cessione del bene o della prestazione di servizi; conseguentemente, ai fini IVA, riteneva applicabile il regime ordinario in quanto l'operazione descritta rappresenta una "prevendita" di beni o servizi, fermo restando che l'operazione andrà fatturata al momento in cui il *token* è restituito dall'acquirente a fronte della fruizione della prestazione o della consegna del bene ad esso collegato.

[403] Vengono richiamati, al riguardo, i chiarimenti resi dalla risoluzione del 22 febbraio 2011, n. 21/E avente ad oggetto il trattamento tributario ai fini IVA dei "buoni acquisto o regalo".

[404] Contrariamente a quanto sostenuto dalla Società, l'Agenzia delle Entrate è dell'avviso che la cessione degli *utility token* sia più correttamente riconducibile ad una mera movimentazione finanziaria, non rilevante agli effetti dell'IVA e che l'imposta si renderà esigibile solo al momento in cui i beni saranno ceduti o i servizi prestati con la spendita dei *token*.

[405] L'interpello era stato presentato da una società a responsabilità limitata intenzionata a prestare servizi connessi all'utilizzo di valuta virtuale e, in particolare, operazioni di acquisto e vendita di Bitcoin per conto della propria clientela.

[406] Il guadagno per l'intermediario è rappresentato dalla differenza tra quanto anticipato dal cliente e quanto speso dalla società per l'acquisto o tra quanto incassato dalla società per la vendita e quanto

l'amministrazione finanziaria equipara *tout court* l'attività svolta dalla istante a quella di qualsiasi intermediario[407] senza che rilevi il particolare oggetto dell'attività. Una importante delucidazione è contenuta nella parte finale della risoluzione, laddove si precisa che, in relazione ai Bitcoin che si trovano nella disponibilità della società a fine esercizio *«gli stessi debbano essere valutati secondo il cambio in vigore alla data di chiusura dell'esercizio»* che il contribuente potrà ricavare dalla media delle quotazioni ufficiali rinvenibili sulle piattaforme *online* in cui avvengono le compravendite di valute virtuali.

Circa il regime fiscale applicabile alle plusvalenze d'investimento realizzate al di fuori del regime di impresa, nella successiva risposta n. 14 del 2018 l'Agenzia afferma che i redditi realizzati dalle persone fisiche che detengono gli *utility token* sono tassabili come redditi diversi *ex* art. 67, comma 1, lettera c-*quater*) TUIR poiché il possesso dell'*asset* dà luogo a un rapporto da cui deriva il diritto di acquistare a termine il prodotto o il servizio.

Traendo le fila del discorso, la posizione dell'amministrazione finanziaria in materia di imposte dirette può essere così sintetizzata: l'attività di intermediazione avente ad oggetto operazioni di cambio di valute virtuali in valute tradizionali (e viceversa) costituisce attività d'impresa e, pertanto, i proventi derivanti da essa vengono assoggettati al relativo regime; la detenzione di cripto-attività da parte di persone fisiche è invece assoggettata al regime dei redditi diversi, nella misura in cui l'operazione dia luogo a un diritto di acquisto a termine.

Decisamente meno chiaro il trattamento fiscale delle plusvalenze d'investimento realizzate mediante operazioni di *trading* al di fuori dell'attività d'impresa. Nel dettaglio, ci si chiede se il differenziale netto tra il prezzo di acquisto e quello di vendita dei valori virtuali sia fiscalmente imponibile come reddito di capitale o reddito diverso. Secondo una parte della dottrina alle plusvalenze sarebbe applicabile – in via analogica, tenuto conto della natura valutaria degli asset virtuali – l'art. 67, comma 1-*ter* TUIR[408], a condizione che nel periodo d'imposta di riferimento la giacenza media del portafoglio titoli e dei depositi complessivamente detenuti dal soggetto abbia superato il controvalore di 51.645, 69 euro per almeno sette giorni lavorativi[409].

---

rimborsato al cliente. Sul punto, CLAPS, PIGNATELLI, *L'acquisto e la vendita per conto terzi di "bitcoin",* cit., 3073.

[407] Secondo l'Agenzia l'attività va qualificata *ex* art. 11, comma 2, lett. c, del D. Lgs. 21 novembre 2007, n. 231, come modificato dal D.Lgs. 25 maggio 2017, n. 90, come quella dei soggetti operanti nel settore finanziario iscritti nelle sezioni dell'elenco generale previste dall'articolo 155, comma 5, del TUB. *Amplius*, § 3.3.1.

[408] La disposizione ascrive ai redditi di natura diversa *«le plusvalenze, diverse da quelle di cui alle lettere c) e c-bis), realizzate mediante cessione a titolo oneroso ovvero rimborso di titoli non rappresentativi di merci, di certificati di massa, di valute estere, oggetto di cessione a termine o rivenienti da depositi o conti correnti, di metalli preziosi, sempreché siano allo stato grezzo o monetato, e di quote di partecipazione ad organismi d'investimento collettivo»,* con la precisazione che *«agli effetti dell'applicazione della presente lettera si considera cessione a titolo oneroso anche il prelievo delle valute estere dal deposito o conto corrente».*

[409] La tesi è difesa da MOLINARO G., *Sono tassabili le manifestazioni di capacità economica emergenti nelle operazioni relative a Bitcoin?,* in *Il Fisco*, 2014, 25, 2447 ss.

La tesi non ci pare affatto condivisibile, poiché rischia di eludere il principio di riserva (relativa) di legge in materia tributaria mediante una interpretazione del tutto creativa. L'assimilazione del *trading* virtuale alle operazioni speculative aventi ad oggetto valute estere dovrebbe essere condotta in modo estremamente cauto per non invadere l'area di competenza del legislatore. Nel corso della trattazione abbiamo più volte fatto riferimento alle similitudini tra le valute virtuali e la moneta legale[410], sottolineando la necessità di un diverso trattamento giuridico delle prime rispetto alla seconda. Per quanto da un punto di vista funzionale queste ultime siano assimilabili, a detta della Corte di Giustizia, alle valute tradizionali, ciò non sembra poter legittimare una applicazione analogica delle disposizioni tributarie contraria agli interessi contribuente. L'assunto trova conforto nei principi generali che regolano l'imposizione fiscale, contenuti nella legge 27 luglio 2000, n. 212, la quale pone un limite alla discrezionalità dell'amministrazione finanziaria disponendo che *«l'adozione di norme interpretative in materia tributaria può essere disposta soltanto in casi eccezionali e con legge ordinaria, qualificando come tali le disposizioni di interpretazione autentica»* (art. 1, comma 2). Spetterà dunque al legislatore intervenire per adeguare l'ordinamento fiscale alle esigenze di una economia sempre più virtualizzata.

6.3. Profili di rilevanza penale dell'evasione delle imposte sui redditi e sul valore aggiunto relative ad operazioni in valuta virtuale.

L'indagine sui profili di rilevanza penale delle operazioni aventi ad oggetto valori virtuali non può che partire dalla considerazione della necessaria strumentalità dell'apparato sanzionatorio del D. Lgs. 74/2000 rispetto alle violazioni della disciplina tributaria. Il diritto penale si muove entro uno spazio piuttosto limitato, reso angusto dalle scelte di politica legislativa legate all'opportunità di punite determinate condotte e dalla sussidiarietà rispetto alle ipotesi sanzionate in via amministrativa. La funzione ancillare riservata alla pena emerge piuttosto chiaramente dalla tecnica descrittiva utilizzata dal legislatore, facente leva su elementi normativi della fattispecie propri del diritto tributario e delle scienze contabili.

Non desta dunque stupore che, anche nel caso oggetto di studio, la risposta sanzionatoria dipenda dal trattamento fiscale di una determinata operazione. Così, ad esempio, l'omessa dichiarazione o l'omesso versamento dell'IVA (artt. 5 e 10-*ter* D. Lgs. 74/2000) rileverà nei soli casi in cui sia ceduto un bene o prestato un servizio a fronte di un corrispettivo pagato in criptomoneta, ma non quando l'operazione sia esentata da IVA (come per la conversione di moneta legale in valuta virtuale). Allo stesso modo una dichiarazione potrà dirsi infedele (art. 4) soltanto se gli elementi attivi non indicati (es. plusvalenza tra il prezzo di acquisto e quello di vendita di un *asset* virtuale) costituivano base imponibile. Essendo la violazione tributaria un presupposto (implicito) di esistenza del reato, si spiega facilmente perché la qualificazione a fini fiscali dell'operazione sia il fattore determinante la risposta sanzionatoria. Detto

[410] In questo capitolo, *supra* § 1.5 e 3.1

francamente, non sembra che la natura virtualizzata dei valori sollevi questioni degne di nota sul versante strettamente penalistico[411] a causa della funzione meramente strumentale del reato rispetto all'illecito fiscale. Vi sono tuttavia alcuni aspetti meritevoli di attenzione, tra cui quello dello sfruttamento nel sistema valutario virtuale allo scopo di evadere le imposte sui redditi o sul valore aggiunto.

Poniamo il caso di un imprenditore operante nel settore dell'*e-commerce* che, volendo sottrarsi agli oneri fiscali, decida di accettare Bitcoin come mezzo di pagamento. Giunto al termine del periodo d'imposta dichiara di aver realizzato un utile di poche migliaia di euro (somma dei corrispettivi pagati dai clienti in euro al netto dei costi di esercizio), omettendo *tout court* di inserire in dichiarazione i proventi delle vendite pagati in valuta virtuale, per un ammontare complessivo di oltre un milione di euro. Non potendosi in alcun modo dubitare della rilevanza penale della condotta – almeno sul piano del dolo specifico e del superamento delle soglie di punibilità – ci si domanda se l'imprenditore dovrà rispondere di dichiarazione infedele (art. 4) o del più grave reato di dichiarazione fraudolenta (art. 3). Come noto le due fattispecie di pongono in rapporto di specialità, giacché presentano alcuni elementi costitutivi comuni differenziandosi per la presenza di una nota di fraudolenza, presente nel secondo ma non anche nel primo reato[412]. L'integrazione dell'uno piuttosto che dell'altro reato dipende dalla possibilità di ravvisare nella omessa indicazione dei corrispettivi percepiti in valuta virtuale un "mezzo fraudolento idoneo ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria".

Secondo una parte della dottrina l'intenzione del legislatore del 2000 era quella di escludere che la mera omessa indicazione in dichiarazione e nelle scritture contabili potesse integrare la tipicità del delitto di cui all'art. 3 D. Lgs 74/2000, dovendo a questa sempre affiancarsi sempre la componente positiva dei mezzi fraudolenti[413]. La norma ha subito numerose modifiche nel corso degli anni, per giungere all'attuale conformazione per effetto delle modifiche apportate dal D. Lgs. 158/2015. Rispetto alla formulazione precedente, viene eliminato il riferimento alla "falsa rappresentazione nelle scritture contabili obbligatorie", mentre la condotta penalmente rilevante si concretizza nel compimento di operazioni simulate oggettivamente o

[411] Le fattispecie penaltributarie sono infatti imperniate su elementi descrittivi propri del diritto tributario (presentazione della dichiarazione, versamento dell'imposta, emissione di fatture, certificazione delle ritenute etc.) e sono ispirate al modello del reato "ad offesa funzionale".

[412] Il reato di dichiarazione fraudolenta mediante altri artifici punisce con la reclusione da un anno e sei mesi a sei anni chi al fine di evadere le imposte sui redditi o sul valore aggiunto, *«compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi»,* Il successivo delitto di dichiarazione infedele punisce chi, fuori dei casi previsti dagli articoli 2 e 3, al fine di evadere le imposte sui redditi o sul valore aggiunto, *«indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti».*

[413] In argomento, v. AMBROSETTI E. M., *La frode fiscale mediante altri artifici: vecchi e nuovi aspetti problematici*, in *Archivio Penale*, 2017, 1, 4 ss., al quale si rinvia per gli opportuni approfondimenti bibliografici.

soggettivamente, ovvero nell'avvalersi di "documenti falsi o di altri mezzi fraudolenti[414]. In sede di commento alla riforma si è fatto rilevare che l'eliminazione dalla struttura materiale della norma del riferimento alla falsa rappresentazione nelle scritture contabili ha ampliato il novero dei soggetti potenziali autori del delitto in questione, che può ora essere commesso da qualunque soggetto obbligato alla presentazione della dichiarazione dei redditi o della dichiarazione IVA[415]. È rimasto invece invariato il riferimento all'avvalersi di mezzi fraudolenti idonei ad ostacolare l'accertamento fiscale, arricchito dal riferimento alla induzione in errore dell'amministrazione finanziaria.

Di particolare importanza – per quel che qui interessa – è la nozione di "mezzi fraudolenti" con cui legislatore ha voluto porre fine al dibattito che era insorto con riguardo alle precedenti versioni della fattispecie sulla rilevanza penale dell'omissione antidoverosa[416]. Nell'elenco contenuto nell'art. 1 è stata inserita la nuova lettera g-*ter*) che definisce i mezzi fraudolenti come le *«condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà»*. La disposizione va letta in combinato disposto con il nuovo terzo comma dell'art. 3 che testualmente esclude che *«la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali»* costituiscano un mezzo fraudolento. Con questa precisazione il legislatore ha voluto, verosimilmente, positivizzare l'orientamento giurisprudenziale secondo cui l'elemento della fraudolenza non può prescindere dall'accertamento della componente positiva dei mezzi fraudolenti. L'assunto trova conferma nella relazione dell'Ufficio del Massimario della Corte di Cassazione[417] che mette in evidenza come, secondo gli arresti più recenti, la semplice violazione degli

[414] Il legislatore ha messo mano anche alle soglie di punibilità, prevedendo che l'imposta evasa debba essere superiore, con riferimento a taluna delle singole imposte, a euro trentamila, e che l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, debba superare il cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, la somma di un milione cinquecentomila euro.

[415] Sebbene la norma utilizzasse il pronome "chiunque" si riteneva comunemente che la fattispecie costituisse un reato proprio dell'imprenditore commerciale e degli altri soggetti tenuti ad osservare le norme in materia di contabilità obbligatoria. In dottrina v. CINGARI F., *La dichiarazione fraudolenta mediante altri artifici*, in BRICHETTI R, VENEZIANI P. (a cura di), *I reati tributari*, Torino, 2017, 205 ss. PERINI A., voce *Reati tributari,* in *Dig. Pen., Agg*., Torino, 2016, 573 ss.; SOANA G., *I reati tributari*, Milano, 2018, 166 ss.; AMBROSETTI E.M., *I reati tributari*, in AMBROSETTI E.M., MEZZETTI E., RONCO M., *Diritto penale dell'impresa,* Bologna, 2016, 505 ss.; PUTINATI S., *Dichiarazione fraudolenta mediante altri artifici*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Diritto penale dell'economia*, vol. I, Vicenza, 2017, 723 ss.; MAZZACUVA F.., *Il nuovo delitto di dichiarazione fraudolenta mediante altri artifici*, in AA. VV., *Scritti in onore di Luigi Stortoni*, Bologna, 2016, 585 ss.; SANFILIPPO P., *L'incerta riforma dei reati di dichiarazione fraudolenta: la riformulazione degli artt. 2 e 3 d.lgs. 74/2000 ad opera del d.lgs. 158/2015 e gli evanescenti profili di differenziazione tra le fattispecie*, in *Legislazione penale*, 2016, 4, 2 ss.

[416] Cfr. AMBROSETTI, *La frode fiscale mediante altri artifici*, cit., 8

[417] Si richiama la relazione dell'Ufficio del Massimario III/05/2015 del 28ottobre 2015 intitolata "Novità legislative: Decreto Legislativo n. 24 settembre 2015, n. 158, Revisione del sistema sanzionatorio, in attuazione dell'articolo 8, comma 1, della legge 11 marzo 2014, n. 23", 9 ss.

obblighi di fatturazione e registrazione, pur se indirizzata all'evasione, non integra il "mezzo fraudolento"[418].

Venendo ora alla concreta individuazione delle condotte caratterizzate dal requisito della fraudolenza, vengono in rilievo espedienti quali l'utilizzazione di conti correnti o depositi accesi a nome di terzi per il deposito di somme relative ad operazioni non registrate in contabilità, la falsa intestazione di beni, l'intestazione a prestanome o a nomi di fantasia di conti correnti bancari o libretti al portatore[419], la tenuta di una contabilità "in nero"[420]. Calati nel contesto dell'economia virtuale, tali espedienti potrebbero realizzarsi mediante l'intestazione fittizia a un prestanome del portafoglio nel quale far confluire i corrispettivi sottratti all'imposizione, l'utilizzo di un *wallet* privato (non registrato presso alcun *provider*) che garantisca un anonimato totale, o il compimento di transazioni intermedie per far disperdere le tracce dei pagamenti ricevuti dai clienti.

Affinché possano ravvisarsi gli estremi del "mezzo fraudolento" non si ritiene sufficiente la semplice omessa indicazione dei corrispettivi ricevuti in valuta virtuale, dovendo questa essere accompagna da una condotta decettiva di tipo attivo o dalla violazione di uno specifico obbligo di legge. L'aura di "sospetto" che avvolge il sistema valutario virtuale non sembra poter giustificare alcuna aprioristica presunzione di fraudolenza dell'accettazione della criptomoneta come mezzo di pagamento. Con l'introduzione del riferimento alle "condotte artificiose attive" (art. 1, lett. g-*ter*) il legislatore ha rimarcato la necessità di un accertamento positivo della sussistenza di una o più azioni che abbiano determinato una falsa rappresentazione della realtà: un *quid pluris* rispetto alla mera omissione informativa posta alla base del delitto di dichiarazione infedele (art. 4).

---

[418] La nota di fraudolenza richiede un *quid pluris* che, affiancandosi alla falsa rappresentazione offerta nelle scritture contabili e nella dichiarazione, consenta di attribuire all'elemento oggettivo una valenza di insidiosità, derivante dall'impiego di artifici idonei a fornire una falsa rappresentazione contabile ed a costituire ostacolo al suo accertamento (cfr. Cass., Pen., Sez. III, 22 novembre 2012, n. 2292; Sez. III, 12 febbraio 2002 n. 13641).

[419] CINGARI, *La dichiarazione fraudolenta mediante altri artifici*, cit., 218; SOANA, *I reati tributari*, cit., 176 ss. Se i corrispettivi derivanti dalle operazioni in nero vengono dirottati su conti correnti di soggetti diversi dal contribuente, l'elemento di fraudolenza sarebbe integrato dalla interposizione fittizia di persona. L'occultamento del possesso dei redditi ostacola significativamente l'accertamento della capacità contributiva, ledendo le prerogative di controllo dell'amministrazione finanziaria. Così, ad esempio, la giurisprudenza ha ritenuto che l'intestazione di un conto corrente a una società gestita da un prossimo congiunto costituisse un mezzo fraudolento (cfr. Cass. Pen. Sez. III, 15 ottobre 2014, n. 50308).

[420] La giurisprudenza di merito ha riconosciuto che integrasse l'elemento del mezzo fraudolento la tenuta di un'analitica "contabilità nera", dalla quale emergesse il reale volume d'affari della società, rinvenuta casualmente nel corso di verifica da parte della Guardia di finanza (Trib. Nola, 18 marzo 2004, in *Diritto e pratica tributaria*, 2004, II, 1094, citato da AMBROSETTI, *La frode fiscale mediante altri artifici*, cit., 9. Un tale orientamento è stato aspramente criticato dalla dottrina, la quale ritiene che la mera tenuta della contabilità in nero non dovrebbe rilevare *ex* art. 3 D. Lgs. 74/2000, poiché, oltre ad essere priva del requisito della idoneità ingannatoria, rende possibile la ricostruzione del reddito effettivamente percepito dal contribuente. Cfr. MUSCO E., ARDITO F., *Diritto penale tributario*, Bologna, 2016, 178 ss.; VENEZIANI P., sub *Art. 3*, in CARACCIOLI I., GIARDA A., LANZI A. (a cura di), *Diritto e procedura penale tributaria. Commentario al D. Lgs. 10 marzo 2000 n. 74*, Padova, 2000, 147).

Non potrebbero del resto tacersi gli effetti paradossali di una frettolosa presa di posizione in favore della natura *in re ipsa* fraudolenta dell'accettazione dei valori virtuali come strumento di pagamento. Nel corso della trattazione di è più volte fatto cenno al funzionamento tecnico della *blockchain*, che si basa sulla registrazione delle transazioni su un libro mastro pubblico, pubblicamente accessibile e tendenzialmente inalterabile[421]. Richiamando il caso addotto come esempio, ipotizziamo che il gestore del sito di *e-commerce* abbia indicato l'indirizzo di portafoglio a cui gli acquirenti potranno far pervenire i pagamenti; il dettaglio delle operazioni dirette verso il conto del negoziante restano impresse in modo indelebile sulla catena di blocchi e chiunque può accedervi connettendosi al client di Bitcoin (o dell'infrastruttura utilizzata per il pagamento). Ne deriva la totale inidoneità della condotta ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, la quale è messa in condizione di determinare il reddito imponibile relativo a un determinato periodo d'imposta con pochi clic, senza dover neppure ricorrere alla consultazione degli archivi dell'anagrafe tributaria. Tutti i dati (indirizzo pubblico, marca temporale, e quantità di valuta ricevuta) sono disponibili *open source* e vi resteranno per un periodo pressoché illimitato di tempo, con sufficienti garanzie di inalterabilità del dato e di corretta conservazione dello stesso. Considerata da questa prospettiva, la scelta del contribuente di non dichiarare i ricavi delle vendite si rivela decisamente poco avveduta.

A diverse conclusioni si perviene qualora l'accettazione *in solutum* della valuta virtuale sia strumentale al compimento di azioni volte a dissimulare la provenienza dei proventi dell'evasione fiscale e a servirsi dello schermo dell'anonimato. Numerosi sono gli espedienti mediante i quali il contribuente potrebbe eludere i controlli da parte dell'amministrazione finanziaria. Sarebbe sufficiente, ad esempio, ricevere pagamenti in valute strutturate *by design* per non rendere tracciabile il flusso di transazioni sul registro pubblico, oppure indicare come *public address* un conto di rimbalzo per il *mixing* delle transazioni[422]. In alternativa, il contribuente potrebbe non rendere pubblico l'indirizzo di conto ma comunicarlo di volta in volta ai singoli utenti, intestando fittiziamente a un prestanome il portafoglio nel quale far confluire i corrispettivi sottratti all'imposizione. In entrambi i casi non sembra potersi dubitare della connotazione fraudolenta, ai sensi della disposizione in esame, della condotta tenuta dal contribuente.

Volendo riassumere in sintesi la risposta all'interrogativo formulato in apertura del paragrafo, riteniamo che l'accettazione di pagamenti in unità di conto virtuale non costituisce una condotta *ex se* idonea a integrare l'elemento del mezzo fraudolento ai sensi dell'art. 3 D. Lgs. 74/2000, dovendosi accertare al caso concreto l'esistenza di artifici determinanti una falsa rappresentazione della realtà idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria. Pertanto, nel caso esemplificato il gestore della piattaforma di commercio elettrico dovrà rispondere del

[421] *Amplius*, v. in particolare Cap. I, § 2

[422] In tal caso le risultanze della *blockchain* non saranno intellegibili, oppure richiederanno uno sforzo notevole per ricostruire il dettaglio delle operazioni.

meno grave reato di dichiarazione infedele, avendo semplicemente omesso di dichiarare i proventi delle vendite corrisposti in Bitcoin.

Resta da domandarsi se l'utilizzo di un *wallet* privato, non registrato presso alcun *provider*, per la ricezione dei pagamenti possa assumere rilevanza ai sensi della disposizione in esame. Si ricorderà che i fornitori di servizi di portafoglio elettronico sono oggi sottoposti all'obbligo di identificazione della clientela, al pari degli intermediari finanziari[423]; non vi è tuttavia alcuna disposizione che imponga a possessori delle valute virtuali di servirsi degli intermediari autorizzati. Deve quindi ritenersi, alla stregua di quanto sopra considerato, che l'utilizzo di un portafoglio privato sia un fatto di per sé neutro, non sufficiente ad integrare la nota di fraudolenza se non supportato da azioni ulteriori idonee ad eludere l'accertamento fiscale.

Una seconda questione riguarda la rilevanza, ai sensi della disposizione in esame, del fenomeno dell'elusione fiscale[424]. Il sistema finanziario virtuale attribuisce ai contribuenti uno strumento nuovo per porre in essere complesse operazioni negoziali finalizzate a raggirare le norme tributarie. Gli esempi potrebbero essere svariati: si pensi alla società di informatica che offra ai propri clienti dei token di pagamento a un prezzo ridotto che questi potranno utilizzare per estinguere parte del prezzo per i servizi di assistenza tecnica così da creare le premesse per una sottofatturazione quantitativa[425]; oppure alla creazione di valori virtuali che "incorporano" diritti su beni mobili o immobili il cui scambio sul mercato è giustificato dal godimento del bene per un determinato periodo di tempo, operazione finalizzata ad eludere le disposizioni sui redditi immobiliari o di natura diversa.

Dalla prospettiva penalistica il *core* del problema è rappresentato dalla rilevanza dell'abuso del diritto ai sensi dell'art. 3 D. Lgs. 74/2000. Tra gli aspetti positivi della riforma del sistema sanzionatorio penaltributario vi è certamente quello di aver tracciato un confine più netto fra le condotte di mera elusione fiscale e quelle di evasione[426]. La questione aveva assunto una particolare rilevanza a seguito di alcune pronunce della giurisprudenza di legittimità[427] sulla rilevanza penale del fenomeno elusivo. Gli approdi più recenti della Suprema Corte avevano tuttavia affermato, in

[423] Sulle novità introdotte dalla Direttiva 2018/843/UE *amplius,* v. § 3.4

[424] L'art. 10-*bis*, comma 1, della legge 27 luglio 2000, n. 212, introdotto dal, D. Lgs. 5 agosto 2015, n. 128 definisce l'abuso del diritto (o elusione fiscale) come «*una o più operazioni prive di sostanza economica che, pur nel rispetto formale delle norme fiscali, realizzano essenzialmente vantaggi fiscali indebiti*», stabilendo che tali operazioni *«non sono opponibili all'amministrazione finanziaria, che ne disconosce i vantaggi determinando i tributi sulla base delle norme e dei principi elusi e tenuto conto di quanto versato dal contribuente per effetto di dette operazioni»*.

[425] Fermo restando che lo scambio di valuta virtuale per moneta corrente rientra tra le ipotesi di esenzione di cui all'art. 135, lett. e), rimane il fatto che il mancato assolvimento dell'IVA sulle operazioni di cambio realizza un vantaggio fiscale indebito, poiché all'atto dell'erogazione del servizio verrà emessa una fattura per l'importo pagato dal cliente (che tuttavia non riflette il reale prezzo di scambio del bene, che dovrebbe comprendere anche il controvalore dei *token* utilizzati per beneficiare dello sconto).

[426] Cfr. AMBROSETTI, *La frode fiscale mediante altri artifici*, cit., 10

[427] *Ex plurimis*, Cass., Sez. II, 22 novembre 2011, n. 7739 (sentenza c.d. Dolce e Gabbana), in *Diritto penale contemporaneo*, 22 giugno 2012, con nota di VIZZARDI M., *La Cassazione sul caso Dolce e Gabbana: elusione fiscale e truffa aggravata a danni dello Stato.*

omaggio al principio di tassatività, la rilevanza penale delle sole ipotesi di elusione espressamente previste dalla legge[428]. La questione sembra ormai aver perduto di attualità con l'introduzione del citato art. 10-*bis* dello Statuto del contribuente che, oltre a codificare una precisa nozione di elusione fiscale, dispone espressamente che *«le operazioni abusive non danno luogo a fatti punibili ai sensi delle leggi penali tributarie»*. Il dettato normativo consente di giungere alla conclusione che le ipotesi sopra esemplificate di elusione fiscale non sono riconducibili alla frode fiscale mediante altri artifici. Se ne trae conferma anche dalla nuova lett. g-*bis*) dell'art. 1 D. Lgs. 74/2000, che, nel definire le operazioni simulate oggettivamente e soggettivamente[429], esclude *per tabulas* quelle disciplinate dall'art. 10-*bis* della legge 27 luglio 2000, n. 212. Si dovranno dunque distinguere accuratamente le ipotesi di evasione da quelle più propriamente elusive, limitando la rilevanza penale del fatto soltanto alle prime. Nei casi esemplificati può ben darsi che la creazione e il successivo scambio di *asset* virtuali siano preordinati all'ottenimento di un indebito vantaggio fiscale, ma, nella misura in cui non siano ravvisabili indici sintomatici dell'inesistenza dell'operazione o della simulazione soggettiva o oggettiva dei trasferimenti, le condotte non assumeranno rilevanza penaltributaria.

Più complesso stabilire se tali operazioni diano luogo a una evasione d'imposta, agevolata dalla mancanza di indicazioni normative chiare sul regime fiscale applicabile alle diverse tipologie di *token*. È questa una questione assai delicata che, rientrando solo collateralmente nel nostro campo d'indagine, chiama in causa valutazioni di ordine pratico non riducibili a una mera riflessione teorica.

6.4. La sottrazione fraudolenta al pagamento delle imposte.

Per un compiuto esame dei profili di rilevanza penaltributaria delle operazioni in valuta virtuale, l'attenzione non può essere rivolta unicamente ai reati in materia di dichiarazione. I valori digitali sono suscettibili di essere impiegati anche come strumento per la commissione di reati inseriti nel Capo II del D. Lgs. 74/2000[430], in particolare del delitto di sottrazione fraudolenta al pagamento delle imposte (art. 11).

[428] Si veda in tal senso Cass. Pen., Sez. V, 16 gennaio 2013, n. 36859. Le conclusioni raggiunte dalla S. C. nella sentenza appaiono condivisibili poiché in campo penale appare piuttosto azzardato affermare l'esistenza di una clausola generale antielusiva, così come ritenuto dalla giurisprudenza di legittimità in materia tributaria.

[429] Si intendono per "operazioni simulate oggettivamente o soggettivamente" *«le operazioni apparenti, diverse da quelle disciplinate dall'articolo 10-bis della legge 27 luglio 2000, n. 212, poste in essere con la volontà di non realizzarle in tutto o in parte ovvero le operazioni riferite a soggetti fittiziamente interposti»*.

[430] Ci si riferisce al Capo II del Titolo II dei "delitti in materia di documenti e pagamento di imposte". Non saranno oggetto d'esame le fattispecie di cui agli artt. 8-10-*quater* (emissione di fatture per operazioni inesistenti, occultamento e distruzione di documenti contabili, omesso versamento di ritenute certificate, omesso versamento dell'IVA, indebita compensazione) rispetto ai quali la natura virtuale dei valori (mediante i quali si è realizzata l'evasione d'imposta) non solleva questioni meritevoli di particolare attenzione.

La disposizione punisce chi, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila *«aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva»*[431]. Il reato è posto a tutela dell'interesse finale del Fisco alla percezione dei tributi e, in via strumentale, a presidio del corretto svolgimento della procedura di riscossione coattiva di competenza dell'amministrazione finanziaria e dei concessionari della riscossione[432].

I valori virtuali rappresentano uno strumento formidabile di smobilizzazione della ricchezza, che facilmente si presta ad essere utilizzato per occultare alcune componenti patrimoniali. Ci si riferisce non soltanto alle tradizionali forme di conversione di valuta reale per valuta virtuale – più volte esaminata – ma anche alla pratica di c.d. tokenizzazione degli asset. Con questo termine si indica l'insieme di operazioni consistenti della creazione di informazioni digitali univoche, non alterabili né duplicabili, rappresentative di diritti di proprietà o di godimento su beni mobili o immobili destinati alla circolazione tra il pubblico e allo scambio mediante un sistema di registri distribuiti[433]. Possiamo addurre come esempio il caso del debitore erariale che, possedendo una preziosa collezione di opere d'arte, decida di emettere *token* rappresentativi del diritto di proprietà sulle stesse, affidando la custodia a una famosa casa d'asta. Dopo aver ricevuto una notevole quantità di Bitcoin, o altra valuta virtuale, quale corrispettivo per la vendita "a quote" delle opere, accantona il ricavato su un portafoglio elettronico privato, rendendo così di fatto inefficace la procedura di riscossione coattiva.

Quale che sia l'espediente negoziale concretamente posto in essere, rimane il fatto che la conversione degli averi in valuta virtuale rappresenta per l'Erario un ostacolo quasi insormontabile. La procedura di riscossione coattiva non può che arrestarsi dinanzi all'impossibilità di aggredire la ricchezza digitalizzata, poiché, pur laddove l'amministrazione finanziaria avesse la certezza del possesso di una determinata disponibilità economica, non disporrebbe di adeguati strumenti per individuare con

---

[431] Nella Relazione di accompagnamento al D. Lgs. 74/2000, in *Finanza e fisco*, 2000, 15, 2080 ss. si legge che rispetto al suo antecedente storico (contenuto nell'art. 97, comma 6, DPR 29 settembre 1973, n. 602) il delitto di caratterizza per *«la soppressione del presupposto rappresentato dall'avvenuta effettuazione di accessi, ispezioni o verifiche, o dalla preventiva notificazione all'autore della manovra di inviti, richieste, atti di accertamento o iscrizioni a ruolo»*, presupposto che aveva contribuito, in effetti, a limitare fortemente le capacità di presa dell'incriminazione. Inoltre, la linea della tutela penale è stata opportunamente avanzata richiedendosi ai fini del perfezionamento del delitto *«la semplice idoneità della condotta a rendere inefficace la procedura di riscossione - idoneità da apprezzare, in base ai principi, con giudizio ex ante - e non anche l'effettiva verificazione di tale evento».*

[432] In dottrina, senza pretese di esaustività v. INGRASSIA A., *Le diverse forme di sottrazione fraudolenta al pagamento delle imposte*, in BRICHETTI, VENEZIANI (a cura di), *I reati tributari*, cit., 378 ss.; MUSCO, ARDITO, *Diritto penale tributario,* cit., 212 ss.; DELSIGNORE F., *Il delitto di sottrazione fraudolenta al pagamento di imposte in sede di riscossione coattiva*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Diritto penale dell'economia*, cit., 1009; SOANA, *I reati tributari*, cit., 429.

[433]

precisione il luogo di conservazione delle somme e per sottrarne al reo la disponibilità. Il contribuente infedele si guarderà bene dal depositare le somme presso intermediari del mercato (*exchange* o *wallet provider*), potendo fare uso di *software* privati per la gestione del portafoglio e di chiavette USB per la conservazione delle chiavi crittografiche[434]. Da questa prospettiva le valute virtuali vengono nuovamente in considerazione come *strumento del reato*[435], costituendo il mezzo materiale per il compimento della condotta descritta dalla fattispecie incriminatrice.

La prima condotta esecutiva consiste nella alienazione simulata dei beni, che si attua mediante un programma negoziale che non corrisponde, in tutto o in parte, all'effettiva volontà dei contraenti; la divergenza può aver riguardo al titolo negoziale, all'entità del corrispettivo, ovvero ai soggetti coinvolti (c.d. interposizione fittizia)[436]. Un trasferimento in valuta virtuale può, non diversamente da ogni altro negozio, avere una causa simulata; basti pensare all'invio di somme verso un conto corrente intestato a un prestanome, alla vendita di criptomoneta effettuata *nummo uno* a un corrispettivo di gran lunga inferiore al valore di mercato per dissimulare una donazione; al conferimento di valori virtuali in società di comodo.

Se l'alienazione simulata non solleva particolari problematiche applicative, per contro la nozione di "atto fraudolento" risulta decisamente più problematica. L'espressione potrebbe riferirsi qualsiasi atto, preordinato alla lesione delle ragioni creditori, che produca una apprezzabile *deminutio patrimonii*. L'esistenza di rimedi civilistici per far fronte ai suddetti atti dispositivi suggerisce di circoscrivere il campo di rilevanza penale alle sole condotte fraudolente idonee a configurare una situazione di apparenza (*immutatio veri*), costituita dalla riduzione del patrimonio del debitore.

Poniamo il caso del soggetto che, intenzionato a sottrarsi alla procedura di riscossione coattiva dei crediti erariali, venda il proprio appartamento a una società di gestione immobiliare ricevendo in cambio *utility token*, rappresentativi del diritto di abitazione dell'immobile. Potrebbe l'atto di cessione essere ritenuto fraudolento ai sensi della disposizione in esame?

Secondo una condivisibile opinione giurisprudenziale[437] nella categoria degli atti fraudolenti rientrano anche gli strumenti giuridici leciti che siano utilizzati dal debitore

---

[434] Naturalmente non si tratta di una impossibilità assoluta, ma soltanto relativa. Esistono delle particolari procedure per sottrarre al reo la disponibilità dei valori una volta che siano stati individuati mediante perquisizioni o sequestri. Per approfondimenti, *infra* Cap. V, § 7

[435] Sulla classificazione delle valute virtuali come strumento, oggetto materiale e profitto del reato v. *supra*, § 1

[436] La dottrina ha posto l'attenzione sulla necessità di accertare che l'alienazione sia realmente simulata. Ove il trasferimento sia effettivo, la relativa condotta potrà tuttalpiù essere considerata come un atto simulato. Cfr. DI VIZIO F., *Il delitto di sottrazione fraudolenta del pagamento delle imposte ed i rapporti con i reati di bancarotta fraudolenta per distrazione e di riciclaggio*, in *Discrimen*, 1 ottobre 2018, 26.

[437] La giurisprudenza di legittimità più recente ha affermato che il dolo della sottrazione fraudolenta si rinviene *«nella volontà dell'agente di sottrarsi al pagamento delle imposte che superino la soglia prevista e richiede la dimostrazione della strumentalizzazione della causa tipica negoziale o l'abuso dello strumento giuridico utilizzato»*. Cfr. Cass. Pen., Sez. III, 15 aprile 2015, n. 15449 richiamata da DORIGO S., *Nuovi confini giurisprudenziali del reato di sottrazione fraudolenta al pagamento di imposte*, in *Giurisprudenza penale web*, 2017, 7-8, 6 ss.

in maniera abusiva, fungendo da espedienti per eludere l'azione esecutiva. La criminalizzazione di condotte di questo tipo si muove su un terreno estremamente scivoloso, per via dell'assenza di criteri in grado di delimitare l'ambito applicativo del reato. Deve pertanto attribuirsi rilevanza agli indici rivelatori della causa concreta del negozio e agli elementi sintomatici della volontà di occultare la reale sostanza economica dell'operazione. L'accertamento della natura fraudolenta degli atti contribuisce infatti a rimarcare il *disvalore di azione*, delimitando in modo razionale l'area del penalmente rilevante. In tal senso si sono espresse anche le Sezioni Unite che, chiamate a pronunciarsi sulla nozione di "atti fraudolenti" contenuta nell'art. 388 c.p.[438], hanno ritenuto in contrasto con il principio di legalità una lettura della norma che facesse coincidere il requisito della natura fraudolenta degli atti con la loro mera idoneità alla riduzione delle garanzie del credito, poiché *«può essere ritenuto penalmente rilevante solo un atto di disposizione del patrimonio che si caratterizzi per le modalità tipizzate dalla norma, non potendosi in definitiva far coincidere la natura simulata dell'alienazione o il carattere fraudolento degli atti con il fine di vulnerare le legittime aspettative dell'Erario»*[439].

Restano pertanto fuori dall'ambito applicativo della disposizione quelle condotte che comportino un decremento patrimoniale effettivo. Con la fuoriuscita del bene dal patrimonio del debitore viene meno ogni possibilità di rappresentare artificiosamente una situazione economica deteriore rispetto a quella reale[440].

Facendo applicazione di questi principi al caso sopra esemplificato, deve ritenersi che la vendita dell'immobile in cambio di *utility token* rientri appieno nella nozione di atto fraudolento. Benché l'operazione non abbia carattere simulato, il trasferimento dell'appartamento alla società ingenera una falsa rappresentazione della realtà. Il debitore continuerà infatti a godere e a disporre del bene mediante il controllo dei *token* emessi quale corrispettivo della compravendita, con facoltà di rivendere gli *asset* sul mercato in cambio di denaro.

Una seconda questione riguarda la rilevanza dei comportamenti materiali: l'ipotesi in cui il debitore erariale, avendo un conto acceso presso un fornitore di servizi di portafoglio elettronico, decida di caricare le chiavi private di accesso su un *hardware wallet* per evitare l'espropriazione presso terzi.

In dottrina si registra una disparità di opinioni in merito alla riconducibilità dei meri fatti alla categoria degli atti fraudolenti[441]. A nostro modo di vedere risulta di gran

[438] Cass. Pen., Sez. Un., 21 dicembre 2017 n. 12213. Il principio di diritto affermato dalle Sezioni Unite può essere esteso anche alla nozione di "atti fraudolenti" utilizzata all'art. 11 D. Lgs. 74/2000.
[439] Cass. Pen., Sez. Un., 21 dicembre 2017 n. 12213 § 8.2
[440] Viene fatto l'esempio del padre, oberato di debiti, che doni al figlio un immobile di proprietà. La liberalità realizza, tendenzialmente, un effettivo e definitivo impoverimento del contribuente, tale da non poter essere qualificato come fraudolento. *A fortiori*, la mera conversione di cespiti in valuta virtuale non dovrebbe assumere rilevanza penale, se la transazione non è simulata e il corrispettivo congruo. Cfr. DORIGO, *Nuovi confini giurisprudenziali del reato di sottrazione fraudolenta al pagamento di imposte*, cit., 7.
[441] Per gli opportuni riferimenti bibliografici di rinvia a INGRASSIA, *Le diverse forme di sottrazione fraudolenta al pagamento delle imposte*, cit., 385.

lunga preferibile la tesi che nega la rilevanza, ai sensi della disposizione in esame, dei comportamenti materiali. Oltre ad essere più fedele alla lettera della legge, che tecnicamente indica i soli "atti", può contare su un validissimo argomento di carattere sistematico; nel descrivere il precetto del reato di mancata esecuzione dolosa di un provvedimento del giudice (art. 388 c.p.) il legislatore fa espresso riferimento – in alternativa al compimento di atti simulati o fraudolenti – alla commissione di *«altri fatti fraudolenti»*. Dal confronto tra le fattispecie sembra possibile dedurre la volontà del legislatore di punire sotto la rubrica della sottrazione fraudolenta al pagamento delle imposte le sole condotte di abuso degli strumenti negoziali[442]. Scelta indubbiamente discutibile sul piano politico-criminale, alla quale andrebbe tuttavia data ortodossa applicazione in sede giudiziaria.

Affinché il fatto assuma rilevanza penale occorre un positivo riscontro sulla idoneità degli atti a rendere inefficace la procedura di riscossione coattiva, secondo uno schema che ricorda quello dei reati di pericolo concreto[443]. Tenuto conto della straordinaria volatilità ed evanescenza dei valori virtuali, appare piuttosto arduo ipotizzare, con riferimento alle condotte sopra esaminate, che il relativo accertamento possa dare esito negativo.

6.5. Le novità in materia di monitoraggio fiscale e i connessi profili sanzionatori.

Le norme in materia di monitoraggio fiscale sono state introdotte al fine di regolare i rapporti con l'estero nella detenzione e nel trasferimento di attività finanziarie; tale esigenza divenne particolarmente viva all'indomani dell'affermazione del principio di libera circolazione dei capitali tra gli Stati membri della Comunità. Più precisamente, con la Direttiva 88/361/CEE del Consiglio del 24 giugno 1988 il Legislatore europeo mosse il passo decisivo verso la creazione del mercato comune, richiedendo che i legislatori nazionali intervenissero al fine di eliminare le restrizioni alla libera circolazione dei capitali[444].

---

[442] Deve comunque darsi conto del fatto che la dottrina maggioritaria e la giurisprudenza sono dell'avviso opposto. L'affermazione della rilevanza *ex* art. 11 del compimento di fatti fraudolenti è giustificata dal timore per il vuoto di tutela che ingenererebbe l'opposta soluzione, con il rischio di svuotare di contenuto la disposizione incriminatrice. In giurisprudenza v. da ultimo Cass. Pen, Sez. III, 26 luglio 2017, n. 37136 secondo cui nel novero degli "altri atti fraudolenti" devono essere ricompresi tanto gli atti materiali di occultamento e sottrazione dei propri beni, quanto gli atti giuridici diretti, secondo una valutazione concreta, a sottrarre beni al pagamento delle imposte. Cfr. MUSCO, ARDITO, *Diritto penale tributario*, cit., 313.

[443] In giurisprudenza, di recente Cass. Pen., Sez. III, 11 maggio 2016, n. 35853; Sez. III 24 febbraio 2016, n. 13233. Cfr. SOANA, *I reati tributari*, cit., 445; DI VIZIO F., *Il delitto di sottrazione fraudolenta del pagamento delle imposte*, cit., 39. Sul tema, *passim* Cap. II, § 2.3.

[444] L'Italia diede attuazione alla Direttiva all'esito di un iter legislativo piuttosto tortuoso. Il Decreto del Presidente della Repubblica del 31 marzo 1988 n. 148, contenente il «Testo unico delle norme di legge in materia valutaria» consacrò il principio della libertà delle relazioni economiche con l'estero, fissando le regole fondamentali e i limiti al relativo esercizio. Successivamente fu varato da parte del Ministero del Commercio con l'Estero e del Ministero del Tesoro il D. M. 27 aprile del 1990, rubricato «disposizioni in materia valutaria». Il recepimento del quadro normativo comunitario rendeva cogente

Per recepire integralmente le disposizioni della direttiva fu emanato il D.L. 28 giugno 1990, n. 167, poi convertito in legge 4 agosto 1990, n. 227, con lo specifico intento di creare un sistema di monitoraggio dei capitali in entrata ed in uscita con l'istituzione di un controllo di tipo fiscale, in sostituzione di forme di controllo di natura prettamente valutaria.

Si prevedeva così l'obbligo, in capo ai contribuenti, di riportare nella dichiarazione annuale dei redditi e nel quadro RW una serie di informazioni sui flussi finanziari transfrontalieri e sulla detenzione di attività all'estero[445]. Tale provvedimento costituì il fondamento della normativa in materia di monitoraggio fiscale, rappresentando il *corpus* di riferimento sul quale il legislatore ha poi effettuato gli interventi "ortopedici" successivi. Il primo *step* fu l'adeguamento della disciplina dell'antiriciclaggio[446] con quella del monitoraggio fiscale, attuata con D.L. 3 maggio 1991, n. 143.

Un significativo mutamento di disciplina di ebbe con la legge 6 agosto 2013, n. 97 che ha rivisitato la disciplina del monitoraggio fiscale modificando gli art. 4 e 5 del D.L. 28 giugno 1990, n. 167 per far fronte alle necessità di semplificazione del sistema e di conformità al diritto eurounitario[447]. La *ratio* della novella è deliberatamente quella di porre rimedio alle criticità sollevate dalla Commissione Europea nell'ambito della procedura precontenziosa *EU Pilot 1711/11/TAXU* in relazione al principio della libera circolazione dei capitali. Come si evince dai lavori preparatori[448], il legislatore ha voluto dare una tempestiva risposta legislativa ai chiarimenti richiesti dalla Commissione circa l'utilità dell'obbligo di indicare nella dichiarazione dei redditi i

---

la necessità di predisporre specifiche misure di natura fiscale volte a consentire il controllo delle transazioni da e per l'estero, poste in essere dai soggetti fiscalmente residenti nel territorio italiano che, diversamente, sarebbero sfuggite alla specifica possibilità di controllo da parte dell'Amministrazione Finanziaria. Cfr. D'AGOSTINO L., *La nuova disciplina sanzionatoria del monitoraggio fiscale tra limiti eurounitari e controlimiti costituzionali: la parola alla Corte di giustizia*, in *Diritto e pratica tributaria internazionale,* 2017, 3, 957 ss.; BONFIGLIO A., *Monitoraggio fiscale e regime sanzionatorio*, in *Corr. Trib*., 2002, 27, p. 2439.

[445] Più precisamente, nella Sezione I del modulo RW il contribuente doveva indicare l'ammontare dei trasferimenti da e verso l'estero di denaro e titoli (o valori mobiliari, quali certificati del Tesoro, BOT, i BTP, i CCT e le obbligazioni emesse dalle società di capitali), per cause diverse dall'investimento all'estero o dall'attività estera di natura finanziaria effettuati attraverso soggetti non residenti, senza il tramite di intermediari residenti. La Sezione II era deputata all'indicazione della consistenza degli investimenti all'estero e delle attività estere di natura finanziaria, dai quali sarebbero potuti derivare redditi imponibili in Italia. Nella Sezione III il contribuente doveva riportare i trasferimenti da, verso e sull'estero di denaro o titoli che hanno interessato i suddetti investimenti e attività, se complessivamente superiore ai valori soglia (al tempo l'equivalente di Euro 10.000).

[446] La disciplina del monitoraggio fiscale, mutuando alcuni dei principi fondanti la struttura dell'antiriciclaggio, completa il quadro normativo in materia creando un modello omogeneo di governo del sistema di controllo fiscale e valutario degli investimenti all'estero. Ai medesimi fini il D. Lgs. 21 novembre 1997, n.461 (art. 10, comma 4) introdusse alcune disposizioni relative ad all'obbligo di segnalazione a carico degli intermediari. Successivamente il D.L. 24 dicembre 2002, n. 282, convertito in legge 21 febbraio 2003, n. 27 individuò alcune ipotesi di esenzione per determinati redditi di capitali provenienti dall'estero.

[447] Legge 6 agosto 2013, n. 97 recante «Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea».

[448] *Dossier del Servizio Studi del Senato della Repubblica*, Scheda di lettura dell'art. 10 al DDL S. 588, p. 61, http://www.senato.it

trasferimenti da o verso l'estero, pur in presenza di strumenti informativi meno onerosi per i contribuenti. Pertanto, l'intervento riformatore si caratterizza per il preciso intento di ridurre gli adempimenti a carico dei contribuenti che detengono all'estero investimenti o attività di natura finanziaria, per i quali deve essere compilato l'apposito quadro RW della dichiarazione annuale dei redditi[449].

Tra le principali novità della riforma vi è anche la soppressione dell'obbligo di monitoraggio dei trasferimenti da e verso l'estero che nel periodo d'imposta hanno interessato gli investimenti oltreconfine e le attività estere di natura finanziaria che dovevano essere indicati nella Sezione III del quadro RW. L'eliminazione fa sorgere criticità notevoli dal punto di vista della continuità normativa, in particolare nei casi in cui l'omissione dell'obbligo dichiarativo dei trasferimenti medesimi abbia dato luogo ad accertamenti fiscali (e all'irrogazione di sanzioni) non ancora divenuti definitivi[450].

In sede di recepimento della IV Direttiva antiriciclaggio il legislatore italiano ha messo nuovamente mano alla disciplina del monitoraggio fiscale. Il più volte citato D. Lgs. 90/2017, nell'inserire i prestatori di servizi aventi ad oggetto valuta virtuale tra i soggetti destinatari della normativa antiriciclaggio[451], ha esteso loro anche gli obblighi previsti dall'art. 1 del D.L. 28 giugno 1990, n. 167. Gli *exchange provider* e gli altri prestatori di servizi sono dunque tenuti[452] a trasmettere all'Agenzia delle entrate i dati relativi alle operazioni di trasferimento all'estero per importo pari o superiore a 15.000 euro, indipendentemente dal fatto che si tratti di un'operazione unica o di più operazioni che appaiano collegate per realizzare un'operazione frazionata. Ai sensi dell'art. 2 dovranno, inoltre, conservare e, a richiesta dell'Autorità, fornire evidenza delle operazioni intercorse con l'estero anche per masse di contribuenti e con riferimento ad uno specifico periodo temporale.

A nostro avviso, la scelta del legislatore di sottoporre al medesimo regime giuridico l'attività dei cambiavalute virtuali e quella degli altri operatori finanziari – pur nobile nell'intento – appare destinata all'insuccesso. Invero, l'obbligo di segnalazione e di conservazione documentale sorge ogniqualvolta gli *exchange* intervengano come intermediari «*anche attraverso movimentazione di conti, nei trasferimenti da o verso*

[449] Nella Circolare 38/E del 23 dicembre 2013 l'Agenzia delle Entrate precisa che la nuova formulazione dell'art. 4 ha condotto alla soppressione delle Sezioni I e III che caratterizzavano il precedente modulo RW con evidenti vantaggi di semplificazione degli adempimenti, in linea con quanto indicato dalla Commissione europea. Nel quadro RW il contribuente è quindi tenuto indicare soltanto la consistenza delle attività finanziarie e patrimoniali detenute all'estero nel periodo d'imposta di riferimento e senza limite di importo. Gli investimenti e le attività dovranno essere sempre dichiarati anche se al termine del periodo d'imposta siano di importo inferiore a 10.000 euro.

[450] Cfr. D'AGOSTINO, *La nuova disciplina sanzionatoria del monitoraggio fiscale tra limiti eurounitari e controlimiti costituzionali*, cit., 959

[451] *Amplius*, in questo capitolo § 3.4.

[452] Le novità introdotte dal D. Lgs. 125/2019 hanno toccato anche la disciplina del monitoraggio fiscale, poiché il richiamo contenuto nell'art. 1, comma 1, D.L. 167/1990 deve oggi essere riferito al nuovo testo dell'art. 3, comma 5, D. Lgs. 231/2007 che ha eliminato il riferimento alle attività dei cambiavalute virtuali. L'effetto pratico è che tutti i prestatori di servizi connessi all'utilizzo delle valute virtuali sono assoggettati alla disciplina del monitoraggio fiscale. Nel regime precedente, invece, l'obbligo era limitato ai servizi di cambio da e per valuta avente corso legale.

l'estero di mezzi di pagamento» (art. 1, comma 1, D.L. 167/1990)[453]. Ciò presuppone che il *provider* abbia conoscenza del luogo di destinazione delle somme, ovvero del luogo di residenza fiscale del soggetto che controlla l'indirizzo di accredito.

Sennonché, a differenza delle comuni rimesse bancarie, la residenza estera dell'avente causa non è in alcun modo evincibile dai dettagli della transazione in valuta virtuale. L'indirizzo di portafoglio viene infatti generato in modo casuale, e non presenta alcun codice identificativo che permetta di risalire alla provenienza o alla destinazione estera delle somme. Teoricamente, con l'istituzione di un archivio unico degli indirizzi registrati presso i fornitori di servizi di portafoglio elettronico sarebbe possibile ottenere simili informazioni, ma soltanto qualora il mittente o il destinatario delle somme sia stato identificato da un intermediario autorizzato. Per contro, quando la transazione provenga da (o sia diretta verso) un indirizzo di portafoglio privato, non è dato conoscere se si tratti di una operazione sottoposta o meno a monitoraggio fiscale[454].

In base a queste premesse, riteniamo che l'estensione degli obblighi di monitoraggio fiscale ai cambiavalute virtuali abbia, per il momento, natura soltanto programmatica, essendo limitata al ristretto numero di casi in cui l'utente spontaneamente dichiari di aver ricevuto somme dall'estero o di voler trasferire fondi oltreconfine, oppure ai quei casi in cui l'utente si rivolga a una piattaforma di cambio avente sede legale in Italia.

Non potrebbe del resto tacersi l'opinabilità della scelta del legislatore di circoscrivere l'ambito di applicazione della disciplina sul monitoraggio ai soli cambiavalute virtuali. Sono infatti esentati dell'obbligo di segnalazione i fornitori di servizi di portafoglio elettronico, soggetti che, più di ogni altro, intervengono nei trasferimenti di valuta all'estero[455].

---

[453] La dottrina penalistica che per prima si è occupata del tema ritiene che le disposizioni di recente introduzione attribuiscano un peso significativo alla natura monetaria dei valori virtuali. In particolare, ai fini della disciplina del monitoraggio fiscale, la valuta virtuale viene in rilievo *«quale mezzo di pagamento e segnatamente quale strumento che permette di trasferire, movimentare o acquisire, anche per via telematica, fondi, valori o disponibilità finanziarie»*. Così DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 116.

[454] L'aporia sistematica è solo apparentemente risolta dalla eventuale richiesta di informazioni al cliente sullo scopo dell'operazione (artt. 17, 35 ss. D. Lgs. 231/2007), non essendovi modo di accertare l'eventuale falsità nella dichiarazione sul luogo di destinazione delle somme. Va dunque rammentato che nel caso in cui le transazioni non avvengano attraverso intermediari, ma coinvolgano esclusivamente privati sarà comunque garantito l'anonimato delle parti coinvolte.

[455] L'effetto paradossale sta nell'aver inserito tra i destinatari degli obblighi previsti dal D.L. 167/1990 i prestatori di servizi connessi all'utilizzo delle valute virtuali *«limitatamente alle attività di conversione da e per valuta avente corso legale»*. Considerato che la disciplina si applica ai soli operatori aventi sede legale in Italia, è dato ipotizzare che l'obbligo di segnalazione avrà ad oggetto unicamente le richieste di conversione provenienti da una persona fisica o giuridica fiscalmente residente all'estero. Viceversa, laddove l'operazione sia effettuata da cittadino (o società) italiana mancherebbe il presupposto applicativo fondamentale della disciplina sul monitoraggio, cioè il trasferimento di valori da o per l'estero. Si evidenzia in tal modo una vistosa lacuna normativa: l'acquisto di valuta virtuale da parte del cittadino italiano preordinata al trasferimento dei valori all'estero sfugge completamente all'attuale disciplina normativa.

Venendo agli sviluppi più recenti, con un provvedimento del 30 gennaio 2018 l'Agenzia delle Entrate ha approvato il Modello Redditi per le persone fisiche, in cui è collocato il quadro RW, relativo ai dati degli investimenti detenuti all'estero e alle attività estere di natura finanziaria. Esso prevede, tra le varie voci, anche le attività detenute all'estero in valuta virtuale[456].

Avuto riguardo, infine, ai profili sanzionatori, la novella del 2013 ha modificato l'articolo 5 del D.L. n. 167 del 1990, riducendo sensibilmente il carico sanzionatorio per le violazioni degli obblighi di monitoraggio: la sanzione amministrativa pecuniaria – originariamente prevista nella forbice tra il 10 al 50 per cento dell'ammontare degli importi non dichiarati – è ora comminata nella misura compresa tra il 3 e il 15 per cento dell'ammontare degli importi non dichiarati[457], mentre la disposizione che prevedeva la confisca per equivalente è stata espunta. La riforma del 2017 non ha toccato l'impianto sanzionatorio del D.L. 167/1990, che rimane dunque caratterizzato dall'assenza di fattispecie di reato e dal ricorso a illeciti amministrativi sanzionati *per relationem* rispetto all'entità della violazione tributaria.

7. Ablazione patrimoniale e confisca di valori virtuali.

Il tema della confisca del profitto è divenuto ormai un *cliché* ricorrente del diritto penale dell'economia. Il dibattito tra gli studiosi è alimentato dalla introduzione di ipotesi speciali di confisca in funzione prettamente sanzionatoria[458], con l'intento di creare uno stigma contro la criminalità organizzata e la commissione di illeciti volti all'ottenimento di indebiti vantaggi patrimoniali[459].

---

[456] I soggetti tenuti alla compilazione del quadro RW sono i titolari effettivi dell'investimento, che, pur non essendo i possessori diretti degli investimenti esteri, siano residenti nel territorio dello Stato. Secondo la dottrina il presupposto di tale obbligo dichiarativo è la potenziale produzione di reddito imponibile in Italia delle attività o investimenti detenuti all'estero. In argomento v. PARISOTTO R., *Il quadro RW tra valute virtuali e normativa antiriciclaggio*, in *Corriere tributario*, 2018, 15, 1156; DE MASI M., *Le criptovalute entrano nel quadro RW*, in *Il Fisco*, 2018, 20, 1929.

[457] La sanzione è tuttavia applicata in più alta misura, compresa tra il 6 e il 30 per cento dell'ammontare degli importi non dichiarati, qualora la violazione abbia ad oggetto investimenti all'estero ovvero attività estere di natura finanziaria detenute negli Stati o territori a regime fiscale privilegiato indicati nel decreto del Ministro delle finanze 4 maggio 1999 e nel decreto del Ministro dell'economia e delle finanze 21 novembre 2001 (c.d. *black list*).

[458] MANES V., *L'ultimo imperativo della politica criminale:* nullum crimen sine confiscatione, in *Riv. it. dir. proc. pen*., 2015, 3, 1260 ss.

[459] La letteratura sul tema della confisca è davvero vasta. Tra le monografie più recenti v. Senza pretese d'esaustività recenti in materia: FORNARI L., Criminalità del profitto e tecniche sanzionatorie. Confisca e sanzioni pecuniarie nel diritto penale "moderno", Padova, 1997; MAUGERI A. M, *Le moderne sanzioni patrimoniali tra funzionalità e garantismo*, Milano, 2001, 127; ALESSANDRI A., *La confisca*, in ID. (a cura di), *Il nuovo diritto penale delle società*, Milano, 2002; ID., *Criminalità economica e confisca del profitto*, in DOLCINI E., PALIERO C.E., *Studi in onore di Giorgio Marinucci*, Milano, 2006, 2107; FONDAROLI D., *Le ipotesi speciali di confisca nel sistema penale. Ablazione patrimoniale, criminalità economica, responsabilità delle persone fisiche e giuridiche*, Bologna, 2007; ID., *Splendori e miserie della confisca obbligatoria del profitto*, in ID. (a cura di), *Principi costituzionali in materia penale e fonti sovranazionali*, Padova, 2008, 117 ss.; VERGINE F., *Confisca e sequestro per equivalente*, Milano, 2009; GRASSO G., *sub* Art. 240, in ROMANO M., GRASSO G., PADOVANI T. (a cura di), *Commentario*

Il movente lucrativo che muove la criminalità di impresa suggerisce di far leva su un articolato sistema sanzionatorio composto da pena, sanzione amministrativa e misure di sicurezza patrimoniale. La combinazione di questi fattori solleva problematiche di non poco conto in punto di violazione del *ne bis in idem* sostanziale e di individuazione del soggetto (persona fisica o ente) destinatario delle misure di ablazione patrimoniale.

La dottrina prevalente ha ampiamente superato l'inquadramento codicistico tra le misure di sicurezza, mettendo in luce il progressivo venir meno della funzione preventiva della confisca, avvalorata – nelle ipotesi speciali – dall'astrazione del giudizio di pericolosità e dalla possibilità di aggredire anche beni o denaro di valore equivalente[460]. Specialmente in relazione alla forma indiretta, non sono mancate in giurisprudenza prese di posizione nel senso della funzione precipuamente sanzionatoria dell'istituto[461] emersa di pari passo con l'allentamento del nesso di pertinenzialità dei beni confiscati con l'illecito. La dottrina più attenta ha addirittura parlato di una funzione compensativo-ripristinatoria – distinta da quella preventiva e punitiva – che fornirebbe una spiegazione all'applicazione della misura anche nei casi di estinzione del reato per intervenuta prescrizione[462].

Delle questioni oggi più dibattute potremo occuparci soltanto cursoriamente, nell'ambito di una riflessione dedicata, più in generale, agli strumenti di ablazione patrimoniale dei valori virtuali. Il tema non può essere affrontato unicamente dalla prospettiva del diritto penale sostanziale, mettendo da parte gli aspetti più critici relativi all'esecuzione delle misure ablative. Riservandoci di esaminare questi ultimi nel prosieguo della trattazione[463], dovremo ora dar conto degli attuali margini di operatività della confisca in caso di condanna per uno dei delitti in precedenza esaminati.

L'art. 240 c.p. indica come obbligatoria la confisca dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione determinati reati informatici *«nonché dei beni che ne costituiscono il profitto o il prodotto ovvero di somme di denaro, beni o altre utilità di cui il colpevole ha la disponibilità per un valore corrispondente a tale profitto o prodotto, se non è*

---

sistematico del codice penale, Milano, 2011, 606 ss.; EPIDENDIO T.E., *La confisca nel diritto penale e nel sistema delle responsabilità degli enti*, Padova, 2011; NICOSIA E., *La confisca, le confische. Funzioni politico-criminali, natura giuridica e problemi ricostruttivo-applicativi*, Torino, 2012; MENDITTO F., *Le confische di prevenzione e penali*, Milano, 2015; MAZZACUVA F., *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico*, Torino, 2017, 95 ss.;

[460] Cfr. ALESSANDRI, *Criminalità economica e confisca del profitto*, cit., 2107 ss.

[461] Tra le pronunce più importanti v. Cass. Pen., Sez. Un., 31 gennaio 2013, n. 18374, *Adami*; Cass. Pen., Sez. Un., 30 gennaio 2014, n. 10561, *Gubert*, in *Diritto penale contemporaneo*, 12 marzo 2014, con nota di TRINCHERA T., *La sentenza delle Sezioni Unite in tema di confisca di beni societari e reati fiscali*; Cass. Pen., Sez. Un., 26 giugno 2015, n. 31617, *Lucci*; Cass. Pen., Sez. Un., 25 ottobre 2005, n. 41936, *Muci*, in *Cass. Pen.*, 2006, 3, 1387 ss. Anche la Corte Costituzionale ha affrontato il tema da punto di vista del rispetto dei principi fondamentali della materia penale v. sent. 196/2010; ord. 97/2009; sent. 112/2019.

[462] In tal senso v. MAZZACUVA, *Le pene nascoste*, cit., 174 a proposito della citata sentenza Lucci (Cass. Pen., Sez. Un., 26.6.2015, n. 31617) e del tema c.d. della confisca senza condanna.

[463] *Infra*, Cap. V, § 7

possibile eseguire in via diretta la confisca del profitto o del prodotto»[464]. Considerato che nell'elenco figurano sia l'accesso abusivo (art. 615-*ter*) che la frode informatica (art. 640-*ter*), la misura troverà applicazione, anche nella forma per equivalente, in tutte le ipotesi di sottrazione e indebito utilizzo di chiavi crittografiche[465]. Lo stesso dicasi in caso di condanna o applicazione della pena su richiesta per i reati di riciclaggio, reimpiego e autoriciclaggio ai sensi dell'art. 648-*quater* c.p.

Similmente, ogniqualvolta un reato tributario si realizzi per effetto del mancato pagamento (o dell'omessa dichiarazione) dell'imposta sulle plusvalenze di investimento o sulle operazioni in valuta virtuale, l'ablazione patrimoniale colpirà in via diretta l'indebito risparmio d'imposta oppure beni per un valore corrispondente. Pur non essendo chiaro se la confisca penaltributaria dei valori virtuali abbia forma diretta oppure per equivalente, sta di fatto che anche in questo caso la misura deve necessariamente essere ordinata.

Parimenti obbligatoria è la confisca del prezzo del reato ai sensi dell'art. 240, comma 2, n. 1, che può riferirsi a tutti quei casi in cui la valuta virtuale costituisce il bene dato o promesso, quale corrispettivo, per la commissione del reato. Si pensi alle ipotesi, sopra esaminate, di acquisto di beni intrinsecamente illeciti sul *dark web* e di *cybercrime-as-a-service*[466].

Insomma, per tutte le fattispecie di reato finora considerate l'ablazione del prodotto o del profitto del reato è, oltre che obbligatoria, applicabile anche nella forma per equivalente. Tale circostanza appare in linea con le ragioni politico criminali alla base dell'introduzione delle ipotesi speciali di confisca, trattandosi di illeciti caratterizzati da un chiaro movente lucrativo[467]. Ciò posto, sarà bene soffermarsi brevemente sul concetto di "profitto" in relazione ai valori virtuali, dando conto di alcuni profili problematici di operatività della confisca rispetto a questi ultimi.

7.1. La valuta virtuale come profitto del reato. Inafferrabilità della ricchezza digitale e limiti applicativi alla confisca.

Per evitare una eccessiva dilatazione della confisca verso vantaggi economici non direttamente riconducibili al fatto illecito, la giurisprudenza di legittimità ha precisato che il profitto del reato consiste *«nel vantaggio di natura economica ovvero nel beneficio aggiunto di tipo patrimoniale di diretta derivazione causale dall'attività del*

[464] Ai sensi dell'art. 240, comma 2, numero 1-*bis*, c.p. è sempre ordinata la confisca […] dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui agli articoli 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*,617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies*, 640-*ter* e 640-*quinquies*, nonché dei beni che ne costituiscono il profitto o il prodotto ovvero di somme di denaro, beni o altre utilità di cui il colpevole ha la disponibilità per un valore corrispondente a tale profitto o prodotto, se non è possibile eseguire la confisca del profitto o del prodotto diretti.

[465] *Supra*, § 5 ss.

[466] *Supra*, § 4.3.

[467] Per un efficace contrasto alla cybercriminalità economica risulta senza dubbio opportuno sottrarre definitivamente al reo i vantaggi economici comunque connessi o collegati alla condotta illecita.

reo», sicché, laddove si proceda a confisca dei profitti "indiretti" occorre, in ogni caso, che *«il bene sia ricollegabile in modo preciso all'attività criminosa posta in essere dall'agente»*[468]. Che il beneficio economico espresso in moneta virtuale rientri nella nozione di profitto accolta dal diritto vivente non è dato dubitare; la definizione è volutamente ampia, tale da ricomprendere qualsiasi entità suscettibile di valutazione economica. Gli aspetti più controversi riguardano il *modus operandi* della confisca, che dovrà essere adattata alle peculiarità degli *asset* virtuali.

Per sottrarre al reo la disponibilità di questi ultimi si dovranno anzitutto superare le logiche tradizionali, legate alla materialità dei beni o alla centralizzazione nella gestione del denaro, mettendo a punto strumenti investigativi innovativi e incentivi processuali volti ad ottenere la collaborazione della persona sottoposta alle indagini. La fruttuosa esecuzione del provvedimento dipenderà dalla disponibilità dell'indagato a "trattare" con l'autorità, specie nelle ipotesi in cui la gestione della ricchezza avvenga al di fuori del controllo di qualsiasi intermediario[469].

La volatilità del prezzo dei valori virtuali rischia inoltre di mettere in crisi la definizione stessa di profitto. Si pensi, ad esempio, alla omessa indicazione di plusvalenze di investimento che superino le soglie di punibilità del delitto di dichiarazione infedele (art. 4, D. Lgs. 74/2000), realizzate nell'arco di un periodo d'imposta, ma successivamente venute meno a causa di una contrazione del mercato valutario virtuale. Sarà possibile in questo caso disporre la confisca nonostante la sopravvenuta perdita di valore dei titoli? A quale parametro si dovrà fare riferimento per determinare la misura del profitto confiscabile?

È questo un problema che investe, più in generale, tutti i provvedimenti aventi ad oggetto *asset* speculativi. Nelle ipotesi che abbiamo esaminato, il deprezzamento potrebbe verificarsi anche in un arco temporale molto ristretto, ad esempio tra la data di pronuncia della sentenza di condanna e il giorno dell'esecuzione della misura. Ai fini della confisca si dovrà far riferimento al valore nominale indicato nel provvedimento, oppure rivalutare l'importo considerando le perdite realizzatesi *medio tempore*?

Assumiamo che un soggetto sia condannato per frode informatica consistita nell'aver fatto indebito uso delle chiavi crittografiche altrui al fine di impossessarsi di una certa quantità di valuta virtuale. Se alla data del fatto il valore venale dei *token* era di molto superiore rispetto al giorno in cui è pronunciata la sentenza di condanna, a quale parametro dovrà attenersi il giudice nel commisurare il *quantum* del profitto da sottoporre a confisca? Se la misura fosse eseguita in forma diretta sul *tantundem* – vale a dire *token* dello stesso tipo e per la stessa quantità di quelli sottratti – si avrebbe una

[468] Cass. Pen., Sez. Un., 27 marzo 2008, n. 26654 con cui la Suprema Corte ha preso posizione su una delle questioni più discusse intorno alla nozione di profitto. Il dubbio interpretativo verteva sulla possibilità di assoggettare a confisca i soli vantaggi economici derivati in via diretta dalla commissione dell'illecito, ovvero anche i vantaggi non immediati. La tesi restrittiva, inizialmente prevalente, è stata nel tempo accantonata in favore di una lettura estensiva, che ammette la confisca anche dei beni non direttamente derivanti dal reato, ma costituenti oggetto del successivo reimpiego del profitto originario.
[469] Il tema coinvolge diversi profili processuali, sui quali v. *infra*, Cap. V § 6

ablazione patrimoniale "monca" perché il valore attuale dei beni è nettamente inferiore rispetto al profitto conseguito; laddove invece fosse disposta nella forma per equivalente su altri beni nella disponibilità del reo, per un valore corrispondente a quello originario, si finirebbe per presumere in modo assoluto che questi ha realizzato un utile convertendo i *token* sottratti alla quotazione che avevano al tempo. Per procedere correttamente si dovrebbe dapprima accertare – anche facendo uso di tecniche di *blockchain forensics* – se i valori sono stati trasferiti dal conto dell'imputato verso un terzo indirizzo e, in caso di riscontro positivo, la relativa data. Ove le somme siano rimaste immobili il giudice potrà rivalutare l'entità del profitto originaria al prezzo attuale degli asset, ordinando la confisca per il valore corrispondente. Al contrario, se figura dal libro mastro pubblico una transazione verso un altro contro, il giudice si potrà legittimamente presumere che il reo abbia conseguito un vantaggio economico corrispondente al valore di scambio dei beni alla data di tale trasferimento.

Numerosi soni dunque gli interrogativi sollevati dalla virtualizzazione dei patrimoni e dalla instabilità dei mercati valutari digitali. Sono tutte questioni ancora inesplorate, che giungeranno all'attenzione degli operatori del diritto di pari passo con la progressiva diffusione della moneta decentralizzata come strumento di pagamento.

7.2. Risparmio d'imposta e confisca diretta del denaro. *Quid iuris* nel caso della moneta virtuale?

Tra le disposizioni di maggiore interesse contenute nel D. Lgs. 24 settembre 2015 n. 158 spiccano quelle dirette a ridisegnare la disciplina della confisca del profitto del reato tributario, contenute nel nuovo articolo 12-*bis* del D. Lgs. n. 74 del 2000. In materia penaltributaria, una forma di confisca per equivalente era prevista già prima della riforma. Infatti, l'art. 1, comma 143, della l. n. 244/2007 (ora abrogato dal D.lgs. n. 158/2015) sanciva l'applicabilità della confisca di cui all'art. 322-*ter* c.p. rispetto a numerosi reati tributari. Il nuovo art. 12-*bis* si limita a ripetere la formulazione della disposizione prevista per i delitti contro la pubblica amministrazione; in questo la riforma si è limitata a conferire all'istituto una più razionale collocazione sistematica, inserendolo nell'ambito suo proprio[470]. Non cambia, dunque, il *modus procedendi* per il giudice che pronunci sentenza di condanna per un reato tributario: egli sarà chiamato a verificare, anzitutto, se sia possibile procedere alla confisca diretta dei beni che costituiscono profitto del reato; solo laddove verifichi l'impossibilità di apprendere direttamente il profitto dovrà disporre la confisca di valore, cioè l'ablazione di una parte

[470] Rispetto alla previgente disciplina, la novella ha esteso l'ambito di operatività della confisca in quanto richiama, genericamente, tutti i delitti previsti dal decreto legislativo n. 74/2000, consentendo di applicare la misura ablativa anche al reato di occultamento o distruzione di scritture contabili di cui all'art. 10, non incluso nella elencazione precedente. Sul tema v. MELIS G., *La nuova disciplina degli effetti penali dell'estinzione del debito tributario,* in *Rass. Trib.* n. 3/2016 p. 589 ss.; D'AGOSTINO L., *L'operatività della confisca e le sorti del sequestro preventivo in presenza di impegno al pagamento del debito tributario: in dubio pro reo?*, in *Rivista Trimestrale di diritto tributario,* 2017, 2, 367 ss.

del patrimonio legittimamente posseduto dal condannato, avente valore corrispondente all'ammontare del profitto derivante dal reato.

La definizione di profitto assume una connotazione molto peculiare nel diritto penale tributario. Fino a non molto tempo addietro era radicata la convinzione che l'infedeltà fiscale non generasse alcun vantaggio economico aggiuntivo nel patrimonio dell'evasore, sicché si tendeva ad escludere che i reati tributari potessero essere interessati da strumenti di ablazione patrimoniale diversi dalle procedure di riscossione coattiva dei crediti[471]. Con l'approvazione della legge finanziaria 2008 si ebbe un repentino cambio di rotta dovuto alla necessità di dare un senso alle previsioni legislative; la giurisprudenza iniziò a individuare il profitto confiscabile nel risparmio di spesa che, pur non comportando alcuna variazione fisica del patrimonio del contribuente, rappresenta un vantaggio economico aggiuntivo che questi non avrebbe ottenuto se avesse adempiuto ai suoi obblighi fiscali[472]. Detto altrimenti, il risparmio di spesa equivale a quella parte di guadagno che il contribuente avrebbe dovuto computare, nel suo reddito complessivo, ai fini del pagamento delle imposte.

Con la celebre sentenza Gubert[473] le Sezioni Unite hanno preso posizione a favore dell'orientamento prevalente, affermando che la confisca del profitto disposta sul denaro o altri beni fungibili, non è confisca per equivalente, ma confisca diretta. La tesi è stata ampiamente criticata in dottrina sulla scorta della condivisibile considerazione che, in tal modo, viene meno l'accertamento del nesso di pertinenzialità tra il bene oggetto di confisca e l'utile prodotto dal reato[474]. Senza scendere nel merito della delicata questione possiamo qui limitarci a segnalare che l'odierno diritto vivente ritiene che, nei reati tributari, il profitto assoggettabile a confisca coincida con il risparmio di spesa realizzato dall'evasore e può essere aggredito direttamente presso la persona giuridica, avendo ad oggetto denaro o altri beni fungibili.

La tesi avallata dalla giurisprudenza solleva numerosi interrogativi in relazione all'oggetto della presente trattazione. Si faccia il caso del gestore di una piattaforma di *e-commerce* che, omettendo di dichiarare i corrispettivi percepiti in valuta virtuale, evada l'imposta sul valore aggiunto per svariati milioni di euro. In caso di condanna per il reato di cui all'art. 4 D. Lgs. 74/2000, la confisca potrà essere disposta (ed eseguita) direttamente sui valori virtuali posseduti dalla società?

---

[471] Per approfondimenti sull'evoluzione giurisprudenziale si vedano, per tutti, in BRICHETTI R, VENEZIANI P., *La confisca*, in ID. (a cura di), *I reati tributari*, cit., 464 ss.

[472] Si vedano, tra le più autorevoli, Cass., Sez. Un., 23 aprile 2013, n. 18374, Adami, in *Cass. pen.*, 2013, 4, 2913; Cass. Pen., Sez. II, 16 gennaio 2012, n. 1199; Cass. Pen., Sez. V, 10 novembre 2011, n. 184 nelle quali di afferma il principio di diritto secondo cui in tema di reati tributari il profitto è costituito da «*qualsivoglia vantaggio patrimoniale direttamente conseguito alla consumazione del reato e può, dunque, consistere anche in un risparmio di spesa come quello derivante dal mancato pagamento del tributo*».

[473] Cass. Pen, Sez. Un., 30 gennaio 2014, n. 10561, *Gubert*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2015, 4, con nota di PALIERO C.E., MUCCIARELLI F., *Le Sezioni Unite e il profitto confiscabile: forzature semantiche e distorsioni ermeneutiche;* in *Guida al diritto,* 2014, 15, 85, con nota di BRICHETTI R.

[474] Cfr. GULLO A., *Autoriciclaggio e reati tributari*, in *Diritto penale contemporaneo*, 13 marzo 2018, 11 ss.; PALIERO C.E., MUCCIARELLI F., *Le Sezioni Unite e il profitto confiscabile*, cit., 247 ss.

A stretto rigore l'indebito risparmio d'imposta, che dà luogo al profitto confiscabile, è rappresentato dalla moneta avente corso legale, trattandosi dell'unico mezzo solutorio dell'obbligazione fiscale. L'equiparazione compiuta dalla sentenza *Gubert* tra il denaro e gli altri beni fungibili lascia tuttavia presupporre che il provvedimento ablatorio possa colpire anche gli *asset* virtuali. Non solo questi soddisfano appieno il requisito della fungibilità, ma costituiscono anche l'utilità economica originaria prodotta dall'illecito, senza che vi sia stata alcuna ulteriore trasformazione del denaro in beni di altra natura per l'investimento o il reimpiego del profitto illegittimamente ottenuto[475].

Parimenti, sembra doversi ammettere la possibilità di disporre la confisca diretta dei valori virtuali nel caso del contribuente infedele che utilizzi le riserve monetarie per acquistare criptomoneta anziché per pagare le tasse. Difatti, la giurisprudenza considera come "profitto del reato" non soltanto i beni che l'autore del reato apprende per effetto diretto ed immediato dell'illecito, ma altresì di ogni altra utilità che lo stesso realizza come conseguenza, anche indiretta o mediata, della sua attività criminosa[476]. A ciò si aggiunga che, nel caso appena descritto, il contante digitale potrebbe a certe condizioni persino considerarsi lo strumento per realizzare una sottrazione fraudolenta al pagamento delle imposte. Sarebbe in tal caso ancor più evidente il legame di diretta pertinenzialità tra l'illecito e le utilità economiche da questo derivate.

7.3. Osservazioni conclusive.

A chiusura dell'indagine sulle nuove frontiere della criminalità economica, riteniamo di dover richiamare l'attenzione sui numerosi interrogativi sollevati dalla diffusione della moneta *peer-to-peer*. La dematerializzazione degli scambi e la virtualizzazione della proprietà portano alla deriva un concetto di patrimonio, inteso come signoria su informazioni digitali. Affidare alle fattispecie comuni il presidio penale contro le aggressioni della ricchezza digitale potrebbe risultare talvolta problematico, per via dei limiti imposti dal principio di stretta legalità.

Si impone peraltro la necessità di porre un freno allo sfruttamento delle nuove risorse in via strumentale per il compimento di attività illecite come il riciclaggio e il trasferimento fraudolento di valori, il traffico di droga, il finanziamento del terrorismo, l'evasione fiscale.

L'analisi svolta in questo capitolo dimostra come le fattispecie attualmente vigenti siano in linea di principio sufficienti a far fronte alle sfide lanciate dal nuovo fenomeno. Sul fronte repressivo non si evidenziano lacune normative o zone franche da responsabilità penale anche grazie all'ampia copertura offerta dal delitto di frode

[475] Depone in questo senso anche la riconosciuta funzione monetaria di Bitcoin, che la Corte di Giustizia ha richiamato proprio a proposito dell'assoggettamento ad IVA delle operazioni di conversione da e per valuta avente corso legale. *Amplius*, in questo capitolo § 6.1.

[476] Principio ormai consolidatosi in seno alla Suprema Corte a partire da Cass. Pen., Sez. VI, 21 ottobre 1994 n. 4114, richiamata in più punti dalle Sezioni Unite *Gubert*.

informatica (art. 640-*ter* c.p.). La fattispecie, introdotta con la riforma degli anni novanta, si distingue per la formidabile duttilità applicativa e rappresenta un baluardo irrinunciabile dinanzi alla sofisticazione degli attacchi informatici.

Sorgono però molti dubbi sul titolo di responsabilità cui ricondurre condotte *borderline* come la sottrazione di chiavi crittografiche e l'intestazione fittizia di capitali virtuali, nonché problematiche di varia natura sulla individuazione e la sottrazione del profitto e del prezzo del reato integrato da *asset* digitali.

Ad ogni modo, le preoccupazioni maggiori riguardano l'enorme cifra nera della *underground economy* virtuale, alimentata dalla possibilità di trasferire valori senza ricorrere all'opera di terzi intermediari. La questione trascende l'area di competenza del diritto penale sostanziale, spostandosi verso il fronte della prevenzione amministrativa e della cooperazione investigativa. L'efficacia deterrente delle disposizioni incriminatrici dipende, invero, dalla percezione soggettiva sull'attivazione della macchina della giustizia per la punizione dei responsabili. In questa direzione risulta fondamentale assumere consapevolezza del fenomeno, superando quel timore verso l'*ignoto digitale* che, negli ultimi decenni, ha indotto atteggiamenti di ingiustificata chiusura da parte degli operatori del diritto.

Ebbene, proprio sul fronte preventivo il legislatore ha lanciato un importante monito mediante l'estensione della normativa antiriciclaggio a tutte le attività di acquisto, scambio e utilizzo di valori virtuali "per finalità speculative"[477]. Su tali finalità si dovrà ora concentrare l'attenzione per cogliere i punti di contatto più significativi tra diritto penale e disciplina finanziaria.

[477] Si richiama al riguardo la "nuova" nozione di valuta virtuale introdotta dal D. Lgs. 125/2019, che ha modificato l'art. 1, comma 2, lett. qq) del D. Lgs. 231/2007.

CAPITOLO IV

VALORI VIRTUALI E TUTELA DEL MERCATO FINANZIARIO.

SOMMARIO: 1. Dal mezzo di pagamento allo strumento d'investimento: l'informazione digitale come *asset* di natura finanziaria. – 1.1. La "piazza" finanziaria virtuale tra mercato di scambio ed economia di prodotto. Considerazioni iniziali sulla necessità di tutela degli interessi collettivi. – 1.2. L'*asset* virtuale come strumento finanziario. *Bene iudicat qui bene distinguit*? – 1.2.1. I margini applicativi della definizione nazionale di prodotto finanziario. – 1.2.2. *Trading* valutario e normativa antiriciclaggio. Rinvio. – 1.3. Il *Fintech Action Plan* e le prime misure di attuazione. – 1.4. Tipologia, natura e funzioni dei *token*. Incertezze ricostruttive ed equilibrismi classificatori. – 2. Regolazione finanziaria, tutela dell'investitore e prerogative di controllo pubblico. Riflessioni sulla opportunità di un approccio flessibile alla tutela penale del risparmio. – 2.1. *Blockchain* e *Fintech*. Spunti comparatistici sulle prime esperienze regolatorie. – 2.1.1. L'esperienza statunitense e quella canadese. – 2.1.2. La legislazione giapponese. – 2.1.3. L'esperienza svizzera. Rinvio. – 2.1.4. La normativa di Malta e di San Marino. – 2.2. Verso un modello di regolazione flessibile? Il punto di vista della Consob sull'emissione e lo scambio di criptoattività. – 2.2.1. Rilievi critici. – 3. Abusivismo bancario e finanziario. Profili di rilevanza penale dell'esercizio non autorizzato delle attività e dei servizi di investimento. – 3.1. Il regime autorizzatorio previsto dal D. Lgs. 90/2017. Limiti esegetici e criticità applicative delle fattispecie di abusivismo previste dal Testo Unico Bancario. – 3.1.1. Conclusioni in punto di irrilevanza penale dell'esercizio non autorizzato dell'attività di cambiavalute virtuali. – 3.2. Esercizio non autorizzato di "servizi" e le "attività" di investimento. I vasti orizzonti applicativi dell'art. 166 del Testo Unico della Finanza. – 3.3. L'ineludibile certezza del diritto. Riflessioni sull'opportunità di regolare l'emissione e lo scambio di criptoattività finanziarie. – 4. *Trading* di asset virtuali e tutela del mercato finanziario. – 4.1. L'inapplicabilità delle fattispecie di *market abuse*. – 4.2. Omissioni informative e falsità in prospetto. – 5. Prospettive *de iure condendo*. L'assoggettamento dei valori virtuali alla disciplina finanziaria e i riflessi sul versante sanzionatorio.

1. Dal mezzo di pagamento allo strumento d'investimento: l'informazione digitale come *asset* di natura finanziaria.

Il tema della natura giuridica dei valori virtuali è quello che, fino ad oggi, ha maggiormente attirato l'attenzione della dottrina[1]. Per quanto la questione possa apparire astratta o priva di fondamento pratico, presenta in realtà un nodo estremamente concreto: il dualismo tra funzione monetaria e speculativa delle informazioni scambiate in *blockchain*.

Trattando dell'utilizzo della moneta *peer-to-peer* come mezzo di pagamento, si è fatto cenno all'elevata propensione degli attori economici ad acquistarla e scambiarla

[1] Si vedano tra i primi commentatori, GASPARRI G., *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. Inf.*, 2015, 1, 429; VARDI N., *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. Inf.*, 2015, 1, 450 ss.

per finalità meramente speculative, circostanza che mette in luce l'esistenza di forti similitudini con le *securities* finanziarie[2]. Lungi dal permettere una qualificazione in termini generali, la natura ibrida dei valori virtuali impone a nostro avviso di considerare – in base allo specifico segmento di disciplina – quale sia la funzione economica preponderante. Se fino a qualche tempo fa non si avvertiva neppure il problema di un inquadramento dei valori virtuali tra gli asset finanziari, in tempi recenti vi è stata una forte presa di coscienza in tal senso, che ha condotto il legislatore italiano ad estendere la nozione di valuta virtuale, al fine di far rientrare tra gli elementi definitori anche l'utilizzo "per finalità d'investimento"[3].

I dubbi sulla natura finanziaria degli *asset* virtuali sorgono spontanei, se solo si considera che la maggior parte degli utenti è interessata al *trading* nella speranza di ottenere una rapida remunerazione del capitale investito. La tendenza deflazionistica dei valori induce gli operatori a trattenere o a cedere le attività in base alle aspettative di andamento del mercato. Gli investitori non istituzionali saranno per lo più portati a detenere per lungo tempo l'*asset* sperando in una sua rivalutazione: l'emissione di una quantità predeterminata di circolante osta così alla diffusione dei valori virtuali come mezzo di pagamento, accentuandone il connotato finanziario.

Osservando questa "irrituale" dimensione finanziaria con le lenti del giurista, affiorano numerosi interrogativi sul *come* il fenomeno debba essere regolato. Non si potrebbe seriamente credere che in una società progressivamente sempre più digitalizzata le forme nuove di proprietà e di raccolta del risparmio debbano sfuggire alle prerogative di controllo pubblico. Non potrebbe del resto ignorarsi l'esistenza di norme imperative di legge che regolano l'emissione e lo scambio di attività qualificabili come finanziarie, rispetto alle quali si pone il problema di definire precisamente il campo di applicazione. Laddove l'emissione e lo scambio fossero ricondotti nel perimetro delle attività regolamentate, soggiacerebbero *in toto* alla disciplina di settore; diversamente sarebbero da ricondurre a un regime di esercizio libero, sottratto alla supervisione statale. Nel dubbio sulla scelta che possa attuare il più razionale bilanciamento tra interessi individuali e collettivi, la stasi normativa non è certamente la strada migliore. Eppure il legislatore si è finora ben guardato dall'intervenire, consegnando nelle mani dell'interprete la soluzione di un problema piuttosto "scottante".

L'interrogativo di fondo è dato dall'opportunità di proteggere alcuni beni giuridici tradizionali – già oggetto di riconoscimento normativo – quali la stabilità del mercato finanziario e la fiducia nello stesso, il risparmio, l'autodeterminazione e l'interesse patrimoniale degli investitori. L'indagine svolta nel presente capitolo avrà pertanto a oggetto la tutela penale di questi beni collettivi dinanzi ai rischi di una economia virtuale priva di regole. A tal fine sarà necessario alzare il tiro e guardare al fenomeno

[2] Si richiamano le riflessioni svolte nel precedente capitolo al paragrafo § 1.3.
[3] *Amplius*, a proposito della "nuova" nozione di valuta virtuale introdotta dal D. Lgs. 125/2019 v. Cap. III, § 1 e 3.4.

dalla prospettiva del mercato, in modo da cogliere i possibili punti di tensione con il quadro normativo vigente.

1.1. La "piazza" finanziaria virtuale tra mercato di scambio ed economia di prodotto. Considerazioni iniziali sulla necessità di tutela degli interessi collettivi.

I valori digitali registrati in *blockchain* sono stati fino ad ora considerati come mezzo di pagamento e veicolo di circolazione della ricchezza. Un tale utilizzo assume rilevanza per la configurabilità di diverse ipotesi di reato, accomunate dalla funzione *lato sensu* monetaria che a detti valori può essere riconosciuta[4].

Mutando la prospettiva d'indagine, si guarderà ora all'*asset* virtuale come strumento per il finanziamento di progetti imprenditoriali, finalizzato alla raccolta di risparmio e alla successiva quotazione su mercati secondari di scambio[5].

Guardando al nuovo fenomeno dalla prospettiva macroeconomica, ci si rende subito conto dell'esistenza di un fiorente mercato, in cui la domanda e l'offerta di valori virtuali hanno raggiunto proporzioni davvero ragguardevoli. In questo "universo parallelo" la compravendita di *asset* di natura finanziaria è del tutto libera dai vincoli dei mercati regolamentati. Se da un lato ciò alimenta il timore per i rischi associati alla criptomoneta, dall'altro apre le porte al paradiso della speculazione, non essendovi limiti all'aumento del prezzo dei titoli o procedure particolari per la concentrazione di valori nelle mani di pochi investitori.

Si tratta di un mercato che a pochi anni dalla sua nascita vanta una capitalizzazione di quasi 300 miliardi di dollari statunitensi[6] che, per rendere l'idea, è in proporzione il PIL nominale annuo di uno stato di medie dimensioni. Queste statistiche dovrebbero far seriamente pensare all'opportunità di introdurre regole a tutela della concorrenza e della fiducia degli investitori, non diversamente da quanto accaduto con l'affermazione del mercato della finanza tradizionale. Senza entrare nel merito di una questione[7] davvero complessa, *de iure condito* l'idea di una tutela penale del mercato dei valori virtuali sembra un'ipotesi purtroppo ancora remota.

Le attuali dimensioni del "mercato della blockchain" – misurabili in termini di capitalizzazione del mercato, volume di transazioni, numero di *start-up*, platea di investitori – sono da sé sufficienti a spiegare le ragioni di una riflessione avente ad

[4] Non a caso fino alla recente novella l'unica definizione legislativa di valuta virtuale, contenuta nel D. Lgs. 231/2007, faceva sull'utilizzo come mezzo di scambio per l'acquisto di beni o servizi.

[5] Esiste oggi una congiuntura molto stretta tra decentralizzazione degli scambi ed economia virtuale. Sebbene, in linea di principio, la *distibuted ledger technology* permetta la disintermediazione nella gestione di rapporti di qualunque genere, le applicazioni nel campo economico-finanziario ne hanno segnato il vero successo. La natura ibrida (valutaria, finanziaria e monetaria) degli *asset* virtuali ne consente un utilizzo differenziato a seconda dei bisogni di ciascuno: come strumento di pagamento, come riserva di valore, come capitale di rischio.

[6] Per statistiche aggiornate si visiti il sito *internet* https://coinmarketcap.com

[7] Il tema sarà esaminato nel prosieguo, v. *infra* § 5

oggetto, da un lato, l'impatto della circolazione dei nuovi valori sul sistema finanziario tradizionale, e dall'altro la necessità di dettare le "regole del gioco" della piazza finanziaria virtuale[8]. Quand'anche si volesse ricondurre il fenomeno all'autonomia negoziale dei privati, considerando la finanza virtuale un modo innovativo di fare *business* mediante le tecnologie della comunicazione e dell'informazione, ci si dovrebbe comunque interrogare sui limiti imposti dall'ordine pubblico. Al riguardo ci sembra opportuno richiamare le conclusioni dell'Autorità Bancaria Europea (EBA) che nel rapporto del 2014[9] aveva espresso serie preoccupazioni per la possibile destabilizzazione dell'integrità finanziaria dell'Unione a causa della crescita del mercato valutario virtuale. Partendo da rischi per gli utenti, per i professionisti e per le imprese – distinti a seconda che le valute virtuali siano utilizzate come strumento di pagamento ovvero di investimento – il documento individua oltre trenta minacce per il sistema economico nel suo complesso, che incombono, in particolare, sull'integrità del mercato finanziario, sui sistemi di pagamento in valuta corrente, e sulle Autorità pubbliche di vigilanza.

Una attenzione particolare è rivolta alla necessità di salvaguardare le prerogative di controllo pubblico sulla stabilità finanziaria all'interno del mercato unico. Secondo la EBA l'economia della *blockchain* rischia di condurre all'erosione della sfera di controllo pubblico sui sistemi elettronici di pagamento e sull'emissione di strumenti finanziari, potendo facilmente sfuggire al sistema di controlli delle autorità indipendenti. La circostanza che il livello di rischio fosse determinato in medio-basso risulta tutt'altro che incoraggiante, alla luce della macroscopica crescita che il mercato valutario virtuale ha avuto negli ultimi cinque anni[10]; non sembra fuori luogo ritenere che all'aumento degli investimenti e del volume delle transazioni abbia fatto seguito un innalzamento del coefficiente di rischio per l'integrità finanziaria. L'inerzia degli Stati e dell'Unione nel disciplinare il fenomeno rende estremamente concreto il pericolo espresso al punto E02 del documento: *«regulators do not regulate VCs but the viability of regulated financial institutions is compromised as a result of their interaction with VCs»*[11], affermazione che descrive in modo decisamente efficace le possibili contaminazioni tra le due dimensioni finanziarie. Per far fronte a tali rischi

[8] Sembra che soltanto in tempi recenti questi temi abbiano ancora suscitato l'interesse della dottrina. Cfr. ANNUNZIATA F., *Speak if you can: what are you? An alternative approach to the qualification of token and ICOs*, Bocconi legal studies research paper, n. 2636561, in attesa di pubblicazione in *European Company and Financial Law Review*; CARRIÈRE P, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche di "strumenti finanziari", "valori mobiliari" e "prodotti finanziari"; tra tradizione e innovazione*, in *Rivista di diritto bancario*, 2019, 2; ANNUNZIATA F., *Distributed Ledger Technology e mercato finanziario: le prime posizioni dell'ESMA*, in PARACAMPO M.T. (a cura di), *FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2017, 229 ss.; GIRINO E., *Criptovalute: un problema di legalità funzionale*, in *Rivista di Diritto Bancario*, 2018, 55, 2 ss.

[9] Il riferimento è alla già richiamata *Opinion on virtual currencies* del 04 luglio 2014. Cfr. Cap. III, § 2.1.

[10] Quando fu pubblicato il rapporto della EBA il mercato aveva un a quota di capitalizzazione cinquanta volte inferiore rispetto a quello attuale (all'incirca 7 miliardi di dollari contro i quasi 300 attuali).

[11] *Opinion on virtual currencies*, cit., 22 -36.

l'Autorità europea sollecitava le Istituzioni verso un *«immediate and consistent regulatory response across the EU»* per disciplinare in modo adeguato le attività di emissione e scambio di valori virtuali. Il monito è rimasto tuttavia privo di riscontro poiché, fatta eccezione per le novità introdotte con la quinta direttiva antiriciclaggio, il legislatore non ha ancora preso posizione per regolare gli aspetti più propriamente finanziari del mercato valutario virtuale.

Che gli orizzonti di tutela del mercato debbano estendersi ai valori dell'economia virtuale, è un assunto che trova conferma nella *biridezionalità* del flusso della criptomoneta. Com'è noto, i possessori di valute virtuali "quotate" su piattaforme di scambio possono facilmente convertire i propri averi in moneta avente corso legale, e viceversa. Questa possibilità fa apparire un vero "portale dimensionale" tra i due mondi – quello dell'economia reale e quello dell'economia virtuale – attraverso cui transitano, a doppio senso di marcia, quantità enormi di denaro[12].

Se da una parte lo scambio di valori di natura finanziaria presenta rischi notevoli per la stabilità dei mercati regolamentati, dall'altra appaiono evidenti i limiti all'applicazione delle fattispecie di reato poste a salvaguardia degli investitori. La definizione di "strumento finanziario"[13] sembra escludere che la moneta virtuale possa beneficiare della tutela penale prevista per i mercati regolamentati; se così fosse, risulterebbero inapplicabili non soltanto le fattispecie di abuso di informazioni privilegiate e manipolazione del mercato di cui, rispettivamente, agli artt. 184 e 185 TUF, per l'evidente ragione della non quotazione in borsa dei valori virtuali, ma anche la fattispecie di aggiotaggio comune di cui all'art. 2637 c.c. dal momento che il requisito della *price sensitivity* è riferito appunto al prezzo degli strumenti finanziari non quotati o per i quali non è stata presentata richiesta di ammissione alle negoziazioni in un mercato regolamentato. L'inerzia del legislatore nel disciplinare il mercato della finanza virtuale potrebbe pertanto condurre all'ulteriore effetto negativo di incentivare condotte di *market abuse* a danno degli investitori.

1.2. L'*asset* virtuale come strumento finanziario. *Bene iudicat qui bene distinguit*?

Secondo la legge nazionale un mezzo di pagamento non può, per definizione, essere incluso nella categoria degli strumenti finanziari[14]. Questi ultimi rappresentano, come

[12] Una asimmetria nella tutela del denaro (reale o virtuale) produrrebbe l'effetto perverso di consentire ai criminali informatici la scelta del luogo in cui delinquere per essere esposti a un minor carico sanzionatorio. Un risultato questo palesemente irragionevole, se lo si inquadra nella cornice di una ormai evidente contiguità spaziale tra queste due dimensioni dell'economia.

[13] Guardando oltre i confini nazionali, è assai nota la presa di posizione dell'Autorità Finanziaria Federale tedesca (BaFin), secondo cui le criptovalute debbono essere inquadrate a tutti gli effetti tra gli strumenti finanziari, e, in quanto tali, sono sottoposte agli stringenti vincoli della normativa di settore. In dottrina, ROSEMBUJ T., *Bitcoin*, Barcelona, 2016, 75.

[14] In tal senso l'art. 1, comma 2, TUF. L'esclusione dalla definizione di strumento finanziario e valore mobiliare è anche prevista dall'art. 4, par. 1, 44) della direttiva 2014/65/UE (MIFiD II). Con tutta evidenza l'esclusione è giustificata dal fatto che per i mezzi di pagamento esiste già uno specifico *corpus*

pocanzi anticipato, una categoria chiusa e tendenzialmente tassativa, salva la facoltà di ampliamento *ex* art. 18, comma 5, TUF da parte del Ministero dell'Economia e delle Finanze.

Le difficoltà classificatore sorgono in ragione della natura ibrida dei valori virtuali, che, almeno *prima facie*, tenderebbe ad escludere la qualificazione in termini finanziari. Secondo una parte della dottrina si tratta di un ostacolo certamente superabile, poiché la natura monetaria viene in considerazione solo per alcune discipline di settore, tra cui l'antiriciclaggio e la normativa fiscale, mentre per fini diversi dovrebbe porsi l'accento sul connotato fortemente speculativo che caratterizza il circolante virtuale[15]. In effetti, il solo fatto che possa essere accettato come mezzo di pagamento non preclude la possibilità di un diverso inquadramento in base al concreto utilizzo che se ne faccia. È ormai principio radicato nella cultura giuridica moderna, pur con diverse accezioni quello di prevalenza della sostanza sulla forma, secondo cui, per un corretto inquadramento legale, dovrà guardarsi non alla forma esteriore ma alla causa concreta dell'operazione posta in essere. Facendo applicazione di questo principio al caso che ci occupa, è possibile porre un primo punto fermo: la sussunzione delle valute virtuali nelle categorie finanziarie risulta non solo possibile, ma anzi doverosa in tutte quelle ipotesi in cui assolve la funzione solutoria nasconde un fine unicamente o prevalentemente speculativo. Risulta dunque condivisibile la tesi – proposta dalla dottrina da ultimo citata – secondo cui il nuovo fenomeno andrebbe ricondotto alle categorie giuseconomiche tradizionali (investimento, finanziamento, speculazione, impiego e raccolta di capitali, appello al pubblico risparmio, intermediazione, mercato etc.) e alle connesse specifiche definizioni settoriali (servizi di investimento, valori mobiliari, prodotti finanziari).

A tali considerazioni sembra essersi ispirata l'Autorità europea di vigilanza sui mercati finanziari (ESMA) nella redazione di una avvertenza in cui richiama all'attenzione delle Istituzioni la circolazione di cripto-attività assimilabili a *securities*[16]; in mancanza di un intervento del legislatore questi valori rischiano di eludere la tassonomia dei servizi e delle attività finanziarie con effetti negativi rilevanti sul mercato regolamentato. Nello stesso documento si rivolge un invito ai legislatori nazionali a introdurre un regime specifico per quei valori che non integrano la nozione comunitaria di "strumento finanziario" [17], ipotesi che sembra aver trovato seguito nel

normativo *ad hoc* che ne disciplina la riserva di accesso al mercato e i requisiti soggettivi di esercizio dell'attività.

[15] Di quest'avviso GIRINO, *Criptovalute: un problema di legalità funzionale*, cit., 22 alla cui ricostruzione riteniamo, almeno in questa parte, di poter aderire.

[16] Il riferimento è al documento denominato *Advice on Initial Coin Offering and Crypto-Assets*, del 9 gennaio 2019, disponibile sul sito della ESMA https://www.esma.europa.eu, 36 ss.

[17] Secondo la ESMA *«EU policymakers could consider the opportunity to set up a bespoke regime for those crypto-assets that do not qualify as financial instruments. Such a bespoke regime, which would require Level 1 measures,would allow tailoring the rules to the specific risks and issues posed by those crypto-assets that do not qualify as financial instrumentsor electronic money. It may also provide for different requirements depending on the features of these crypto-assets, as somemay be further away from traditional financial instruments than others and therefore not raise the same risks and issues, e.g., 'pure' utility-type crypto-assets, which appear to have little relation to financial*

nostro paese a seguito dell'avvio di una procedura di consultazione pubblica presso la Consob[18].

Come noto, l'ordinamento italiano appresta elevate garanzie a tutela degli investitori, ampliando il campo di applicazione di alcune norme imperative oltre i confini segnati dal diritto dell'Unione Europea[19]. La creazione di una definizione nazionale di "prodotto finanziario" – più ampia di quello di "strumento finanziario" secondo la MiFID II – è l'espediente tecnico-giuridico con cui il legislatore ha avocato alla sfera di controllo pubblico le operazioni speculative caratterizzate dalla presenza di rendimenti di natura finanziaria. Ciò spiega il motivo per cui la Commissione Nazionale per le società e la borsa è intervenuta adottando numerosi provvedimenti di sospensione e ordini di inibitoria a carico di emittenti di valori virtuali stabiliti in Italia[20]. Per contro, non vi sono molti casi giunti all'attenzione della giurisprudenza di merito fatta eccezione per la nota pronuncia con cui il Tribunale di Verona ha per la prima volta affermato la natura finanziaria delle cripto-attività[21].

Ai fini della successiva disamina penalistica sul contrasto all'abusivismo, appare anzitutto opportuno esaminare entro che limiti sia possibile ricondurre un *asset* virtuale alla nozione armonizzata di "strumento finanziario" e, la relativa intermediazione nello scambio, un "servizio di investimento". Per quanto l'opera classificatoria sia complicata dalla circostanza, non escludibile *a priori*, che l'operazione sia realizzata senza intento speculativo, la soluzione al problema andrà ricercata su un piano evidentemente oggettivo.

La riconducibilità alla nozione di servizio di investimento[22] non presenta particolari problemi, dal momento che le piattaforme di scambio svolgono attività che, per molti

markets and can only be redeemed for certain goods or services (e.g. non-tradable vouchers) and certain payment-type crypto-assets» (§ 183 del documento).

[18] Il tema sarà approfondito nel prosieguo di questo capitolo (*infra*, § 6).

[19] Per approfondimenti sul tema v. CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche,* cit. 2 ss. alla cui analisi si rinvia per gli opportuni riferimenti bibliografici sul diritto dei mercati finanziari.

[20] Si vedano, tra le più recenti, la Delibera 31 ottobre 2018 n. 20660 (Sospensione, ai sensi dell'art. 99, comma 1, lett. b), del d.lgs. n. 58/1998, dell'offerta al pubblico residente in Italia avente ad oggetto "token TGA", effettuata da Togacoin Ltd); la Delibera 14 novembre 2018 n. 20693 (Sospensione, ai sensi dell'art. 99, comma 1, lett. b), del Tuf, dell'offerta al pubblico avente ad oggetto la moneta digitale denominata "Crypton"); Delibera del 19 dicembre 2018 n. 20751 (Divieto ai sensi dell'art. 99, comma 1, lett. d) del Tuf, di offerta al pubblico residente in Italia avente ad oggetto il "Piano di investimento AvaCrypto"); Delibera del 14 febbraio 2019 n. 20814 (Divieto, ai sensi dell'art. 99, comma 1, lett. d), del D. lgs. n. 58/1998, dell'offerta al pubblico avente ad oggetto investimenti di natura finanziaria promossa dalla Cryptoforce Ltd). *Amplius*, v. CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche,* ibidem

[21] Tribunale di Verona, sentenza 24 gennaio 2017, n. 195, in *Banca Borsa Titoli di Credito*, 2017, 4, 471 ss. con nota di PASSARETTA M., *Bitcoin: il leading case italiano.* Secondo il giudicante la compravendita di valute virtuali è una operazione ad alto rischio, inquadrabile tra gli strumenti finanziari, il che obbliga colui che ne pubblicizzi la vendita ad informare preliminarmente l'utente interessato all'acquisto sui rischi connessi all'investimento ex art. 67 ss. D. Lgs. 206/2005.

[22] I servizi e le attività di investimento sono puntualmente individuati dall'art. 1, comma 5, TUF nei seguenti: esecuzione di ordini per conto dei clienti; negoziazione per conto proprio; gestione di sistemi multilaterali di negoziazione; ricezione e trasmissione di ordini; sottoscrizione e/o collocamento; gestione di portafogli; consulenza in materia di investimenti.

versi, può essere assimilata alla "negoziazione" per conto proprio o dei clienti", alla "mediazione" e alla "gestione di portafogli di titoli".

Laddove la piattaforma DLT sia utilizzata come strumento per la "tokenizzazione" e la circolazione di titoli che, secondo la direttiva MiFID, sono inquadrabili nell'elenco di cui all'allegato C (che individua gli strumenti finanziari) non vi potranno essere dubbi sul regime giuridico al quale detti titoli dovranno essere soggetti. Più complesso è il caso in cui il *token* non rappresenti l'informazione digitale per la circolazione di uno strumento finanziario nominato, ma incorpori in *quid* di similare[23].

Concentrando l'attenzione sulla normativa nazionale oggetto di armonizzazione, occorre prendere le mosse dalle disposizioni contenute nel Titolo II della Parte II del D. Lgs. 58/1998. Il Testo Unico ha introdotto – recependo le indicazioni dal legislatore dell'Unione – una definizione ben precisa di strumento finanziario[24] facente leva su una elencazione che, ad avviso della dottrina, lascerebbe fuori le valute virtuali[25]. Questa tesi ci sembra assolutamente convincente, tanto più nell'ottica di una applicazione tassativa delle fattispecie penali a presidio del mercato finanziario. In senso contrario si potrebbe tuttavia argomentare che la categoria dei "valori mobiliari" di cui all'art. 1, comma 1-*bis* del TUF[26] si presta a ricomprendere anche le valute virtuali, laddove sia riscontrabile il tratto della negoziabilità ed esista un sottostante riferito a valute, indici, merci o *commodities* di altro tipo. L'obiezione non può tuttavia essere generalizzata poiché molte valute virtuali difettano dei requisiti previsti per i valori mobiliari. Si dovrà, in altre parole, effettuare una distinzione in base alle caratteristiche specifiche dei *token*, ammettendo la riconducibilità ai valori mobiliari – e dunque agli strumenti finanziari – dei soli titoli rappresentativi di quote di società o di debito oppure di valori reali regolati a pronti[27]. Riservandoci ogni opportuno

[23] La disciplina MiFID non esaurisce il quadro normativo di riferimento. Esiste infatti la direttiva AIFMD (2011/61/UE) che stabilisce le regole per l'autorizzazione, il funzionamento e la trasparenza dei gestori dei fondi di investimento alternativi (AIFM). A seconda di come è strutturata, l'offerta di *token* potrebbe qualificarsi come un fondo di investimento alternativo, nella misura in cui viene utilizzato per raccogliere capitali da un certo numero di investitori, al fine di investire in conformità con una politica di investimento definita. Le imprese coinvolte nelle ICO potrebbero pertanto dover rispettare le norme AIFMD.

[24] L'art. 1, comma 2, TUF annovera tra gli strumenti finanziari: 1) i valori mobiliari; 2) gli strumenti del mercato monetario; 3) le quote di un organismo di investimento collettivo del risparmio; 4) i contratti di opzione, contratti finanziari a termine standardizzati («future»), «swap»; gli accordi per scambi futuri di tassi di interesse e altri contratti derivati connessi a valori mobiliari; 5) altre categorie di contratti di opzione. Salvo quanto si dirà oltre, nessuna di queste categorie si presta ad includere apertamente i valori virtuali.

[25] Tale è l'opinione di CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche,* cit. 16.

[26] Per "valori mobiliari" si intendono le categorie di valori che possono essere negoziati nel mercato dei capitali, quali ad esempio: a) azioni di società e altri titoli equivalenti ad azioni di società, di *partnership* o di altri soggetti e ricevute di deposito azionario; b) obbligazioni e altri titoli di debito, comprese le ricevute di deposito relative a tali titoli; c) qualsiasi altro valore mobiliare che permetta di acquisire o di vendere i valori mobiliari indicati o che comporti un regolamento a pronti determinato con riferimento a valori mobiliari, valute, tassi di interesse o rendimenti, merci o altri indici o misure.

[27] I contratti a pronti sono una tipologia di contratti di borsa che prevedono la consegna materiale dei titoli da parte del venditore e il pagamento immediato (a pronti) da parte dell'acquirente. Per

approfondimento per la parte dedicata alle diverse tipologie di criptoattività, possiamo qui limitarci a concludere che – salvo un ristretto nucleo di ipotesi – i valori virtuali non potranno essere considerati strumenti finanziari.

1.2.1. I margini applicativi della definizione nazionale di prodotto finanziario.

La nozione di "prodotto finanziario" non viene descritta attraverso una elencazione tassativa di titoli nominati, bensì ricorrendo a una definizione in chiave funzionale. Esiste un rapporto di *genus ad speciem* tra prodotti e strumenti finanziari, giusta la nozione contenuta all'art. 1, comma 1, lett. u) TUF in cui i primi sono qualificati come *«gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria»*. Secondo la dottrina prevalente si tratta di una categoria aperta[28], facente leva su un elemento per così dire *statico* (l'individuazione degli strumenti finanziari) e su uno *dinamico* (gli investimenti aventi natura finanziaria).

Concentrando l'attenzione su questo secondo indice definitorio, emerge piuttosto chiaramente la volontà del legislatore di creare una sorta di *backdoor* di sistema, per far sì che non sfuggano allo statuto di disciplina del Testo Unito della Finanza tutte quelle ipotesi caratterizzate dagli elementi tipici degli investimenti finanziari. Si vuole in tal modo ricondurre sui binari della regolazione pubblica ogni manifestazione dell'autonomia privata che, pur non integrando la definizione (nazionale e comunitaria) di strumento finanziario, condivida con questi ultimi lo scopo e la funzione economica. Scelta sicuramente apprezzabile, poiché accresce l'elasticità del sistema permettendo un adeguamento continuo alle evoluzioni del mondo finanziario.

La locuzione si riferisce a quelle forme di impiego di un capitale caratterizzate dall'aspettativa di un rendimento e dall'assunzione di un rischio di natura finanziaria[29]; in essa potrebbe dunque rientrare ogni strumento, comunque denominato, che sia rappresentativo dell'impiego di un capitale in misura prevalente rispetto al godimento

---

approfondimenti sulla definizione v. ANNUNZIATA F., *La disciplina del mercato mobiliare*, Torino, 2014, 94 ss.

[28] CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche,* cit. 35; ANNUNZIATA, *La disciplina del mercato mobiliare*, cit., 319 ss.

[29] Nel recente documento per la consultazione pubblica *"Le offerte iniziali e lo scambio di criptoattività",* 19 marzo 2019, 5 ss. la Consob ha richiamato la propria prassi affermando che gli investimenti di natura finanziaria ricompresi nella categoria dei prodotti finanziari sono le proposte di investimento che implichino la compresenza dei seguenti elementi: (i) impiego di capitale; (ii) promessa o aspettativa di rendimento di natura finanziaria, intendendosi per tale l'accrescimento della disponibilità investita, senza l'apporto di prestazioni da parte dell'investitore; (iii) assunzione di un rischio direttamente connesso e correlato all'impiego di capitale; (iv) prevalenza del connotato finanziario rispetto a quello di godere e disporre del bene acquisito con l'operazione; (v) effettiva e predeterminata promessa, all'atto dell'instaurazione del rapporto contrattuale, di un rendimento collegato alla *res*. L'affermazione è suffragata anche dal richiamo ad alcuni precedenti di legittimità tra cui Cass. Civ., Sez. II, 5 febbraio 2013, n. 2736, secondo cui *«La causa negoziale è finanziaria ove la ragione giustificativa del contratto, e non il suo semplice motivo interno privo di rilevanza qualificante, consiste proprio nell'investimento del capitale (il "blocco" dei risparmi) con la prospettiva dell'accrescimento delle disponibilità investite, senza l'apporto di prestazioni da parte dell'investitore diverse da quella di dare una somma di denaro»*.

del bene[30]. Non può tuttavia tacersi come il criterio della prevalenza presenti in sé il rischio dell'imprevedibilità del diritto, lasciando all'interprete un margine di discrezionalità eccessivamente ampio. Si faccia il caso di un c.d. *utility token* rappresentativo di una frazione di godimento in multiproprietà di un immobile sito in una rinomata località turistica, oggetto di scambio su una piattaforma a ciò dedicata. Se da un punto di vista astratto lo schema negoziale soddisfa la nozione di "prodotto finanziario" – data l'esistenza di un mercato secondario di scambio con funzione anche speculativa – dall'altro risulta evidente l'utilità effettiva che l'acquirente dei valori trae dall'acquisto. La prevalenza del connotato finanziario rispetto a quello di godimento del bene non potrebbe che essere accertata in concreto, avendo riguardo a *quel* tipo di servizio in *quel* determinato mercato. Ma anche in tal caso l'indagine dovrebbe fare i conti con le intenzioni degli operatori economici, al fine di accertare se, in una apprezzabile maggioranza di casi, l'acquisto e la vendita siano effettuati con una aspettativa di ritorno finanziario. Benché un tale approccio "funzionale" sia giustificato dalla opportunità di tutelare gli investitori, non potrebbero non considerarsi gli effetti negativi sulla certezza giuridica e sulla libertà di iniziativa economica privata causati da un intervento *ex post* delle autorità di vigilanza del mercato.

Nel tentativo di delimitare il campo di applicazione della disciplina dei mercati finanziari all'emissione e allo scambio di valori virtuali, la dottrina più recente attribuisce rilevanza alle limitazioni al godimento del bene e alla emissione di certificati che attestino la titolarità del bene e che siano commercializzabili su un mercato secondario[31]. Detto altrimenti: nell'impossibilità di qualificare l'*asset* virtuale come prodotto dotato di intrinseca natura finanziaria, si dovrà guardare all'operazione economica sottostante per accertare la presenza di indici rivelatori quali promesse di rendimento, obblighi di riacquisto, promesse di realizzazione di profitti ovvero vincoli al godimento del bene. Solo in caso di riscontro positivo si potrà qualificare il *token* come "prodotto finanziario", applicando ai relativi servizi di investimento la disciplina prevista per l'offerta al pubblico[32]. Il proponente e l'intermediario saranno in particolare tenuti all'osservanza della disciplina del collocamento a distanza di servizi e attività di investimento *ex* art. art. 32 TUF, e del Regolamento con cui la Consob riserva tali attività ai soli soggetti abilitati. La violazione della riserva in favore di questi

[30] L'elemento della prevalenza del godimento della *res* rispetto alla rendita finanziaria ha costituito sin un importante indicatore per valutare se ad alcuni titoli di legittimazione dovesse essere applicata la disciplina dei prodotti finanziari.

[31] Si veda, in relazione alla prassi interpretativa in materia di emissione di certificati di vendita di diamanti e altri preziosi CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche,* cit. 40.

[32] *Contra,* GIRINO, *Criptovalute: un problema di legalità funzionale*, cit., 30 ss. il quale riconosce la natura di prodotto intrinsecamente finanziario alla criptovaluta, giungendo ad affermare che il commerciante che accetti un pagamento in criptovalute rende, per la parte del negozio afferente alle modalità solutorie, un servizio di investimento al cliente. La tesi non pare convincente, poiché tende a generalizzare l'assunto della natura finanziaria senza effettuare le opportune distinzioni in base alla causa concreta dell'operazione.

ultimi potrà assumere rilievo – come si dirà ampiamente nel prosieguo – come esercizio abusivo di attività finanziaria ai sensi dell'art. 166 TUF[33].

Dovranno inoltre rispettare le norme sull'offerta al pubblico di prodotti finanziari (art. 94 ss. TUF) che impongono una serie di obblighi di trasparenza e di informazione nei confronti degli investitori. Nel dettaglio, la proposta dovrà essere accompagnata dalla pubblicazione di un prospetto informativo redatto secondo gli schemi predisposti dalla Consob; in caso di omissione gli interessati saranno esposti alle onerose sanzioni pecuniarie di cui all'art. 191 del TUF, salva la rilevanza penale del fatto in caso di informazione mendace.

1.2.2. *Trading* valutario e normativa antiriciclaggio. Rinvio.

Il riconoscimento legislativo della natura monetaria dei valori virtuali rischia di complicare ulteriormente l'opera classificatoria. Sorge infatti spontaneo il dubbio che l'esercizio autorizzato dell'attività di cambiavalute virtuali, previsto dalla normativa antiriciclaggio, possa in parte derogare all'applicazione della disciplina dei mercati finanziari. Si potrebbe infatti ritenere – secondo un ragionamento logicamente coerente basato sul principio *ubi lex lex voluit dixit* – che la qualificazione in termini monetari dei valori virtuali escluda indirettamente il connotato finanziario, tant'è che l'art. 17-*bis* del D. Lgs. 141/2010 prevede autonomi presupposti e modalità di controllo pubblico sull'attività svolta da questi soggetti. L'argomento è suadente, ma non risolutivo. Ci pare infatti preferibile attribuire alle disposizioni introdotte dal D. Lgs. 90/2017 una valenza solo settoriale ai fini antiriciclaggio, evitando contaminazioni con la qualificazione civilistica del fenomeno. Depone in tal senso anche la *ratio* dell'intervento normativo che, lungi dall'aver disciplinato in modo organico la materia, si limitato a porre un freno all'elevato rischio di sfruttamento delle criptovalute per fini di riciclaggio.

Rinviando alle sedi più opportune l'approfondimento circa il regime autorizzatorio dell'attività di cambiavalute virtuali[34], appare qui sufficiente ribadire come l'episodico intervento del legislatore non esonera l'interprete dalla delicata indagine sulla natura finanziaria dei nuovi valori.

1.3. Il *Fintech Action Plan* e le prime misure di attuazione.

Le preoccupazioni espresse delle autorità europee di settore (BCE, EBA, ESMA) di fronte all'espansione del mercato valutario virtuale non hanno sinora condotto ad alcun organico intervento legislativo. Le Istituzioni dell'Unione hanno mostrato un atteggiamento piuttosto cauto, incline all'osservazione più che alla regolazione del fenomeno. Se ciò da un lato appare giustificato dalla necessità di non soffocare le prime

[33] *Infra*, § 3.2.
[34] *Amplius*, Cap. III, § 3.4. e in questo capitolo § 3

applicazioni della tecnologia DLT al settore finanziario, dall'altro alimenta la tendenza alla diversificazione delle legislazioni nazionali creando un *vulnus* al mercato unico e alla libertà di stabilimento.

Altrettanto timido l'approccio seguito dalla Commissione europea che di recente ha aperto una consultazione pubblica sul tema che qui ci occupa. Più precisamente, nel marzo del 2018 è stata adottata una comunicazione relativa al piano d'azione per le tecnologie finanziarie (*Fintech Action Plan*) nella quale si mettono in risalto le potenzialità della *blockchain* per il settore finanziario[35] e si affronta il tema della regolazione del settore. La Commissione richiama alcuni documenti del Parlamento europeo e del Consiglio, auspicando un quadro normativo in cui prodotti e soluzioni *fintech* innovativi possano diffondersi rapidamente in tutta l'Unione a vantaggio senza compromettere la stabilità finanziaria o la protezione dei consumatori e degli investitori. Desta stupore l'affermazione secondo cui *«allo stato attuale gli argomenti a favore di un'ampia azione legislativa o regolamentare o di un'ampia riforma a livello dell'UE siano limitati»*[36], che a nostro avviso dimostra a chiare lettere la superficialità dell'approccio sinora seguito. È infatti lecito domandarsi come sia possibile conseguire l'obiettivo prefigurato, scongiurando il rischio di possibili abusi a danno degli investitori, senza un quadro regolamentare di riferimento. L'interrogativo sembra aver solo sfiorato l'attenzione della Commissione che, dopo aver ricordato dell'esistenza di disposizioni relative all'autorizzazione e alla vigilanza sui fornitori di servizi finalizzata a garantire la stabilità, l'integrità e l'equità dei mercati, conclude che *«la maggior parte dei modelli di business innovativi possa funzionare con le attuali norme UE, dato che il quadro legislativo dell'UE prevede la possibilità di applicare il principio della proporzionalità nel processo di autorizzazione»*[37]. Le autorità europee di vigilanza vengono dunque invitate a censire – entro il primo trimestre del 2019 – gli attuali approcci all'autorizzazione e alla concessione di licenze per i modelli di *business fintech* innovativi[38].

Tra le linee della futura azione legislativa, alcune importanti precisazioni riguardano le procedure di identificazione elettronica finalizzate alla conoscenza dei clienti (*Know Your Customer*). L'obiettivo a breve termine sarà quello di consentire

[35] Comunicazione COM(2018) 109 della Commissione al Parlamento europeo, al Consiglio, alla Banca Centrale europea, al Comitato economico e sociale e al comitato delle Regioni, in https://ec.europa.eu. Nel documento si dà atto di come le nuove tecnologie stiano *«modificando il settore finanziario e il modo in cui consumatori e imprese accedono ai servizi, creando opportunità che consentono alle soluzioni basate sulle fintech di migliorare l'accesso ai finanziamenti e l'inclusione finanziaria dei cittadini connessi digitalmente. Le tecnologie finanziarie sono importanti anche per l'Unione dei mercati dei capitali. Esse possono contribuire ad approfondire e ampliare i mercati dei capitali nell'UE integrando la digitalizzazione per cambiare i modelli di business attraverso soluzioni basate sui dati, ad esempio nella gestione patrimoniale, nell'intermediazione negli investimenti e nella distribuzione dei prodotti»*.

[36] Così a pagina 5 della Comunicazione COM(2018) 109

[37] Tale era la posizione condivisa dai partecipanti alla consultazione pubblica, alla quale la Commissione sembra aderire.

[38] Nel dettaglio esse dovranno esaminare in che modo le autorità nazionali applicano la proporzionalità e la flessibilità nella legislazione sui servizi finanziari.

agli operatori finanziari l'identificazione dei clienti attraverso tecnologie digitali nel rispetto degli obblighi antiriciclaggio e delle disposizioni sulla protezione dei dati personali, facendo ricorso agli strumenti di identificazione e autenticazione elettroniche previsti dal regolamento eIDAS[39].

Venendo infine alle misure di attuazione del piano, si segnala l'avvenuta presentazione di una proposta di modifica della direttiva 2014/65/UE[40], avente come unico scopo l'inclusione dei fornitori di servizi di *crowdfunding* tra i soggetti destinatari della MiFID II. Il *crowdfunding* è una soluzione *fintech* che offre alle PMI un canale di accesso alternativo ai finanziamenti. Esso contribuisce a un sistema finanziario più diversificato e meno dipendente dalle banche, limitando quindi gli effetti negativi derivanti dalla concentrazione dei capitali. La tecnologia *blockchain* ha massimizzato le potenzialità di questo strumento grazie alla creazione di valori tokenizzati, facilmente acquistabili e trasferibili tra privati, che attribuiscono al possessore uno più diritti connessi all'investimento[41].

Con la risoluzione legislativa del 27 marzo 2019 il Parlamento europeo ha approvato il testo con emendamenti, invitando la Commissione alla presentazione di ulteriori modifiche. Appare particolarmente significativa l'aggiunta di un nuovo *considerandum* (5-*bis*) che, partendo da una constatazione sulla fungibilità delle valute virtuali rispetto alle altre forme di investimento, mette in guardia sul fatto che *«i mercati delle valute virtuali mancano di trasparenza, possono essere soggetti ad abusi di mercato e soffrono della mancanza di una protezione di base per gli investitori»*, sicché si dovrebbe *«tenere sotto controllo le valute virtuali e proporre orientamenti chiari che definiscano le condizioni alle quali esse potrebbero essere classificate come strumenti finanziari e, se necessario, aggiungere le valute virtuali all'elenco degli strumenti finanziari come nuova categoria»*. Non resta dunque che augurarsi che il monito lanciato dal Parlamento sulla necessità di regolare da punto di vista finanziario le valute virtuali possa mettere fine allo stato di torpore della legislazione comunitaria, inducendo la Commissione a cambiare rotta rispetto ai (discutibili) propositi esposti nel piano d'azione per le tecnologie finanziarie.

1.4. Tipologia, natura e funzioni dei *token*. Incertezze ricostruttive ed equilibrismi classificatori.

Nel corso della trattazione è stato più volte accennato al fatto che i valori virtuali assumono funzioni economiche diverse, in base alla fiducia che gli operatori ripongono in essi come strumento per la circolazione dei diritti o come mezzo per l'estinzione

[39] Per agevolare di questi strumenti, la Commissione ha costituito un apposito gruppo di esperti sulle procedure di identificazione elettronica e sulle procedure KYC remote.

[40] Proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva 2014/65/UE relativa ai mercati degli strumenti finanziari COM (2018)0099 – C8-0102/2018 – 2018/0047(COD).

[41] La raccolta di capitali mediante offerta di valori virtuali (ICO, STO etc.) presenta alcune similitudini con il *crowdfunding.* Si vedrà infatti come la Consob abbia inteso ricondurre ad esso la vendita di *token* per il finanziamento di progetti imprenditoriali (v. *infra*, § 2.2.).

delle obbligazioni pecuniarie. A differenza della nozione di valuta virtuale, normativamente definita, quella di *token* sfugge completamente all'attenzione del legislatore. Il sostantivo, di derivazione anglosassone, indica una informazione digitale preziosa poiché artificialmente scarsa, univocamente identificabile, non duplicabile e trasferibile all'interno di un sistema di registri distribuiti[42]. A stretto rigore un *token* non è altro che un segmento di informazione scambiabile tra coloro che utilizzano l'infrastruttura: non possedendo valore intrinseco né efficacia solutoria propria, la quotazione sul mercato dipende dalla fiducia degli operatori economici in ciò che rappresenta o che è in grado di rappresentare. In alcuni casi il possesso dell'informazione attribuisce al titolare un diritto ad ottenere una prestazione o a ricevere la consegna di una cosa determinata; in altri il *token* rappresenta un paniere di beni reali sottostanti, ma il possessore non può esercitare sugli stessi alcuna facoltà; in altri ancora si ha una totale astrazione dall'economia tangibile, tale per cui l'*asset* è accettato e scambiato come valore in sé[43].

Nel gergo tecnico si parla di tokenizzazione per indicare la procedura di incorporazione di una risorsa o un diritto in un *asset* digitale. Si tratta, in buona sostanza, di una riedizione contemporanea della "cartolarizzazione" istituto già noto alla dottrina civilistica[44]. Si comprende quindi come i *token* abbiano un ambito di applicazione molto più vasto di quello delle valute virtuali, essendo fruibili per una molteplicità di utilizzi diversi da quello di pagamento; essi fungono da veicolo per la circolazione di diritti o da titolo di legittimazione a determinate prestazioni.

Ogni tentativo di inquadrare i *token* entro precisi schemi classificatori peccherebbe di incompletezza e parziarietà, trattandosi di una materia sottoposta all'azione plasmante dell'autonomia negoziale dei privati. Ciononostante si registra una tendenza piuttosto diffusa[45] alla individuazione di alcune categorie in base a due diversi approcci: uno formale l'altro funzionale.

---

[42] Sul tema, senza pretese di esaustività, v. CAPONERA A., GOLA C., *Questioni di Economia e Finanza – Aspetti economici e regolamentari delle 'cripto-attività'*, Paper 484 – Marzo 2019, in https://www.bancaditalia.it; CARRIERE P., *Criptovalute, tokens e ICOs nel vigente ordinamento finanziario italiano: prime note*, in Rivista di diritto bancario, 10 dicembre 2018; DI VIZIO, *Le cinte daziarie del diritto penale*, cit., 103 ss.; FRANZA E., *Le valute virtuali e prodotti finanziari con sottostanti valute virtuali. Una prima indagine sugli interventi*, in http://foroeuropa.it; HACKER, P., THOMALE C., *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*, in *European Company and Financial Law Review*, 2018, 645 ss..

[43] Nelle infrastrutture totalmente decentralizzate i *token* fungono da incentivo economico per coloro che partecipano al processo di validazione delle transazioni. Per contro, nelle *blockchain* private o ibride esiste un titolare della rete (o amministratore di sistema) in capo al quale far gravare i rapporti giuridici derivanti dall'acquisto e dallo scambio di valori virtuali; questi ultimi potranno dunque rappresentare diritti e/o crediti da far valere nei suoi confronti. *Amplius*, Cap. I, § 2.3.

[44] Per spunti di carattere storico sull'istituto, v. di recente SEVERI C., *La tutela degli investitori nella cartolarizzazione dei crediti*, Milano, 2007, 2 ss.;

[45] L'esigenza di redigere una tassonomia dei valori virtuali è stata avvertita anche dalle autorità di settore. Si veda ad esempio la citata risoluzione dell'Agenzia delle Entrate 14/2018 sul regime fiscale relativo alla offerta di valori virtuali, nella quale si fa più volte riferimento alla categoria degli *utility token*; la guida della FINMA svizzera (*Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offering* (ICO), 16 febbraio 2018, in https://finma.ch) nella quale si distinguono tre diverse categorie (*token* di pagamento, di investimento e di utilizzo); la

La *classificazione formale* distingue i valori in base a ciò che rappresentano. Il soggetto emittente può obbligarsi nei confronti degli acquirenti, dichiarando che le singole unità virtuali incorporano porzioni di diritti su beni materiali (es. proprietà o altro diritto reale di oro, diamanti, quantità di energia, merci, porzioni di edificio, terreni) o immateriali (diritti reali e situazione giuridiche di appartenenza su *smart properties*, *know-how*, licenze d'uso, avviamento imprenditoriale, certificati o attestazione di qualità) oppure diritti di credito e diritti potestativi (pretese creditorie discendenti da qualsiasi rapporto giuridico, obbligazioni, titoli di credito, diritti di voto, titoli di legittimazione).

Al contrario, la *classificazione funzionale* considera i *token* come strumento per il raggiungimento di un obiettivo economico da parte del soggetto emittente. Si distingue al riguardo tra valori emessi per raccogliere capitali e valori emessi per far funzionare la piattaforma *blockchain* o un servizio offerto tramite di essa. Quanto ai primi, basti richiamare la pratica denominata *Initial Coin Offering* (ICO), vere e proprie forme di *crowdfunding* in *blockchain* in cui gli investitori acquistano i valori virtuali in attesa di un solido ritorno del capitale attraverso l'aumento del valore dei *token*, senza che a ciò corrisponda necessariamente un diritto da esercitare nei confronti dell'emittente[46]. Nel secondo caso, invece, l'unità virtuale funziona come incentivo economico per i nodi *blockchain*, fungendo da corrispettivo per la validazione delle transazioni; la remunerazione del capitale investito viene garantita dall'esistenza di un mercato secondario in cui i *token* possono essere scambiati per valuta reale o altri beni di consumo.

Partendo da questa *summa divisio* la prassi ha evidenziato ulteriori categorie, risultanti dalla commissione di elementi definitori formali e funzionali.

Per porre l'accento sull'incorporazione di diritti di proprietà o altro diritto reale o di godimento su uno o più beni determinati o determinabili si è delineata la nozione di *asset token*: l'unità di conto virtuale rappresentativa di una frazione indivisibile di tali diritti. Pur dovendo accertare in concreto la causa effettiva del negozio, si può ragionevolmente assumere che l'offerta di tali valori abbia un connotato finanziario recessivo rispetto alla prevalente funzione di godimento del bene. Laddove venga meno la caratteristica della prevalenza del godimento rispetto alle attese di rendimento finanziario, il negozio non potrà essere ricondotto nel perimetro applicativo della disciplina di settore[47].

---

comunicazione (*Guidance note to the financial instrument test*, in https://mfsa.com) con cui l'Autorità finanziaria maltese (MFSA) ha fornito agli addetti ai lavori un test per saggiare la natura finanziaria o meno di una *security* virtuale.

[46] Ci sono varie forme di raccolta di capitale mediante l'offerta al pubblico di asset virtuali (*crypto crowdfunding*) che assumono diverse denominazioni in base alla tipologia di *token* offerta (STO, ETO etc.) e alle modalità di lancio dell'offerta.

[47] Per approfondimenti, v. CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche*, cit., 37 ss.

Al polo diametralmente opposto si collocano i *virtual token*, valori spesso utilizzati per il finanziamento di progetti in *blockchain*, che non hanno alcuna funzione, né rappresentano alcun diritto al di fuori dell'infrastruttura stessa. In essi è predominante la funzione di finanziamento del progetto imprenditoriale e di utilizzo come *medium* di scambio all'interno del sistema; il prezzo di mercato dipende in misura pressoché totale dalla fiducia degli investitori nella buona riuscita del progetto e nel raggiungimento degli obiettivi fissati nel *white paper*. La qualificazione in termini finanziari è qui avvalorata non solo dall'evidente l'intento speculativo che muove gli investitori ma anche dalla presenza a valle di un mercato secondario di scambio. Per non violare apertamente le norme sulla raccolta non autorizzata del pubblico risparmio i promotori delle offerte scambiano *virtual token* per criptovalute servendosi di specifici *smart contract*. Sarà la prassi a dover chiarire se il negozio possa essere ricondotto a una tradizionale permuta civilistica (art. 1552 c.c.) ovvero a una offerta atipica di prodotti finanziari.

La categoria in assoluto più fluida è quella degli *utility token*: unità virtuali che attribuiscono al possessore il diritto a ottenere una prestazione. Solitamente possono essere utilizzati per l'acquisto di beni o servizi offerti dal soggetto emittente, già esistenti sul mercato o di futura produzione/commercializzazione. Il parallelismo con i *voucher* commerciali (o buoni sconto), che a fini fiscali sembrerebbe tutto sommato appropriata[48], non appare risolutiva del regime applicabile nella fase di offerta al pubblico. La riconducibilità di questa tipologia di *token* alla nozione di prodotto finanziario non può in alcun modo essere vagliata in astratto; soltanto un puntuale riscontro in concreto delle caratteristiche tipiche di un "investimento di natura finanziaria"[49] potrà orientare il delicato compito dell'interprete. Si dovrà dunque tener conto delle aspettative di rendimento di natura finanziaria, dell'assunzione di rischi direttamente connessi e correlati all'impiego di capitale, della eventuale prevalenza del connotato finanziario rispetto a quello di godere e disporre del bene acquisito con l'operazione, della promessa, all'atto dell'instaurazione del rapporto contrattuale, di un rendimento collegato alla *res*[50].

Nessun dubbio insiste invece sulla qualificazione in termini finanziari dei *security token*. La denominazione, mutuata dal gergo borsistico anglosassone[51], viene utilizzata per indicare quei valori che incorporano contratti di investimento, rappresentando un credito nei confronti dell'emittente o di un terzo, obbligazioni, prodotti e derivati finanziari. Possono distinguersi alcune sottocategorie: quella degli *equity token*,

[48] In tal senso si veda la posizione espressa dall'Agenzia delle Entrate nell'interpello n. 956-39/2018, Risposta n. 14 (v. Cap. III, § 6.2.).
[49] *Supra*, § 1.2.1.
[50] Cfr. Consob, *Le offerte iniziali e lo scambio di criptoattività*, cit., 5 ss.
[51] TIWARI N., *The Commodification of Cryptocurrency*, in *Michigan Law Review*, vol. 117, 3, 612 ss.; MENDELSON M., *From Initial Coin Offerings to Security Tokens*: *U.S. Federal Securities Law Analysis*, in *Stanford Technology Law Review*, 2019, vol. 22, 52 ss.; Securities and Exchange Commission (SEC), *Report of investigation pursuant to section 21(a) of the securities exchange act of 1934: the DAO*, Release No. 81207 / July 25, 2017, in https://www.sec.gov;

rappresentativi di quote di partecipazione alla proprietà della società emittente[52], e quella dei *debt token*, incorporanti debiti/obbligazioni, assimilabili ai *bond* del mercato finanziario tradizionale.

La *Securities and Exchange Commission* (SEC) americana ha recentemente pubblicato sul proprio sito un documento concernente l'applicazione del noto *Howey Test* al settore che qui interessa[53], fornendo delle linee guida orientative agli operatori economici che intendano trattare prodotti virtuali. L'approccio pragmatico seguito dalle autorità statunitensi non ha eguali nel nostro ordinamento, caratterizzato dalla totale assenza di indicazioni (legislative o amministrative) sulla applicazione delle categorie finanziarie tradizionali all'economia della tokenizzazione. Pur non potendosi prescindere neppure in questo caso da una valutazione *case-by-case* della causa concreta del negozio, risulta abbastanza chiara la prossimità tra la tipologia di *token* in esame e quella dei prodotti finanziari. Non potrebbe peraltro escludersi la qualificazione degli stessi come "valori mobiliari" che comportano *«un regolamento a pronti determinato con riferimento a valori mobiliari, valute, tassi di interesse o rendimenti, merci o altri indici o misure»* (art. 1, comma, 1-*bis*, TUF). La definizione si presta a ricomprendere anche le cosiddette *stablecoin* concepite per minimizzare la volatilità dei prezzi, mediante l'ancoraggio del valore di scambio alle valute *fiat* oppure alle principali *commodities* del mercato internazionale[54]. Per alcune di esse si pongono però significativi ostacoli, dovuti alla prevalente funzione di pagamento che le caratterizza. Laddove il prezzo nominale di cambio sia indissolubilmente legato all'andamento di una valuta reale – o almeno il mercato lo concepisce come tale – le prospettive di rendimento finanziario sono assimilabili all'acquisto di una valuta estera. Diversamente nel caso in cui il sottostante sia rappresentato da una *commodity* come l'oro: l'andamento crescente della quotazione del bene sul mercato internazionale evidenzia chiaramente la natura di derivato finanziario propria del valore virtuale.

Le precisazioni appaiono rilevanti per la possibilità di inquadrare i *security token* tra gli strumenti finanziari, da cui derivano conseguenze significative non solo per l'assoggettamento alla disciplina MiFID ma anche sul versante penalistico[55].

---

[52] Il valore virtuale finisce così per incorporare le azioni o le quote della società emittente. Il prezzo di scambio sul mercato dipende, non diversamente dai comuni mercati finanziari, dalle aspettative degli investitori sull'andamento economico dell'impresa.

[53] Securities and Exchange Commission (SEC), *Framework for "Investment Contract" Analysis of Digital Assets*, April 3, 2019, in https://www.sec.gov. Si deve tuttavia precisare che il documento è stato redatto dal FinHub costituito presso la SEC e non ha valore ufficiale. Esso si limita a fornire alcune precisazioni su questioni che la Commissione aveva già affrontato in precedenza.

[54] Attualmente sulle più note piattaforme di *exchange* vengono vendute oltre 200 *stablecoins*. Queste valute accrescono la fiducia nel mercato valutario virtuale e ne garantiscono la crescita. Oggi più che mai questa tipologia di *token* è sotto i riflettori mondiali a seguito della pubblicazione del *white paper* di Libra, la valuta virtuale promossa da Facebook Inc. con l'intento di istituire, mediante una complessa operazione negoziale, un innovativo strumento di pagamento intercontinentale. Per approfondimenti, v. https://libra.org

[55] La questione sarà approfondita *infra* § 3.2. a proposito della configurabilità delle fattispecie di abusivismo bancario e finanziario.

La classificazione proposta è soltanto orientativa poiché nella maggior parte dei casi le unità virtuali hanno contenuto ibrido a seconda della funzione socio-economica adempiuta[56]. Basti pensare, ad esempio, a un *token* rappresentativo di una quota di proprietà su un immobile ma anche di un diritto nei confronti dell'usufruttuario del bene; oppure ai valori virtuali utilizzati come strumento di *crowdfunding*, ma utilizzabili anche per effettuare scambi o attivare uno *smart contract*. Risultando il fenomeno insuscettibile di cristallizzazione entro rigidi schemi classificatori, si dovrà necessariamente abbandonare l'impronta teorica in favore di un approccio più pragmatico. Risulterà in tal senso fondamentale guardare all'esistenza di mercato secondario in cui gli operatori scambiano i valori con prevalente finalità speculativa. Laddove il riscontro sia positivo che senso avrebbe collocare il valore nell'una piuttosto che nell'altra categoria? Nessuno, chiaramente. Le regole sull'emissione e l'offerta di prodotti finanziari dovrebbero trovare applicazione a prescindere da ciò che il *token* rappresenta o dallo scopo del suo utilizzo.

2. Regolazione finanziaria, tutela dell'investitore e prerogative di controllo pubblico. Riflessioni sulla opportunità di un approccio flessibile alla tutela penale del risparmio.

La disamina storica dell'evoluzione della disciplina dei mercati finanziari – dalle origini fino al *Fintech* – richiederebbe un impegno tale da non poter essere assolto in questa sede. Ci limiteremo pertanto ad una sommaria esposizione della fisionomia del sistema, così da fornire le premesse per il successivo approfondimento penalistico del tema.

L'ambito di disciplina in esame è caratterizzato dalla contrapposizione di due diverse esigenze: da una parte, quella di evitare l'eccesso di regolamentazione e, per l'effetto, l'imposizione di eccessive restrizioni al finanziamento dell'impresa; dall'altra, quella di offrire ai risparmiatori un livello di tutela tale da preservare la fiducia riposta nell'integrità e nel corretto funzionamento del mercato finanziario. L'espressione "mercato finanziario" indica l'insieme delle attività di gestione del risparmio riconducibili al settore bancario, assicurativo e dell'intermediazione finanziaria mobiliare ed immobiliare. La divisione tra questi settori non è più così netta come in passato, essendo sempre più strette le forme di integrazione tra imprese finanziarie e sedi di negoziazione dei prodotti di ciascuna.

La disciplina dei mercati finanziari si è storicamente caratterizzata per la sottoposizione delle attività degli emittenti e degli intermediari a rilevanti poteri pubblicistici di regolamentazione e di vigilanza[57]. Nel corso degli anni il quadro

[56] Alla natura ibrida dei *token* fa riferimento anche l'Autorità finanziaria svizzera (FINMA) nella *Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offering*, cit., 3 ss.

[57] Cfr. DE BELLIS M., voce *Mercati finanziari (disciplina pubblicistica)*, in *Enciclopedia Treccani Online*, 2018, 1 ss.; CAPRIGLIONE, F., *Finalità della supervisione ed articolazione dei controlli pubblici*,

normativo ha subito rilevanti modifiche, che hanno inciso sull'ampiezza e tipologia dell'intervento pubblico e sulla conformazione dell'assetto istituzionale.

Il modello di vigilanza è nato negli anni Trenta come gemmazione del controllo statale sull'attività esercitata dalle banche. Una delle linee principali dell'azione legislativa era la separazione tra istituti di deposito e istituti d'affari (o banche d'investimento), affermatosi a seguito della Grande Depressione del 1929. Con l'emanazione della legge bancaria del 1936, l'attività di raccolta del risparmio e di esercizio del credito furono espressamente qualificate come funzioni di interesse pubblico[58]. Vi erano forti commistioni tra l'attività di vigilanza demandata agli organi governativi e le linee politiche di indirizzo del credito. Alcuni rilevanti decisioni (quali l'autorizzazione all'esercizio dell'attività bancaria o all'apertura di filiali[59]) non dipendevano da presupposti oggettivi, ma dagli esiti della valutazione discrezionale sulle concrete esigenze del mercato.

Il modello ha subito sostanziali mutamenti negli ultimi decenni del Novecento[60]. Nel 1974 venne istituita la Commissione nazionale per le società e la borsa[61] a cui furono attribuite le funzioni in materia di borse valori fino ad allora svolte dal Ministero del Tesoro e assegnati compiti di controllo sulle società quotate. Ecco che, a partire dagli anni Ottanta, si inizia ad affermare l'idea del mercato regolamentato, nel quale i compiti di vigilanza prudenziale sono affidati ad autorità amministrative nazionali, poste in posizione di indipendenza dal potere politico[62]. Alle guarentigie di indipendenza si accompagna, da un lato, l'abdicazione del potere politico alla regolazione degli aspetti più tecnici della materia, e dall'altra la limitazione della discrezionalità amministrativa sul rilascio delle autorizzazioni per lo svolgimento delle attività bancarie e finanziarie. Questo periodo storico fu caratterizzato, secondo una parte della dottrina, dalla proliferazione dei beni giuridici funzionali alla tutela del

in ID. (a cura di), *Manuale di diritto bancario e finanziario*, Padova, 2015, 143 ss.; COSTI R., *Il mercato mobiliare*, Giappichelli, Torino, 2016, 23 ss.; ANNUNZIATA, *La disciplina del mercato mobiliare*, cit., 10 ss.

[58] Il controllo sull'attività creditizia era esercitato da tre organismi: il Ministero del Tesoro, il Comitato interministeriale per il credito e il risparmio (Cicr) e la Banca d'Italia. Rilevanti furono anche le conseguenze per il possesso della qualifica pubblicistica in capo ai funzionari delle banche. Cfr. SEVERINO P., *I delitti dei pubblici ufficiali contro la pubblica amministrazione, Le qualifiche soggettive*, Milano, 1983, 12 ss.

[59] DE BELLIS, voce *Mercati finanziari*, cit., § 2.1

[60] Negli ultimi decenni il modo di finanziamento delle imprese ha subito una profonda evoluzione: da un'impostazione prettamente "bancocentrica" si è passati progressivamente a forme di raccolta di capitali ottenute tramite l'emissione e la negoziazione di strumenti e prodotti finanziari.

[61] Legge 7 giugno 1974, n. 216. La Consob è diventata un'autorità indipendente undici anni dopo, con la legge 4 giugno 1985, n. 281 che le ha riconosciuto personalità giuridica di diritto pubblico ed un'ampia autonomia organizzativa e funzionale.

[62] L'imponente crescita dell'intermediazione non bancaria e l'internazionalizzazione degli scambi presentavano rischi notevoli per la stabilità del sistema, rendendo necessario il ricorso a nuovi strumenti di controllo pubblico sulla trasparenza e l'integrità dei mercati finanziari.

mercato: accanto alla stabilità del sistema finanziario giunsero alla deriva altri interessi pubblici, quali la tutela dei consumatori, la concorrenza del mercato e la trasparenza[63].

L'affermazione del nuovo modello procede di pari passo con il progressivo accentramento di competenze a livello dell'Unione e alla formazione di un sistema multilivello tra diritto nazionale e ordinamento comunitario, che ha toccato l'apice con la crisi finanziaria del 2009[64].

Il breve *excursus* storico aiuta a comprendere quale siano le oggettività giuridiche che interessano il diritto penale dei mercati finanziari. La dottrina più autorevole[65] ritiene che l'intero quadro di disciplina sia rivolto, direttamente o indirettamente, a tutela del "risparmio" che trova fondamento negli artt. 47 e 117, comma 2, lett. e) Cost. Interpretando quest'ultimo in senso evolutivo, adeguato al mutato contesto economico, può ritenersi superata la concezione di una sua protezione statica – finalizzata cioè ad esigenze di conservazione patrimoniale – e molto più moderna la visione del risparmio in prospettiva della tutela dell'interesse economico generale all'investimento e al rendimento fruttifero del denaro. Ben venga dunque l'individuazione di beni giuridici strumentali e funzionali alla difesa risparmio quali l'integrità e la concorrenzialità del mercato, la stabilità finanziaria, la fiducia degli investitori, la trasparenza, il corretto esercizio delle funzioni delle autorità pubbliche di vigilanza, purché non si perda di vista il valore finale che – in modo impercettibile ma indissolubile – accomuna questa pluralità di interessi. Tale considerazione si impone a maggior ragione per quelle attività che sfuggono al controllo pubblico – come appunto la circolazione di valori virtuali – a torto considerata come un *quid alieni* rispetto ai mercati regolamentati e alle sedi rituali di negoziazione. Esistono forse valide ragioni per non salvaguardare il risparmio in questa nuova proiezione del mercato finanziario? La risposta negativa si lascia ampiamente preferire anche in ragione delle strette correlazioni che esistono tra la dimensione economica reale e quella virtuale[66]. A dimostrazione di ciò basti pensare

[63] Cfr. MERUSI F., *Profili pubblicistici dell'attività parabancaria e dell'innovazione finanziaria*, in AA. VV., *Studi in onore di Massimo Severo Giannini*, Milano, 1988, 437 ss., richiamato da DE BELLIS, voce *Mercati finanziari,* cit., § 2.2.

[64] Sulla base degli artt. 114 e 127, par. 6, TFUE è stato istituito il Sistema europeo di vigilanza finanziaria (SEVIF), composto dal Comitato europeo per il rischio sistemico (CERS) e dalle tre autorità europee per i mercati finanziari – Autorità Bancaria Europea (EBA) Autorità Europea degli Strumenti Finanziari e dei Mercati (ESMA), e Autorità Europea delle Assicurazioni e delle Pensioni (EIOPA) – oltre che dai rappresentanti delle autorità di vigilanza nazionali. L'obiettivo principale del SEVIF è garantire che le norme applicabili al settore finanziario siano adeguatamente attuate negli Stati membri allo scopo di mantenere la stabilità finanziaria, promuovere la fiducia dei consumatori e offrire loro protezione. Gli obiettivi del SEVIF includono anche lo sviluppo di una cultura di vigilanza comune e la promozione di un mercato finanziario europeo unico. Nel 2012 è stata poi istituita l'Unione bancaria che ha cambiato il quadro di vigilanza dell'UE introducendo il meccanismo di vigilanza unico (SSM) il meccanismo di risoluzione unico (SRM).

[65] Sul tema v. SGUBBI F., *Il risparmio come oggetto di tutela penale*, in *Giurisprudenza commerciale*, 2005, 1, 345 ss.; ALESSANDRI A., *Un esercizio di diritto penale simbolico: la tutela penale del risparmio*, in ABBADESSA P., CESARINI F. (a cura di), *La legge per la tutela del risparmio*, Bologna, 2007, 169 ss. LOSAPPIO G., *Risparmio, funzioni di vigilanza e diritto penale. Lineamenti di un sotto sistema,* Bari, 2004, 44 ss.

[66] Sulle interferenze tra sistema finanziario tradizionale ed economia virtuale v. Cap. III, § 1.4

alla coincidenza storica tra la creazione di Bitcoin e l'inizio della crisi finanziaria globale; alla crescita esponenziale del mercato delle criptovalute in un periodo storico (2009-2019) caratterizzato dal decremento del tasso di interesse degli strumenti del mercato monetario; alla perfetta simmetria tra la contrazione dei principali indici borsistici e l'esplosione del prezzo dei valori virtuali (2017-2018). Può ancora parlarsi di un universo parallelo? Non sarebbe forse più prudente considerarlo come un mondo contiguo al mercato finanziario tradizionale? Poiché ogni aprioristica presa di posizione rischierebbe di cadere nel formalismo, è bene che le scelte di incriminazione vengano adottate seguendo un approccio di tipo realista facendo ricadere nell'ambito del penalmente rilevante quei comportamenti offensivi degli interessi – individuali e collettivi – alla tutela del risparmio, indipendentemente dalla piazza finanziaria (rituale o irrituale) in cui siano commessi.

Come noto, il presidio penalistico interessa ciascuna delle fasi di vita dell'impresa finanziaria, dal momento in cui entra sul mercato a quello in cui cessa la propria attività. Una prima forma di controllo viene esperita già in sede di accesso, subordinando l'esercizio dell'attività al rilascio di autorizzazioni e al possesso di determinati requisiti patrimoniali e organizzativi. Durante la fase operativa l'impresa è sottoposta al controllo delle autorità di vigilanza che si attua mediante obblighi di comunicazione e segnalazione e al rispetto di specifici vincoli sulla quotazione dei valori mobiliari e sul compimento di operazioni di emissione, acquisto e vendita di strumenti finanziari. Vengono qui in rilievo quelle disposizioni sull'organizzazione societaria e sulla negoziazione dei titoli, al fine di garantire la trasparenza e l'efficienza del mercato e la fiducia degli investitori[67].

Nei paragrafi che seguono l'indagine si concentrerà sul rapporto tra le prerogative di controllo pubblico e la prestazione di servizi connessi all'utilizzo delle valute virtuali, al fine di valutare se l'esercizio non autorizzato delle attività di emissione e scambio di valori integri o meno gli estremi di un fatto penalmente rilevante. Ci si interrogherà infine sulla possibilità di ricondurre alle fattispecie di *market abuse* le condotte aventi ad oggetto valori virtuali, nel caso in cui a questi vada riconosciuta natura finanziaria.

Il tema sarà affrontato da una duplice prospettiva, guardando tanto ai rischi per la tutela del risparmio collettivo e del sistema finanziario tradizionale, quanto alla meritevolezza di tutela del mercato valutario virtuale.

2.1. *Blockchain* e *Fintech*. Spunti comparatistici sulle prime esperienze regolatorie.

Nel corso dell'ultimo biennio l'atteggiamento degli Stati nei confronti delle applicazioni finanziarie della *blockchain* è profondamente mutato. Da un approccio

[67] Si prevede inoltre una apposita disciplina delle situazioni di crisi finalizzata a tutelare i risparmiatori nelle procedure di liquidazione giudiziale o amministrativa.

iniziale di indifferenza verso il fenomeno – o forse di meditata tolleranza mista a disorientamento – i legislatori hanno iniziato ora ad intraprendere le prime scelte di regolazione. Guardando agli interventi legislativi nel settore finanziario, il panorama è diviso tra chi ha disciplinato la materia con l'intento di attrarre capitali, in modo da dare certezza agli investitori, e chi invece è rimasto consapevolmente inerte affidando la tenuta del sistema finanziario ai controlli delle autorità di vigilanza. L'esperienza italiana si colloca indubbiamente in questo secondo filone, di cui fanno parte anche la maggioranza degli Stati membri dell'Unione europea.

Non si vuole qui entrare nel merito delle scelte di politica normativa, se non per ribadire come l'astensionismo del legislatore abbia finora destato una certa confusione, facendo gravare sulla Consob il delicato compito di porre limiti alle offerte di acquisto e di scambio di valori virtuali a suon di sospensive *ex* artt. 7-*octies* e 51 TUF[68]. Una funzione di "supplenza amministrativa" che, teoricamente, potrebbe facilmente essere superata mediante una previsione legislativa dei limiti e delle condizioni di liceità dell'emissione e dello scambio di valori virtuali.

Sarà dunque utile rivolgere lo sguardo oltre i confini nazionali verso quegli ordinamenti che hanno prediletto un approccio interventista alla regolazione finanziaria nella materia in esame. Non potendosi dar conto in chiave comparatistica di tutte le esperienze finora maturate, ci si soffermerà soltanto su quelle maggiormente significative.

2.1.1. L'esperienza statunitense e quella canadese.

Negli Stati Uniti la circolazione delle valute virtuali è regolata diversamente a livello nazionale, entro i limiti fissati dalla normativa federale. Tra le prime legislazioni spicca il *Bit License Act,* approvato nel 2014 dal Dipartimento dei servizi finanziari dello Stato di New York[69]. Il provvedimento detta disposizioni sulla protezione del consumatore, reca misure contro il riciclaggio e fissa gli *standard* minimi di sicurezza informatica per la gestione di servizi connessi all'utilizzo di valuta virtuale[70]. Per ottenere l'autorizzazione all'esercizio dell'attività è necessario che l'istante sia in possesso di requisiti patrimoniali minimi atti a garantirne la stabilità finanziaria.

---

[68] Per riferimenti alle delibere della Commissione v. CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche*, cit., 3; GIRINO, *Criptovalute: un problema di legalità funzionale*, cit., 24.

[69] In argomento ROSEMBUJ T., *Bitcoin*, cit., 48 ss.; 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*, 2018, 1, 19 ss. Il Bit License Act dello Stato di New York ha segnato un passo importante nel processo di regolamentazione del mercato delle valute virtuali. Prima della sua introduzione si era già posto, a livello federale, il problema della legittimità dell'esercizio delle attività commerciali connesse all'utilizzo delle criptovalute.

[70] Il provvedimento definisce la valuta virtuale come *"any type of digital unit that is used as means of exchange, or as a form of depositing digital value, or that is incorporated into a technological payment system"* (Section § 200.2, lett. p).

Tra i soggetti obbligati figurano gli intermediari che svolgono attività di *financial brokering* o altre attività connesse[71]. Le società autorizzate sono tenute a precisi obblighi di *discolusure*[72] nei confronti delle Autorità di vigilanza, nonché di informazione ai clienti sui rischi connessi all'utilizzo delle valute virtuali. Il professionista è tenuto ad avvisare, in modo chiaro e non fraintendibile dal cliente: che la criptovaluta non è valuta reale; che non gode di alcuna garanzia pubblica di rimborsabilità per valori reali; che la regolazione statale e la *public performance* sono in grado di incidere significativamente sull'uso, sul trasferimento e sul tasso nominale di cambio delle valute virtuali; che l'utente è esposto al rischio di frode o di attacchi informatici; che le transazioni in valuta virtuale sono irreversibili e che le perdite derivanti dal fatto illecito di terzi non sono in alcun modo recuperabili[73]. I soggetti autorizzati saranno inoltre obbligati a designare i responsabili della *compliance* interna[74] per assicurare il rispetto delle procedure di contrasto ai reati di frode e riciclaggio, nonché delle *policies* di sicurezza informatica, *privacy*, e sicurezza delle informazioni.

Ancora oggi si discute sull'applicabilità delle norme del Codice di diritto federale che disciplinano la registrazione dei *money transmitting businesses*[75] e puniscono con sanzioni penali molto rigide[76] l'esercizio abusivo di tali attività economiche. Guardando alla *case law* degli ultimi anni, si rinvengono alcune oscillazioni giurisprudenziali degne di nota. Nel celebre processo a carico di Charlie Shrem,

---

[71] Le attività sottoposte ad autorizzazione preventiva sono le seguenti: *«receiving and transfer of virtual currency; depositing, holding, or custody, or control of virtual currency on behalf of others; purchasing and sale of virtual currency for company use; retail sale of exchange services, including legal currency for virtual currency, or virtual currency for legal currency, exchange virtual currency for others»*. Volendo esemplificare, sono sottoposte al regime della BitLicence tutte le attività di *trading* (sia diretto che indiretto) e di custodia di valori. Restano invece esclusi i *miners* e le persone fisiche che acquistano valuta virtuale ai fini meramente speculativi.

[72] La *section 200.14* del BitLicence Act riporta un dettagliato elenco delle informazioni che, entro il quarantacinquesimo giorno dalla chiusura del trimestre fiscale, il beneficiario della licenza deve trasmettere all'Autorità di vigilanza.

[73] L'elenco delle avvertenze comprende ben dieci distinte voci. Cfr. Section § 200.19 (*Consumer protection*), par. 1, lett. a). Cfr. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta*, ibidem.

[74] La Section 200.7 dispone che *«Each Licensee shall designate a qualified individual or individuals responsible for coordinating and monitoring compliance with this Part and all other applicable federal and state laws, rules, and regulations»* (lett. b); *«Each Licensee shall maintain and enforce written compliance policies, including policies with respect to anti-fraud, anti-money laundering, cyber security, privacy and information security, and any other policy required under this Part, which must be reviewed and approved by the Licensee's board of directors or an equivalent governing body»* (lett. c).

[75] U.S. Code § 5330 (Registration of money transmitting businesses) *«(1) In general. – Any person who owns or controls a money transmitting business shall register the business (whether or not the business is licensed as a money transmitting business in any State) with the Secretary of the Treasury not later than the end of the 180-day period […]»*.

[76] U.S. Code § 5322 (Criminal penalties) *«(a) A person willfully violating this subchapter or a regulation prescribed or order issued under this subchapter […] shall be fined not more than $250,000, or imprisoned for not more than five years, or both. (b) A person willfully violating this subchapter or a regulation prescribed or order issued under this subchapter […] while violating another law of the United States or as part of a pattern of any illegal activity involving more than $100,000 in a 12-month period, shall be fined not more than $500,000, imprisoned for not more than 10 years, or both»*.

fondatore della piattaforma *BitInstant*, la Corte distretturale di New York ha condannato l'imputato a due anni di reclusione per concorso in esercizio abusivo di attività di trasferimento di denaro (§§- 5330, 5332 US Code)[77]. A diverse conclusioni è giunta la Corte distrettuale di Miami[78] che, nel disattendere la prospettazione della pubblica accusa – secondo cui la compravendita di Bitcon sarebbe sottoposta allo stesso regime autorizzatorio delle attività di trasferimento di denaro – ha ritenuto che le criptovalute non possano essere considerate alla stregua di uno strumento di pagamento[79].

I differenti esiti decisionali dimostrano che nell'ordinamento americano non vi è ancora giurisprudenza consolidata sulla riconducibilità del *trading* di criptovaluta ai servizi di intermediazione nella trasmissione di denaro[80].

Per quel che riguarda, invece, la regolazione strettamente finanziaria, il formante principale è rappresentato dai provvedimenti della Security and Exchange Commission. L'autorità è intervenuta in numerose occasioni per impedire che gli intermediari[81] del mercato valutario virtuale contravvenissero alle disposizioni del *Securities Act* federale. Tra i primi e più celebri provvedimenti si ricorda il rapporto sul caso *The DAO*, in cui la SEC ha ricondotto l'acquisto di valori virtuali a un vero e proprio contratto di investimento[82] alla stregua del celebre Howey Test[83]. Nel provvedimento viene comunque puntualizzato che la natura finanziaria non potrà essere presunta, dovendo essere oggetto di una valutazione casistica[84]. Tuttavia, nel

[77] I più importanti atti del processo sono pubblicati sul sito istituzionale https://www.justice.gov, nella pagina dell'United States Attorney's Office of Southern District of New York.

[78] State of Florida vs. Espinoza, Order Granting Defendant's Motion to Dismiss the Information (Fla. 11th Cir. Ct. Jul. 22, 2016), in https://www.jud11.flcourts.org

[79] Il provvedimento deve la sua fama alla rigida posizione espressa dall'estensore, il Giudice Pooler, secondo cui la valuta virtuale è una forma di proprietà che «ancora molta strada ha da percorrere prima di poter essere equiparata alla moneta» (*«has a long way to go before it is the equivalent of money»*), tanto che «trattare un venditore di Bitcoin come un servizio monetario sarebbe come inserire un piolo quadrato in un buco tondo» (*«like fitting a square peg into a round hole»*).

[80] In argomento MCKINNEY R. E., SHAO L. P., SHAO D. H., ROSENLIEB D. C., *The evolution of financial instruments and the legal protection against counterfeiting: a look at coin, paper, and virtual currencies*, in *Journal of Law, Technology & Policy*, 2015, 2, 273 ss.

[81] Secondo la Commissione i soggetti che offrono servizi connessi o collegati al *trading* valutario virtuale possono qualificarsi come intermediari; ciò implica l'obbligo di registrazione presso la Commissione e l'adesione a un organismo di autoregolamentazione secondo la disciplina di settore.

[8282] Securities and Exchange Commission (SEC), *Report of investigation pursuant to section 21(a) of the securities exchange act of 1934: the DAO*, Release No. 81207 / July 25, 2017, in https://www.sec.gov.

[83] SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946), secondo cui *«The 'touchstone' of an investment contract is the presence of an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others»*. Negli Stati Uniti è ormai *ius receptum* che un investimento di natura finanziaria sia caratterizzato dalla non necessaria liquidità monetaria dell'investimento, ben potendo essere effettuato tramite altre contribuzioni di valore, purché sia presente una aspettativa di profitto dipendente da sforzi gestionali altrui .

[84] Nel paragrafo conclusivo del rapporto di legge che *«Whether or not a particular transaction involves the offer and sale of a security – regardless of the terminology used – will depend on the facts and circumstances, including the economic realities of the transaction. Those who offer and sell securities in the United States must comply with the federal securities laws, including the requirement to register*

successivo caso Zaslavskiy, Recoin e DRC[85] la Commissione ha contestato più violazioni del *Securities Act* senza premurarsi di accertare in concreto l'esistenza di un contratto di investimento, facendo così gravare sugli interessati l'onere della prova contraria. Ad ogni modo, la prassi dell'autorità in materia di offerta di valori virtuali si pone in linea con i *leading cases* più noti sui requisiti per l'individuazione dei contratti finanziari. Se ne trae conferma anche dalla recente pubblicazione di un documento concernente l'applicazione del noto *Howey Test* al settore degli *asset* digitali[86].

In buona sostanza, la diffusione dei valori virtuali non ha scalfito il consolidato orientamento sulla qualificazione in termini finanziari dei contratti di investimento. In mancanza di una presa di posizione del legislatore federale sembra che il sistema abbia comunque trovato un suo equilibrio grazie alle indicazioni fornite dalla SEC.

Alcuni interessanti chiarimenti provengono anche dalla Corte Distrettuale del Massachusetts, che in una recente ordinanza ha riconosciuto il potere della *Commodity Futures Trading Commission* (CFTC) di perseguire le condotte fraudolente commesse su valute virtuali[87]. Secondo il decidente la valuta My Big Coin (MBC) è da considerarsi una merce ai sensi del *Commodity Exchange Act*, poiché il termine "commodity" include ogni bene, prodotto o articolo deducibile in contratto per la consegna futura. Ne deriva la possibilità di applicare, a seconda dei casi, le disposizioni sugli strumenti finanziari (*securities*) o quelle sui derivati su merci (*commodities*) ovvero entrambe, in base alle caratteristiche del prodotto e alle modalità dell'offerta sul mercato.

Nell'ordinamento canadese lo stato dell'arte appare per molti versi simile rispetto a quello americano. Il Budget Implementation Act del 2017 ha, tra le altre cose, esteso le disposizioni antiriciclaggio agli operatori stranieri che offrono servizi e prodotti ad utenti residenti in Canada. Con specifico riferimento al commercio di valute virtuali, la normativa[88] ha equiparato gli *exchange* ai fornitori di servizi di pagamento sottoponendoli ai medesimi obblighi di collaborazione con l'autorità amministrativa. Le società che prestano servizi connessi all'utilizzo delle valute virtuali sono dunque tenute alla registrazione presso il Financial Transactions and Reports Analysis Centre del Canada (Fintrac), all'adozione di compliance *programs*, alla conservazione di documenti relativi alle operazioni dagli utenti, a fare rapporto delle transazioni sospette.

---

with the Commission or to qualify for an exemption from the registration requirements of the federal securities laws».

[85]Securities and Exchange Commission (SEC), *Plaintiff Securities and Exchange Commission for its complaint against Defendants REcoin Group Foundation*, DRC World, in https://sec.gov

[86] Securities and Exchange Commission (SEC), *Framework for "Investment Contract" Analysis of Digital Assets*, April 3, 2019, in https://www.sec.gov (cfr. *Supra*, § 1.4.).

[87] US Commodity Futures Trading Commission, *Court Denies Defendants' Motion to Dismiss in Commodity Fraud Case Involving the Virtual Currency My Big Coin*, October 3rd, 2018, Press Release n. 7820-18 https://www.cftc.gov

[88]D'ANGLEJAN-CHATILLON A. *et a*, *The Virtual Currency Regulation Review – Canada*, novembre 2018, in https://thelawreviews.co.uk

La regolazione dei mercati finanziari è una delle materie attribuite alla giurisdizione locale. Benché ogni provincia abbia adottato una propria disciplina, il quadro normativo sui valori mobiliari e sulle attività di vigilanza risulta in gran parte armonizzato a livello federale grazie al coordinamento effettuato dal *Canadian Securities Administrators*. Di recente il CSA ha pubblicato due circolari aventi ad oggetto i profili finanziari delle valute virtuali [89], nei quali sono contenuti importanti chiarimenti sull'applicabilità della *securities laws* ai valori virtuali. In sintesi la Commissione ritiene che questi debbano essere soggette a tali leggi nella misura in cui soddisfino i requisiti di uno strumento o un derivato finanziario, come definiti dal Securities Act e dalla tradizione giurisprudenziale affermatasi a partire dal *leading case* Pacific Coast Coin Exchange v. Ontario[90].

L'applicazione del "Pacific Coin test" ai prodotti virtuali risulta però nient'affatto semplice a causa della natura ibrida che li caratterizza. Non a caso la CSA richiama l'esempio degli *utility token* che attribuiscono al titolare il diritto di acquistare (o fruire di) prodotti o servizi, tentando di chiarire a che condizioni possano applicarsi le normative provinciali. Pur ammettendo la possibilità che alcuni valori siano classificati come *token* di utilità, la Commissione osserva come la maggior parte delle offerte di token fino ad ora esaminate virtuali sottintenda in realtà un contratto di investimento di natura finanziaria[91]. Così ragionando, l'avvenuta classificazione di un valore tra gli *utility token* non esime l'interprete dal valutare la causa contrattuale del negozio sottostante; la CSA ha infatti precisato che si dovrà guardare alla sostanza dell'operazione economica e non la sua forma esteriore. Al riguardo viene fornita una lista di possibili indici rivelatori della natura finanziaria del contratto di acquisto o vendita di valute virtuali[92], tra cui il fatto che: la tecnologia o la piattaforma *blockchain* sottostante non sia stata completamente sviluppata; il *token* venga immediatamente consegnato a ciascun acquirente; lo scopo dell'offerta sia quello di raccogliere capitali, che saranno utilizzati per l'esercizio dell'attività dell'emittente; la società abbia mantenuto per sé un numero significativo di *token* senza collocarli sul mercato; il numero di unità vendute è molto maggiore della quantità che ciascun utente potrà utilizzare sulla piattaforma; gli organi gestionali abbiano reso dichiarazioni o compiuto atti dai quali di evinca un suggerimento o una proposta sul futuro aumento del valore dei token; il token non abbia un valore fisso sulla piattaforma; il numero di token

[89] *Staff Notice* 46-307 e *Staff Notice* 46-308 sull'applicabilità delle disposizioni concernenti i valori mobiliari per le offerte di *token* I provvedimenti, adottati il 24 agosto 2017 descrivono *«how securities law requirements may apply to initial coin offerings (ICOs), initial token offerings (ITOs), cryptocurrency investment funds and the cryptocurrency exchanges trading these product».*

[90] Canada Supreme Court, *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, 1978, 2, S.C.R. 112. In esso la Corte Suprema del Canada ha identificato gli attributi fondamentali di un contratto di investimento, che valgono a qualificare un titolo come strumento finanziario: un investimento di denaro in una impresa comune con l'aspettativa di profitto che derivi in misura significativa dagli sforzi altrui. Se un contratto soddisfa il Pacific Coin test allora sarà considerato una *security* finanziaria e sottoposto alle leggi canadesi in materia.

[91] Canadian Securities Administrators, Staff Notice 46-307 – Cryptocurrency Offerings (2017), 40 ss.

[92] Canadian Securities Administrators, Staff Notice 46-307, ibidem

emesso sia finito o esista una ragionevole aspettative che le nuove emissioni saranno estremamente limitate; il *token* possa essere venduto su una piattaforma di *trading* o negoziato in mercato secondario.

Ogni offerta di valori virtuali che soddisfi i criteri della *Pacific Coast* e presenti le caratteristiche descritte nelle linee guida della CSA sarà verosimilmente soggetto alle disposizioni provinciali in materia di valori mobiliari. Per quanto apprezzabile sia lo sforzo della Commissione di fornire degli indici sintomatici, ci sia consentito esprimere qualche perplessità sulla eccessiva ampiezza dei parametri-guida appena elencati, che rende di fatto arduo ipotizzare una offerta di *token* che non presenti almeno uno dei suddetti elementi[93].

2.1.2. La legislazione giapponese.

Il mercato giapponese delle criptovalute ha avuto una crescita esponenziale nel 2017 di pari passo con l'aumento del prezzo di Bitcoin e il crescente entusiasmo per le ICO. Il Giappone rappresenta uno dei più grandi poli economici della *blockchain* a livello globale: non solo è stato il primo paese a stabilire un quadro normativo organico in materia, ma in più occasioni ha incoraggiato la crescita continua e sostenibile del mercato delle criptovalute [94].

Nell'aprile del 2017 il legislatore del Sol Levante ha modificato il *Payment Services Act* (PSA) per includere le criptovalute tra gli strumenti legali di pagamento[95]. La nuova normativa disciplina in modo dettagliato i requisiti per la registrazione dei cambiavalute virtuali, prevedendo anche *protection requirements* e obblighi informativi a tutela degli utilizzatori in condizioni non discriminatorie rispetto agli altri istituti di pagamento. Inoltre vengono disciplinati obblighi di *compliance* per prevenire l'utilizzo delle valute virtuali a scopo di riciclaggio e forme di vigilanza e controllo sul rispetto delle procedure interne. L'ambito oggettivo di operatività della nuova disciplina abbraccia tutti gli operatori che intendano offrire servizi relativi all'utilizzo di valute virtuali a soggetti residenti in Giappone. Di conseguenza, la normativa avrà effetto anche nei confronti dei *providers* stranieri che intendano operare sul mercato giapponese.

Le statistiche diffuse dall'Agenzia dei servizi finanziari giapponese a sei mesi dall'entrata in vigore della legge appaiono estremamente positive. Il Governo ha concesso sedici licenze ufficiali ai prestatori di servizi di *exchange* che ne hanno fatto

[93] Le autorità provinciali conserveranno pertanto piena discrezionalità nel valutare, secondo un criterio di preponderanza, se gli indici in concreto riscontrati siano sufficienti o meno a superare il "test" proposto dalla CSA.

[94] Cfr. KAWAI K., NAGASE T., *The Virtual Currency Regulation Review – Japan,* novembre 2018, in https://thelawreviews.co.uk

[95] Il lungo dibattito sulla regolazione del mercato valutario virtuale è stato acceso dal crollo del colosso giapponese del *trading* di valuta virtuale, Mt. Gox, che chiuse i battenti all'inizio del 2014 a causa delle accuse di frode e delle perdite causate da numerosi attacchi informatici.

richiesta, e emanato i primi regolamenti di attuazione della normativa sulla circolazione delle valute virtuali[96].

La disciplina applicabile alle valute virtuali varia in base alle caratteristiche delle stesse; le disposizioni finora adottate non affrontano direttamente la questione relativa all'applicabilità della normativa sugli strumenti finanziari. Se l'unità virtuale funge da mezzo di pagamento e rientra nella nozione di valuta virtuale, si applicheranno le disposizioni sulla autorizzazione e sui requisiti tecnici e organizzativi dell'intermediario.

Il *Financial Instruments and Exchange Act* (FIEA) troverà indubbiamente applicazione qualora la valuta virtuale rappresenti una partecipazione azionaria in un fondo di investimento e siano corrisposti utili legati ai profitti dell'andamento economico della società[97]. In tal caso l'offerta di *token* deve essere condotta da un intermediario abilitato all'esercizio dell'attività, a meno che l'offerta non costituisca un collocamento privato nei confronti di un investitore istituzionale in possesso di determinati requisiti[98].

Rimane tuttavia il dubbio se l'emittente di *token* d'investimento sia sottoposto a entrambi gli obblighi di registrazione oppure se il regime previsto dal *Payment Service Act* debba prevalere per specialità sulla normativa finanziaria.

Dando infine uno sguardo alle disposizioni penali, sono applicabili ai fornitori di servizi di cambio valuta virtuale le fattispecie di abusivismo previste dal PSA. L'esercizio delle attività di cambiavalute senza registrazione o sotto falso nome è punito con la reclusione non superiore a tre anni e con la multa fino a 3 milioni di yen. La violazione dell'obbligo di separazione patrimoniale dei fondi degli utenti da quelli della società e l'inosservanza dell'ordine di sospensione del servizio con la pena detentiva fino a due anni e con la multa, anche in questo caso, non superiore ai 3 milioni di yen. La stessa pena pecuniaria, oltre la reclusione fino ad un anno, si applica alle violazioni in materia di informazioni obbligatorie al pubblico in caso di operazioni straordinarie sulla società, a quelle sulla corretta tenuta delle scritture contabili e sugli ordini di esibizione e sulla collaborazione in caso di ispezioni[99].

2.1.3. L'esperienza svizzera. Rinvio.

La Svizzera ha ospitato negli ultimi anni una significativa parte dei progetti *blockchain* più importanti a livello globale. Sebbene la legge elvetica sui mercati finanziari non regoli l'emissione, lo scambio e l'offerta al pubblico delle valute virtuali,

[96] D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta*, cit., 19 ss.
[97] KAWAI, NAGASE, *The Virtual Currency Regulation Review – Japan*, cit., § II. Per contro, i *token* che non presentino tali caratteristiche non potrebbero considerarsi strumenti finanziari ai sensi della citata normativa
[98] Secondo la dottrina da ultimo citata fino ad oggi non ci sono stati in Giappone casi di offerte di *equity token* che potessero porre il dubbio sulla violazione della normativa sugli strumenti finanziari.
[99] Artt. 107 e seguenti del PSA giapponese Act No. 59 of June 24, 2009, testo disponibile in lingua inglese su http://www.japaneselawtranslation.go.jp

l'Autorità di vigilanza (FINMA) ha chiarito che, a seconda del modello di *business* prescelto, potrebbe essere necessaria una specifica autorizzazione e l'osservanza delle disposizioni a tutela dell'investitore.

Una circolare del 2016 ha dettato una disciplina specifica sulle modalità per l'identificazione degli utenti di servizi finanziari tramite canali digitali, la cui osservanza rende l'intermediario finanziario *compliant* con le disposizioni antiriciclaggio; il tema è stato già affrontato *funditus* in precedenza.[100].

Nella citata comunicazione del 16 febbraio 2018 l'autorità ha fornito agli operatori una guida pratica[101] con l'obiettivo di prevenire il riciclaggio e proteggere l'investitori dai rischi derivanti dall'investimento in valute virtuali. Il documento muove dalla premessa che, a seconda di come sono strutturate *«alcune ICO possono comportare investimenti regolamentati e le imprese coinvolte in una ICO possono condurre attività regolamentate»*. Alcune di esse presentano forti analogie con le offerte pubbliche di strumenti finanziari quali il collocamento privato di titoli, il *crowdfunding* o persino gli schemi di investimento collettivo; vi è inoltre margine per ritenere che, a determinate condizioni, i *token* rappresentino valori mobiliari da sottoporre alla disciplina in materia di prospetto.

La tassonomia tripartita a cui si ispira la FINMA è probabilmente quella più conosciuta dagli operatori del settore. I token di pagamento (*payment token*), sono considerati quali semplici criptovalute, utilizzate come mezzo solutorio tra le parti, non qualificati come valori mobiliari e assoggettati alla disciplina antiriciclaggio. Gli *utility token* attribuiscono al titolare l'accesso a un'applicazione o a un servizio digitale; qualora si individui in essi una causa finanziaria il regime giuridico applicabile sarà quello dei valori mobiliari. Infine, i token di investimento (*security token*) rappresentano quote di valori reali, aziende, ricavi o il diritto ai dividendi o al pagamento di interessi, e altri prodotti scambiati sui mercati finanziari, sono qualificati come valori mobiliari *«se sono standardizzati e idonei a essere negoziati su vasta scala»*. Alla medesima categoria appartengono quelli assimilabili ai derivati finanziari, quando il valore del credito trasferito dipende da un valore dal valore reale sottostante.

Trattandosi di una materia regolata dal diritto dei mercati finanziari, le ICO di valori appartenenti a quest'ultima categoria dovranno garantire il pieno rispetto degli obblighi in materia di autorizzazione preventiva e di prospetto informativo. L'autorità è però ben consapevole dell'impossibilità di racchiudere il fenomeno entro uno schema rigido, tanto da affermare che le questioni giuridiche relative alle forme "miste" saranno risolte caso per caso in base alla funzione economica e alle finalità dei *token*.

Il documento fornisce, infine, un elenco delle informazioni che i promotori delle offerte dovranno fornire all'Autorità, riguardanti il progetto in generale, la

[100] Per approfondimenti sulla normativa svizzera di contrasto al riciclaggio di rinvia al Cap. III, § 3.7.
[101] *Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offering* (ICO), 16 febbraio 2018, in https://finma.ch

strutturazione e l'emissione dei token nonché le possibilità di un loro commercio secondario[102], affinché la stessa possa pronunciarsi sul regime giuridico applicabile.

La vigilanza sul mercato *fintech* contribuisce a rendere il sistema finanziario virtuale più credibile e sicuro. Da questa prospettiva è comprensibile che la FINMA abbia inteso avocare a sé la funzione di controllo; non si comprende tuttavia la ragione per cui il legislatore non abbia fornito una base normativa per l'intervento dell'autorità. Fatto sta che, nel sistema attuale, gli strumenti di *soft law* e la prassi amministrativa hanno assunto un ruolo centrale, sostituendosi di fatto alla legislazione federale.

2.1.4. La normativa di Malta e di San Marino.

La legislazione più matura a livello europeo è indubbiamente quella maltese. Nel luglio del 2018 il parlamento ha approvato tre provvedimenti di notevole importanza per la materia che ci occupa[103].

Il Digital Innovation Authority Act[104] ha istituito la Malta Digital Innovation Authority, un ente pubblico finalizzato a promuovere l'innovazione e lo sviluppo tecnologici e a garantire la tutela degli utenti e dei consumatori. L'Autorità avrà il compito di autorizzare l'esercizio di determinate attività e fornire certificazioni per servizi e prodotti al fine di garantire la sicurezza nella commercializzazione di prodotti o a distanza; a tal fine le sono attribuiti poteri di vigilanza sugli operatori del mercato che prestano servizi a contenuto tecnologico.

Con l'Innovative Technology Arrangements and Service Act[105] vengono disciplinati alcuni specifici profili concernenti la certificazione di tecnologie DLT e la registrazione dei service provider nel territorio maltese

Le disposizioni più rilevanti sono contenute nel Virtual Financial Assets Act (VFA)[106] che regola in modo puntuale l'emissione e l'offerta al pubblico di valori virtuali. La redazione di un prospetto (*white paper*) è indicata tra i requisiti obbligatori per assicurare agli investitori una corretta informazione sulle caratteristiche del prodotto e sulle specifiche del progetto[107], tant'è che l'art. 10, par. 1, prevede che l'emittente sia direttamente responsabile per i danni cagionati agli investitori, nel caso in cui le informazioni fornite nel *white paper* risultino imprecise, false, o fuorvianti.

---

[102] *Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offering* (ICO), cit., Allegato: informazioni minime per richieste inerenti all'assoggettamento, 8 ss.
[103] I tre atti legislativi sono stati adottati in esecuzione della *National Blockchain Strategy* approvata nell'aprile del 2017 con lo scopo di promuovere lo sviluppo della cripto-economia all'interno del Paese.
[104] Bill n. 45/2018, in https://parlament.mt
[105] Bill n. 43/2018, ibidem
[106] Bill n. 44/2018, ibidem
[107] Affinché sia valido, il *whitepaper* deve contenere le informazioni previste dall'Allegato e recare in calce una dichiarazione formale con la quale l'amministrazione della società si assume la responsabilità della conformità delle dichiarazioni ai requisiti sostanziali previsti dalla legge.

Il provvedimento impone anche la nomina di un responsabile (VFA Agent) con funzioni generali di controllo sul rispetto delle prescrizioni normative, incaricato alla collaborazione con le autorità giudiziarie e amministrative (art. 7).

La sostanziale assimilazione operata dal legislatore maltese tra i *token* e gli strumenti finanziari emerge piuttosto chiaramente anche dalla previsione di sanzioni penali molto severe per le condotte di *market abuse* commesse su valori virtuali. Dal combinato disposto degli artt. 34 ss., 53 e 54 VFA Act si ricava che per le ipotesi più gravi è comminata la pena della multa fino a 15 milioni di euro o fino a tre volte il profitto conseguito, o la reclusione fino a sei anni, da applicare anche congiuntamente alla sanzione pecuniaria[108]. Non può che accogliersi con favore la scelta di presidiare (anche) penalmente il mercato finanziario virtuale contestualmente al suo riconoscimento normativo. D'altronde la presa di posizione del legislatore non lascia dubbi sul fatto che nell'ordinamento maltese quello degli *asset* virtuali sia ormai, a tutti gli effetti, un mercato regolamentato; di qui la necessità di approntare una tutela simmetrica rispetto alle tradizionali sedi di scambio.

Da ultimo, nel luglio del 2018 la Financial Market Authority maltese ha pubblicato le linee guida ai sensi dell'art. 47 VFA relative alla qualificazione degli *asset* DLT come strumento finanziario[109]. Più precisamente, esse forniscono una *checklist* che gli operatori interessati potranno compilare per ottenere una valutazione sulla qualificazione dei valori virtuali (emessi o di futura emissione) come moneta elettronica, strumento finanziario o utilità meramente virtuale. Nel redigere le *guidelines* l'Autorità ha adottato un approccio di tipo funzionale, individuando alcuni indici sintomatici dell'appartenenza del valore all'una piuttosto che all'altra categoria. Per non eccedere la nozione di *virtual token*, l'*asset* dovrebbe essere scambiato soltanto all'interno della piattaforma DLT e utilizzato esclusivamente per acquisto di beni o servizi, senza poter essere scambiato per altra valuta virtuale.

Saranno invece qualificabili come strumenti finanziari (*security*) i *token* negoziati su un mercato di titoli oppure concepiti per essere scambiati o trasferiti in una sede di negoziazione. Ai fini dell'inclusione in questa categoria è necessario che i diritti incorporati nel titolo siano effettivamente simili o rappresentino quote di partecipazione a società, azioni, ricevute di deposito, obbligazioni o altre forme di debito cartolarizzato o che diano il diritto di acquisire o vendere strumenti finanziari[110].

---

[108] Così dispone l'art. 54 VFA: *«A person guilty of an offence under the provisions of article 53 shall be liable on conviction to a fine (multa) of up to fifteen million euro (€15,000,000) or up to three times the profits made or losses avoided by virtue of the offence, whichever is the greater, or to imprisonment for a term not exceeding six years, or both such fine and imprisonment, unless such fine or term of imprisonment is otherwise imposed under article 38»*.

[109] Malta Financial Market Authority, *Guidance note to the Financial Instrument Test*, in https://www.mfsa.com.mt

[110] *Guidance note to the Financial Instrument Test*, cit., 13 ss. Vengono individuati sostanzialmente quattro criteri distintivi: un periodo di rimborsabilità superiore a 397 giorni; il fatto che non sia qualificabile come uno strumento di pagamento; la negoziabilità sul mercato dei capitali e la rappresentazione di almeno uno o più diritti connessi ai titoli trasferibili. Nel caso in cui il valore presenti determinate caratteristiche può essere inquadrato tra i contratti derivati di cui alla Sezione C dell'allegato 1 alla Direttiva MiFID. A tal fine gli emittenti dovrebbero valutare anzitutto se la tipologia contrattuale

Dopo qualche mese dall'entrata in vigore della normativa, la Financial Services Authority maltese ha accreditato le prime agenzie operanti nel settore valutario virtuale e concesso decine di licenze per l'esercizio dell'attività di cambiavalute virtuali. Benché i tempi siano prematuri per esprimere un giudizio sul raggiungimento degli obiettivi fissati nella National Blockchain Strategy, alla normativa maltese va riconosciuto il merito di avere attuato un razionale bilanciamento di interessi tra libertà d'impresa, certezza del diritto e tutela del risparmio. Il legislatore ha disciplinato in modo puntuale e organico i requisiti, le procedure e i controlli per l'emissione di valori virtuali, opportunamente integrando le disposizioni di *hard law* con strumenti di regolazione flessibile. L'approccio "di stampo anglosassone" risulta particolarmente pregevole per la possibilità di valutare le caratteristiche del prodotto virtuale attraverso la compilazione del VFA test sopra richiamato. Evidenti sono i vantaggi per gli operatori economici che possono contare su assetto di regole chiaro e su procedure amministrative snelle per l'esercizio dell'attività. Un modello che, a nostro avviso, dovrebbe servire da esempio al legislatore italiano.

In tempi più recenti anche la Repubblica di San Marino ha disciplinato alcuni profili finanziari della tecnologia a registro distribuito, con il dichiarato intento di creare le premesse per un quadro normativo chiaro ed efficace e di attrarre l'interesse degli investitori stranieri. Il Decreto Delegato 27 febbraio 2019 n. 37 si applica alle società e altri enti dotati di autonoma personalità giuridica che si avvalgano di sistemi *blockchain,* e che siano residenti nella Repubblica di San Marino o in un Paese membro dell'Unione Europea[111].

Nel decreto si distinguono due diverse tipologie di *token,* di investimento e di utilizzo[112], secondo una classificazione che riecheggia quella della FINMA svizzera[113].

---

sia assimilabile a un'opzione o a un prodotto come *futures* o *swap*, e se il sottostante rientra nell'ambito di applicazione della direttiva.

[111]Qualora questi soggetti intendano ottenere il riconoscimento ai fini dell'applicazione della normativa, dovranno presentare una apposita istanza secondo le modalità che verranno stabilite dall'Istituto per l'Innovazione della Repubblica di San Marino S.p.A. (ovvero San Marino Innovation) di cui al Decreto Delegato 7 marzo 2018 n. 23 e successive modifiche.

La richiesta di riconoscimento dovrà contenere le informazioni e/o documenti previsti dal decreto delegato; il riconoscimento verrà rilasciato dall'Istituto, entro e non oltre 20 giorni lavorativi dal ricevimento della richiesta. Al termine della procedura, l'Istituto rilascerà il codice di riferimento necessario per l'iscrizione nel registro pubblico all'interno del quale sono indicati i soggetti che si avvalgono di sistemi *blockchain.*

[112] Ai sensi dell'art. 8 del decreto delegato i *token* di utilizzo sono da qualificarsi come voucher per l'acquisto di servizi o di beni offerti dall'Ente Blockchain. Essi non attribuiscono nessun diritto ai loro portatori al di fuori della piattaforma e non hanno finalità monetaria, speculativa o partecipativa; non danno diritto al rimborso del capitale, alla corresponsione di interessi né alla distribuzione di utili e/o dividendi e non conferiscono alcun diritto quale azionista, obbligazionista o portatore di altro strumento finanziario; non sono a nessun titolo considerati valori mobiliari, strumenti finanziari e/o prodotti finanziari, né moneta elettronica e/o mezzo di pagamento fuori dalla Blockchain in cui sono stati generati; la loro emissione non obbliga a redigere un prospetto e non soggiace alle norme applicabili al mercato dei capitali e alle offerte pubbliche di prodotti finanziari.

[113] *Amplius*, § 1.4 e *supra*, § 2.1.3. La distinzione principale tra le due tipologie di token risiede nel fatto che i *token* di investimento (nel lessico comune, *security token*) sono *asset* digitali che rappresentano uno strumento sottostante come le azioni dell'emittente, strumenti finanziari partecipativi o titoli di debito (art. 9).

L'offerta iniziale di valori virtuali è definita come il momento in cui un ente *blockchain* – cioè il soggetto che ha ottenuto il riconoscimento da parte l'Istituto per l'Innovazione ed iscritto in un apposito registro[114] – emette strumenti digitali consentendo agli utenti di acquistarli sul mercato di scambio o presso una piattaforma dedicata. In questa prima fase esiste un preciso obbligo di *disclosure* di alcune informazioni rilevanti oltre a oneri di pubblicità relativa all'offerta. L'emittente dovrà redigere un *whitepaper* contenente una serie di informazioni relative al progetto imprenditoriale, al prodotto offerto e alle caratteristiche della *blockchain* utilizzata.

Analogamente alla normativa maltese, viene espressamente sancita la responsabilità dell'emittente in caso di danni subiti da investitori o utenti come conseguenza della falsità delle dichiarazioni rilasciate nel *whitepaper* o di omissione dei doveri informativi prescritti dalla legge. Per una compiuta informazione sui rischi si dovrà redigere anche una nota di sintesi, nella quale sono indicate in un linguaggio semplice ad accessibile tutte le informazioni utili affinché l'investitore possa comprendere le caratteristiche fondamentali dei *token* oggetto dell'offerta[115].

Nella successiva fase di negoziazione l'Istituto per l'Innovazione della Repubblica potrà condizionare lo scambio a una serie di misure rafforzate a tutela dell'utente e del mercato, richiedendo se del caso una integrazione delle informazioni fornite dall'emittente, al fine di preservare la trasparenza e la fiducia nel mercato.

2.2. Verso un modello di regolazione flessibile? Il punto di vista della Consob sull'emissione e lo scambio di criptoattività.

Il legislatore italiano ha sinora mostrato disinteresse per la regolazione finanziaria del mercato valutario virtuale, lasciando alle autorità di settore il gravoso compito di trovare un bilanciamento tra i contrapposti interessi.

Dopo aver affrontato diversi casi di offerta al pubblico di valori virtuali, risolti per lo più con lo strumento della inibitoria *ex* art. 101 TUF, la Commissione nazionale per le società e la borsa, traendo ispirazione dal *discussion paper* redatto dall'AMF francese, ha recentemente pubblicato un documento relativo all'avvio di una procedura di consultazione pubblica per regolare le offerte iniziali e lo scambio di cripto-attività con cui, dopo aver abbozzato i lineamenti della futura disciplina, chiede agli interessati di prendere posizione (o esprimere un parere) su 15 quesiti relativi all'opportunità e all'impatto della proposta di regolazione entro il 5 giugno 2019[116].

---

[114] Art. 1, comma 1, lett. *n.*, del decreto delegato n. 37/2019

[115] L'investitore deve essere messo nelle condizioni di valutare in autonomia i rischi associati all'acquisto dei prodotti e di comprendere se l'offerta abbia ad oggetto *token* di investimento o di utilizzo. La pubblicità relativa all'offerta di *token* deve essere chiaramente identificabile e contenere informazioni accurate e non ingannevoli. Il decreto delegato prevede poi che gli enti *blockchain* debbano improntare la propria attività a correttezza e buona fede, comunicando con gli investitori in modo chiaro e preciso e promuovendo i prodotti in modo prudente e diligente (art. 10, comma 6).

[116] *Le offerte iniziali e gli scambi di cripto-attività*, Documento per la Discussione, 19 marzo 2019, in https://consob.it. L'autorità ha inteso avviare un dialogo attivo tra l'Autorità e gli esponenti del settore

Il Documento per la discussione si apre con una sintetica rappresentazione del fenomeno di diffusione delle ICOs e dei connessi aspetti di interesse per l'attività istituzionale della Consob. Nel descrivere le caratteristiche dell'*Initial Coin Offering* l'Autorità individua subito possibili analogie rispetto all'offerta pubblica di strumenti finanziari, che possono essere riassunte nei termini seguenti.

L'obiettivo della creazione dei valori virtuali è rappresentato dall'esigenza di raccogliere fondi per il finanziamento di un'attività o di un progetto; a tal fine si utilizza l'espediente dell'incorporazione di un diritto del sottoscrittore in un *quid* di immateriale, che costituisce titolo di legittimazione per il loro esercizio, oltre che strumento per la più agevole trasferibilità dei diritti. I *token*, come gli strumenti finanziari, sono destinati allo scambio in mercati dedicati, al fine di realizzare plusvalenze di investimento; il prezzo non è sempre legato all'andamento dell'impresa finanziata, ma determinato dal meccanismo della domanda e dell'offerta sul circuito di scambio.

Esistono tuttavia anche notevoli differenze: l'utilizzo della tecnologia *blockchain* permette di disintermediare le infrastrutture tipiche dei mercati dei capitali, mentre il regolamento dei flussi finanziari avviene in valuta virtuale anziché in moneta avente corso legale; la pubblicità e la promozione dei valori si realizzano tramite *world wide web*, che consente la raccolta su base transfrontaliera, senza alcun vincolo territoriale. L'offerta al pubblico dei valori si attua mediante la pubblicazione di un *white paper* in luogo di un prospetto, nel quale vengono riportate le principali caratteristiche dell'operazione e dell'oggetto dell'offerta.

Dopo aver ripercorso brevemente lo stato dell'arte a livello europeo, la Consob si concentra sugli aspetti definitori partendo dalla nozione di prodotto finanziario[117]. I *token* potrebbero, in linea di principio, dar luogo anche a "rendimenti" di natura non finanziaria difettando, ad esempio, il requisito dell'accrescimento della disponibilità investita. Il ritorno economico dell'investimento nei valori virtuali può, a seconda della natura delle c.d. "cripto-attività"[118], essere determinato dai ricavi dell'iniziativa imprenditoriale finanziata o dall'apprezzamento del valore dei *token* negoziati sulle piattaforme di scambio.

Venendo ai motivi dell'introduzione di una specifica nozione di cripto-attività, l'Autorità sostiene che la codificazione di una categoria *ad hoc* (distinta dai prodotti finanziari) abbia il pregio di alleviare l'onere di condurre un'analisi casistica circa la sussistenza (o meno) delle caratteristiche del prodotto finanziario, e di evitare che i

privato sul tema delle offerte iniziali e degli scambi di cripto-attività in relazione alla recente diffusione di operazioni cosiddette di *initial coin offerings* (ICOs). L'invito è rivolto a tutte le categorie di soggetti potenzialmente interessati, tra cui anche imprese, associazioni di categoria, studi professionali, esponenti del mondo accademico.

[117] Sulla quale v. *supra* § 1.2.1.

[118] Viene proposta una definizione dia rilevanza alle seguenti caratteristiche proprie delle "cripto-attività": (i) la natura di registrazioni digitali rappresentative di diritti connessi a investimenti in progetti imprenditoriali; (ii) la creazione, la conservazione e il trasferimento mediante tecnologie basate su registri distribuiti; (iii) la capacità di consentire l'identificazione del titolare dei diritti relativi agli investimenti sottostanti; (iv) la negoziazione dei valori all'interno di uno o più sistemi di scambi.

promotori dell'iniziativa che rispettino determinati requisiti vedano ricondotti i valori virtuali alla nozione di prodotto finanziario da cui deriverebbe l'applicazione della disciplina nazionale in materia di prospetto e offerta a distanza.

L'Autorità è tuttavia consapevole di muoversi su un terreno estremamente scivoloso poiché gli *«investimenti rientranti nella nuova categoria delle cripto-attività potrebbero integrare anche gli elementi definitori del prodotto finanziario (di cui all'articolo 1, comma 1, lett. u), del TUF), in quanto comunque caratterizzati dall'investimento di un capitale finanziario, dall'assunzione del relativo rischio e da un'aspettativa di rendimento»* e pertanto *«le relative attività di emissione, negoziazione e post-negoziazione sono evidentemente soggette alle disposizioni europee di armonizzazione previste per gli strumenti finanziari e per i prodotti di investimento, in quanto sovraordinate nella gerarchia delle fonti»*[119].

Essendo la disciplina del fenomeno funzionale alla tutela degli investitori, si dovranno stabilire le caratteristiche dei soggetti emittenti e introdurre precisi oneri di informazione in merito ai progetti imprenditoriali per i quali la raccolta di fondi viene sollecitata. Per questo l'Autorità propone di individuare il luogo deputato allo svolgimento delle ICOs come una piattaforma per le offerte di cripto-attività, vale a dire *«una piattaforma on line che abbia come finalità esclusiva la promozione e realizzazione di offerte di cripto-attività di nuova emissione»*, da attribuire ai gestori di portali per la raccolta di capitali di rischio autorizzati ai sensi dell'art. 50-*quinquies* del TUF[120], senza tuttavia escludere la possibilità di autorizzare soggetti diversi che siano in possesso di requisiti soggettivi richiesti per i gestori di portali di *crowdfunding* al fine di non precludere lo sviluppo di nuovi modelli di *business*[121]. Le piattaforme e i relativi gestori saranno sottoposti alla vigilanza della Consob, che potrà esperire su di essi tutti i poteri di vigilanza e ispezione riconosciutigli dalla normativa di settore.

In ogni caso, la materia andrà regolata in modo flessibile mediante un meccanismo di *opt-in* che consenta al promotore dell'iniziativa di scegliere liberamente l'impiego di una piattaforma dedicata – al fine di rivolgersi alla platea degli investitori in un contesto regolamentato – ferma restando la piena legittimità delle offerte promosse al di fuori delle piattaforme regolate. Si prevede, tuttavia, un incentivo all'accesso al circuito regolamentato per le offerte di cripto-attività che siano idonee a integrare la nozione domestica di prodotto finanziario, alle quali sarà riconosciuta una deroga rispetto all'applicazione della disciplina dell'offerta al pubblico e dell'offerta a distanza di prodotti finanziari[122].

---

[119] *Le offerte iniziali e gli scambi di cripto-attività,* cit., 7

[120] L'attività dei gestori di portali di *crowdfunding* è disciplinata con il regolamento Consob n. 18592 del 26 giugno 2013 (c.d. Regolamento Crowdfunding).

[121] La normativa di futura emanazione dovrà prevedere le caratteristiche che i soggetti interessati all'emissione e/o i progetti debbono possedere per la promozione delle offerte sulle piattaforme, con norme di dettaglio sui presidi per la selezione dei progetti imprenditoriali meritevoli di accedere alla piattaforma, sull'assolvimento degli obblighi di adeguata informazione, e sulla continuità operativa e sulla sicurezza informatica della piattaforma per le offerte.

[122] Ciononostante l'Autorità ribadisce come le offerte condotte sulle piattaforme il cui oggetto integri le caratteristiche degli strumenti finanziari comporterà l'applicazione della normativa MiFID, con

Nell'ultima sezione del documento la Consob affronta le questioni relative allo scambio (*trading*) di cripto attività, ricordando come il modello operativo attualmente dominante sia costituito dalle c.d. piattaforme centralizzate, che operano sia come piattaforma di *trading* che come fornitore del servizio di *wallet*. Allo stato attuale, la gestione e il funzionamento degli *exchange* di valori virtuali non inquadrabili come strumenti finanziari non sono soggetti ad alcuna riserva di attività ai sensi di MiFID II, né alla relativa disciplina. Per questo motivo l'Autorità propone di codificare la nozione di sistema di scambi di cripto-attività quale *«insieme di regole e di strutture automatizzate, che consente di raccogliere e diffondere proposte di negoziazione di cripto-attività e di dare esecuzione a dette proposte, anche attraverso tecnologie basate su registri distribuiti»*, a fondamento di una disciplina che preveda parametri minimi di *governance* e operatività per le piattaforme, individuando un incentivo all'*opt in* che potrebbe essere costituito dall'esistenza di uno stretto collegamento con le offerte iniziali che siano state condotte per il tramite di piattaforme dedicate e regolamentate (doppio regime di *opt-in*)[123]. Anche gli intermediari del *trading* sarebbero sottoposti alla vigilanza da parte della Consob nell'ottica di tutelare l'ordinato svolgimento degli scambi. A tal fine si prevede che i sistemi di scambio in parola siano dotati di regole e procedure idonee per l'accesso e l'identificazione dei partecipanti in modo tale da rendere inutilizzabili le tecnologie basate su registri distribuiti nella forma c.d. *permissionless* per gli aspetti relativi alla gestione dei processi di scambio e di trasferimento delle cripto-attività sul registro medesimo.

2.2.1. Rilievi critici.

L'apertura di un dialogo sulla regolazione delle ICO e sul *trading* valutario virtuale rappresenta un coraggioso tentativo da parte della Consob di porre al centro del dibattito un tema di grande importanza, finora sfuggito all'attenzione del legislatore.

Pur condividendosi l'approccio seguito nel documento, vi sono alcuni aspetti che, a nostro avviso, andrebbero valutati con maggiore attenzione[124]. Anzitutto, la definizione di cripto-attività andrebbe circoscritta ai soli valori concepiti *ab origine* per essere negoziati su un sistema di scambi e quelli aventi come scopo principale il finanziamento di progetti imprenditoriali. Gli elementi definitori della rappresentazione di diritti connessi a investimenti in progetti imprenditoriali e della negoziazione dei valori all'interno di uno o più sistemi di scambio portano infatti ad escludere dal campo di applicazione dell'emananda disciplina quei valori virtuali

conseguente applicazione delle sanzioni previste per l'abusivismo finanziario o per le violazioni in materia di offerta fuori sede e di prospetto. Cfr. *Le offerte iniziali e gli scambi di cripto-attività,* cit., 10.

[123] Sarebbero ammessi all'iscrizione nel registro degli intermediari i gestori delle sedi di negoziazione, i gestori di portali per la raccolta di capitali, i soggetti che gestiscono le piattaforme per le offerte di cripto-attività e ulteriori soggetti, che rispettano requisiti di carattere soggettivo e oggettivo stabiliti *ad hoc* dalla Consob.

[124] Le riflessioni contenute in questo paragrafo costituiscono una sintesi ragionata delle riflessioni presentate dallo scrivente a Consob nel corso della procedura di consultazione pubblica.

emessi a fine di rappresentare un determinato diritto di natura reale (comunemente definiti *asset token*) o obbligatoria (noti come *utility token*), senza che ciò implichi l'accesso a una forma di finanziamento[125]. Dovrebbe tracciarsi una netta linea di demarcazione tra il finanziamento dell'impresa mediante l'appello al pubblico risparmio (t*oken* di investimento, che rientrano nella nozione contenuta nel Documento) e l'utilizzo di *asset o utility token* in una o più fasi del processo produttivo: nel primo caso lo scopo finanziario dell'operazione è patente, e ciò giustifica l'intervento di Consob a tutela dell'investitore; nel secondo caso invece l'operazione trova fondamento nell'autonomia privata, e la tutela dell'investitore è sufficientemente garantita dalle disposizioni del D. Lgs. 06 settembre 2005 n. 206 (Codice del Consumo).

Si auspica pertanto che nella normativa di futura adozione sia inserito un elemento definitorio che escluda *per tabulas* dalla nozione di cripto-attività «le rappresentazioni digitali non destinate alla negoziazione in sistemi di scambi, emesse, cedute e scambiate nell'ambito del normale esercizio dell'impresa». In tal modo gli attori del mercato potrebbero contare sulla possibilità di sfruttare appieno le potenzialità della tecnologia a registro distribuito senza dover passare – sia pur nel quadro di un regime di *opt-in* – per l'offerta al pubblico di cripto-attività; la deroga sarebbe ben giustificata, tenuto conto delle marcate differenze tra una *Initial Coin Offering* e la semplice vendita di *token* rappresentativi di diritti.

Altrettanto dubbi i parametri discretivi tra le cripto-attività e gli strumenti finanziari. Pur nella consapevolezza delle enormi difficoltà classificatorie, sarebbe auspicabile che l'autorità fornisse un elenco degli indici rilevatori della rilevanza finanziaria del valore virtuale. Non mancano a tal fine modelli da cui trarre ispirazione, come il VFA maltese o le guidelines della SEC statunitense sopra esaminati. Anche la nozione di *prodotto finanziario* richiamata nel documento non chiarisce a che condizioni i *token* possano dar luogo a "rendimenti di natura finanziaria". Ciò introduce un margine di incertezza notevole, che potrebbe frustrare lo scopo ultimo della codificazione di una categoria di "cripto-attività" distinta dai prodotti finanziari[126].

Risulta inoltre condivisibile il proposito di non precludere la possibilità di autorizzare soggetti diversi che siano in possesso di requisiti soggettivi richiesti per i

[125] Sarebbe del resto poco avveduto considerare il *token* un mero strumento di raccolta del risparmio, omettendo di considerarne la natura di strumento per la circolazione dei diritti e di efficientamento degli scambi.

[126] La scarsa capacità selettiva della definizione di cripto-attività emerge piuttosto chiaramente dal *caveat* espresso a pagina 7 del Documento secondo cui gli «*investimenti rientranti nella nuova categoria delle cripto-attività potrebbero integrare anche gli elementi definitori del prodotto finanziario (di cui all'articolo 1, comma 1, lett. u), del TUF), in quanto comunque caratterizzati dall'investimento di un capitale finanziario, dall'assunzione del relativo rischio e da un'aspettativa di rendimento».* L'impossibilità di una *reductio ad unum* della categoria delle cripto-attività caratterizzata da una natura spesso ibrida, in cui il connotato finanziario non è spesso così marcato, porta a guardare con favore la scelta di prevedere una disciplina che non contempli soglie di valore per esenzioni o particolari presidi. Non sarebbe del congruo sottoporre l'offerta al pubblico di valori virtuali a particolari restrizioni sulla in un ipotetico parallelismo tra questi ultimi e gli strumenti/prodotti finanziari; si tratta di realtà connotate da profonde differenze e, come tali, è bene che siano sottoposti a differenti regimi giuridici.

gestori di portali di *crowdfunding,* aspetto che potrebbe favorire lo sviluppo di nuovi modelli di *business* tra coloro che operano o intendono operare esclusivamente sul mercato delle cripto-attività[127].

Il Documento non prende posizione sulla procedura di acquisto dei valori, aspetto che andrebbe chiarito per evitare fraintendimenti sulla disciplina applicabile. Come noto, i gestori dei portali *ex* art. 50-*quinquies* TUF non possono detenere somme di danaro di pertinenza degli investitori né eseguire direttamente gli ordini per la sottoscrizione degli strumenti offerti sui propri portali, dovendo a tal fine trasmetterli a istituti bancari o SIM. La stessa regola non potrebbe valere anche per l'acquisto di cripto-attività che di consueto avviene scambiando Bitcoin o altra valuta virtuale in cambio di *token* di nuova emissione[128].

Ciò posto, alla domanda se un assetto di disciplina facente leva sul meccanismo di *opt-in*, che consenta al promotore dell'iniziativa di scegliere liberamente l'impiego di una piattaforma dedicata, sia compatibile con l'esigenza di tutela degli investitori può darsi risposta affermativa. Si è ben consapevoli che un siffatto regime giuridico verrebbe adottato soltanto in via transitoria, in attesa di una più compiuta evoluzione del fenomeno, ma per il momento l'opzione minimalista, accompagna da incentivi all'*opt-in*, è sicuramente il modello di regolazione più prudente e meno invasivo per la crescita del mercato. Ci si sente tuttavia di dover mettere in evidenza, anche in vista della futura adozione di strumenti di *hard law*, la necessità di prevedere norme di dettaglio sulle informazioni da fornire in sede di promozione dell'offerta, con particolare riguardo ai livelli di rischio dell'investimento e alle modalità di esercizio dei diritti da parte del consumatore/investitore[129].

---

[127] La possibilità di improntare la disciplina dell'offerta di valori virtuali a quella del *crowdfunding* dipende dalla nozione di cripto-attività alla base della disciplina. Ove la definizione faccia riferimento unicamente ai *token* di investimento per il finanziamento dell'impresa mediante l'appello al pubblico risparmio vi sarebbero delle forti analogie con l'attività disciplinata dal regolamento Consob n. 18592 del 26 giugno 2013. Tanto la funzione economica dell'operazione, quanto lo scopo avuto di mira dalle parti sarebbero i medesimi, cioè quello di contribuire al finanziamento di un progetto imprenditoriale, circostanza che rende ragionevole la scelta di attribuirne la gestione ai soggetti all'uopo autorizzati. Ad ogni modo il parallelismo con l'*equity-based crowdfunding* potrebbe risultare fuorviante, poiché non sempre con l'investimento *on-line* si acquista un vero e proprio titolo di partecipazione in una società (con tanto di diritti patrimoniali e amministrativi che derivano dalla partecipazione all'impresa). Ciò suggerisce di mantenere distinti i due piani e soprattutto di procedere con una certa cautela nell'assoggettare le offerte di cripto-attività al medesimo regime giuridico previsto per il *crowdfunding*.

[128] Se si imponessero vincoli alla detenzione di somme per conto dei clienti si finirebbe per sofisticare l'*iter* di raccolta dei capitali, frustando le opportunità del binomio tokenizzazione-semplificazione. Sarebbe dunque preferibile un regime più "liberale" che consenta ai gestori delle piattaforme o direttamente agli emittenti di raccogliere il denaro da destinare al progetto imprenditoriale, senza il necessario passaggio per gli istituti di credito, specie laddove la raccolta non sia realizzata in valuta avente corso legale.

[129] Tra gli incentivi all'*opt-in* si prevede anche la deroga all'applicazione della disciplina dell'offerta al pubblico e dell'offerta a distanza di prodotti finanziari per le offerte di cripto-attività che siano idonee a integrare la nozione domestica di prodotto finanziario. A nostro modo di vedere, una simile deroga darebbe luogo a un formidabile incentivo per il ricorso alla ICO come forma di finanziamento per l'impresa. Una strada da percorrere fino in fondo, che potrebbe rivelarsi vincente se accompagnata dalla previsione di procedure di interpello finalizzate a ottenere una valutazione preventiva sulla qualificazione giuridica dell'operazione. In un quadro normativo così laconico ed evanescente, sarebbe

Per quanto riguarda, infine, il *trading* di valori virtuali ci pare condivisibile la proposta di ammettere all'iscrizione i soli soggetti in possesso di determinati requisiti. La futura regolazione dovrà insistere, in particolare, su due elementi: gli obblighi informativi e la sicurezza informatica. Quanto ai primi, si dovrebbero predeterminare le modalità con cui le informazioni rilevanti sulle varie tipologie di cripto-attività debbono essere fornite agli investitori[130].

L'incentivo all'*opt-in* costituito dall'esistenza di uno stretto collegamento con le offerte iniziali che siano state condotte per il tramite di piattaforme dedicate e regolamentate (doppio regime di *opt-in*) è suggestivo, ma dovrebbe essere accompagnato dalla previsione di un adeguate misure per non pretermettere gli emittenti che abbiano fatto ricorso ad altri canali per l'offerta al pubblico delle cripto-attività. Si ritiene infatti che il successo del modello proposto dipenderà per larga misura – *a fortiori* nella fase iniziale – dal numero di valori offerti e scambiati sulle piattaforme regolamentate; la previsione di requisiti troppo stringenti, specialmente in relazione all'accesso ai sistemi di scambio, potrebbe risultare controproducente, e porsi in contrasto con gli obiettivi presi di mira da Consob.

Una riflessione finale va fatta in merito all'inutilizzabilità delle tecnologie basate su registri distribuiti nella forma c.d. *permissionless* per gli aspetti relativi alla gestione dei processi di scambio e di trasferimento. Se da un lato l'esclusione dalla negoziazione di valori circolanti su questo tipo di infrastrutture assicura la costante esistenza di un centro di imputazione di effetti giuridici, dall'altra omette di considerare che la tenuta di un registro totalmente decentralizzato offre maggiori garanzie di immodificabilità e di sicurezza delle informazioni registrate in *blockchain*. La quotazione sulle piattaforme regolamentate non solleverebbe pertanto alcun problema sul piano dell'anonimato, poiché ai gestori delle piattaforme dovrebbe comunque essere imposto l'obbligo – già in essere per i cambiavalute virtuale ai sensi della vigente normativa antiriciclaggio – di identificare le parti coinvolte nello scambio.

3. Abusivismo bancario e finanziario. Profili di rilevanza penale dell'esercizio non autorizzato delle attività e dei servizi di investimento.

Il lungo *excursus* sulla possibilità di inquadrare i valori virtuali nelle categorie tipiche del diritto finanziario ci consente ora di sciogliere la riserva formulata in apertura del capitolo sui reati configurabili nel caso di esercizio non autorizzato dei servizi e delle attività di investimento.

---

infatti auspicabile fornire all'emittente uno strumento di valutazione sulla fattibilità dell'operazione e sul regime giuridico di riferimento.

[130] Tenuto conto della ormai conclamata vulnerabilità delle piattaforme di scambio agli attacchi informatici – basti pensare al clamore sollevato da vicende come il *crac* di Mt. Gox o Bitfinex, o dell'*exchange* italiano Bitgrail – l'esercizio dell'attività dovrebbe essere consentito ai soli soggetti che assicurino un livello elevato di sicurezza informatica, eventualmente certificato da un organismo nel rispetto degli standard internazionali (norme ISO IEC) o europei (Cybersecurity Act, Regolamento 2019/881/UE).

Per chiarezza argomentativa ci sembra anzitutto opportuno ricapitolare le conclusioni cui siamo pervenuti: le valute virtuali vengono in rilievo non solo come mezzo di pagamento, ma anche come strumento per la smobilizzazione dei contratti di investimento; la natura finanziaria dei *token* andrà accertata in concreto, rilevandosi all'uopo inadeguata qualsiasi classificazione di tipo formale; tutte le volte in cui il connotato finanziario dell'operazione risulti prevalente rispetto all'utilità economica effettiva del bene, l'*asset* sarà qualificabile come prodotto finanziario *ex* art. 1, comma 1, lett. u) TUF; ciò non esclude che alcune tipologie di *token* possano rientrare nella categoria dei valori mobiliari – e dunque degli strumenti finanziari – ai sensi dell'art. 1, comma 1-*bis*, lett. c) TUF[131].

Si giunge così al vero *core* della questione: l'emissione e l'intermediazione nella compravendita di valori virtuali sono attività libere ovvero sottoposte ai vincoli autorizzatori che presidiano il mercato finanziario? Entro che margini poter ritenere che tali attività costituiscano reato ai sensi degli artt. 130 ss. TUB e 166 TUF?

Nell'ordinamento nazionale le attività e i servizi di investimento sono riservati ai soggetti che possiedono particolari requisiti, sottoposti al vaglio preventivo della Consob o della Banca d'Italia.

Ciò spiega il motivo dell'esistenza di fattispecie criminose che, nel tutelare le prerogative di controllo pubblico sul sistema bancario o finanziario[132], assolvono indirettamente alla funzione di assicurare che l'esercizio del credito e l'intermediazione finanziaria siano svolti da soggetti affidabili sul versante organizzativo e patrimoniale[133]. Ad ogni buon conto, la rilevanza penale dell'attività svolta dagli intermediari e dagli emittenti del mercato valutario virtuale (*exchange*, piattaforme di cambio) rischia di scontrarsi contro i limiti imposti dal principio di tassatività in materia penale. Di qui l'ulteriore interrogativo, a cui tenteremo di dare risposta nella parte finale del paragrafo, sulla necessità o meno di un intervento del legislatore al fine di rendere più efficace il presidio penale contro le nuove forme di abusivismo finanziario.

---

[131] Sull'inquadramento degli asset virtuali tra gli strumenti finanziari v. *supra*, § 1.2.

[132] ALESSANDRI A., *Diritto penale e attività economiche,* Bologna, 2010, 265 ss.

[133] In dottrina v. CASTALDO A., *Accesso all'attività bancaria e strategie penalistiche di controllo*, in *Riv. It. dir. proc. pen*., 1996, 81 ss.; CANTONE R., *Abusivismo finanziario: esperienze da un'indagine giudiziaria*, in *Cass. Pen.*, 1996, 3122 ss.; CONTI L., *Profili penalistici del testo unico sull'intermediazione finanziaria*, in *Dir. pen. proc*., 1998, 548 ss.; RUGA RIVA C., *L'abusivismo finanziario: questioni giurisprudenziali e profili di illegittimità costituzionale*, in *Riv. trim. dir. pen. econ.*, 2001, 3, 531 ss.; ZANNOTTI R., *Il nuovo diritto penale dell'economia*, Milano, 2008, 359 ss.; ID., *La tutela dell'accesso al mercato nella prospettiva della lotta contro il riciclaggio: il caso dell'abusivismo*, in *Indice penale*, 2003, 929 ss.; ID., *La tutela penale del mercato finanziario,* Torino, 1997, 209 ss.; MONTANI E., *La tutela del corretto svolgimento dell'attività di intermediazione e bancaria*, in ALESSANDRI A. (a cura di), *Reati in materia economica*, Torino, 2017, 232 ss.; GUIDI D., *Una nuova ipotesi di abusivismo finanziario*, in GIUNTA F., MICHELETTI D. (a cura di), La disciplina penale del risparmio, Milano, 2008, 173 ss.; SORBELLO P., *L'abusivismo finanziario tra atto giuridicamente lecito e fatto penalmente rilevante*, in *Giurisprudenza di merito*, 2009, 2499 ss.

3.1. Il regime autorizzatorio previsto dal D. Lgs. 90/2017. Limiti esegetici e criticità applicative delle fattispecie di abusivismo previste dal Testo Unico Bancario.

L'intermediazione professionale nello scambio di valori virtuali ha dunque sollevato il dubbio sulla violazione delle prerogative pubbliche di gestione del risparmio. Si tratta di una eventualità che la Banca D'Italia[134] dimostra di aver preso in considerazione nell'effettuare una ben precisa distinzione tra gli utilizzatori a scopo privato e i soggetti che invece esercitano un'attività imprenditoriale[135]. Con riferimento a questi ultimi, viene richiamata l'attenzione sul fatto che le attività di emissione di valori, di conversione di moneta legale in valute virtuali e viceversa, e la gestione dei relativi schemi operativi «*potrebbero […] 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)*».

A seguito dell'emanazione del D. Lgs. n. 90/2017, la questione rimane di estrema attualità, in attesa che vengano emanati i decreti del Ministero dell'Economia e delle Finanze recanti la disciplina dei termini e le modalità per regolarizzare l'attività svolta dai prestatori di servizi connessi all'utilizzo delle virtuali[136]. Atteso che, nel nuovo assetto normativo «*la comunicazione costituisce condizione essenziale per l'esercizio*

[134] Si richiama la comunicazione denominata «Avvertenza sull'utilizzo delle cosiddette 'valute virtuali», 30 gennaio 2015, in https://bancaditalia.it. Il documento, pur ribadendo che nell'attuale quadro normativo l'utilizzo delle valute virtuali deve ritenersi in linea di principio lecito, pone in evidenza tutti i rischi collegati alla carenza di informazioni, alla mancanza di tutele legali e contrattuali e di forme di controllo o vigilanza, alla possibile perdita di fondi a causa di malfunzionamenti o attacchi informatici, all'elevata volatilità dei valori, a all'utilizzo della moneta virtuale per finalità illecite.

[135] In argomento anche VARDI, *"Criptovalute" e dintorni*, cit., 450; GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin*, cit., 432.

[136] L'art. 8, comma 1, del D. Lgs. 90/2017, nel modificare le disposizioni del D. Lgs. 141/2010 ha previsto che «*Le previsioni di cui al presente articolo si applicano, altresì, ai prestatori di servizi relativi all'utilizzo di valuta virtuale […] tenuti, in forza della presente disposizione, all'iscrizione in una sezione speciale del registro di cui al comma 1. […] Con decreto del Ministro dell'economia e delle finanze sono stabilite le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti a comunicare al Ministero dell'economia e delle finanze la propria operatività sul territorio nazionale. La comunicazione costituisce condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori […]*». Nel febbraio del 2018 il Ministero ha avviato una procedura di consultazione pubblica prodromica all'adozione della disciplina attuativa. Nello schema di decreto si disciplinano le modalità con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti a comunicare al Ministero dell'Economia e delle Finanze la loro operatività. Tra i destinatari dell'obbligo figurano anche gli operatori commerciali che accettano le valute virtuali quale corrispettivo di per la cessione di beni o la prestazione di servizi. Dal comunicato stampa n. 22 del 02 febbraio 2018 (https://mef.gov.it) si apprende che la consultazione pubblica mira a realizzare una prima rilevazione sistematica del fenomeno, a partire dalla consistenza numerica degli operatori del settore che, a regime, dovranno ad iscriversi in uno speciale registro tenuto dall'Organismo degli Agenti e dei Mediatori (OAM), per poter esercitare la loro attività sul territorio nazionale. Benché sia trascorso più di un anno dal termine dei lavori, il decreto attuativo non è stato ancora approvato.

legale dell'attività da parte dei suddetti prestatori»[137], si dovrà anche chiarire se l'avvenuta iscrizione nell'elenco costituisca un valido titolo di legittimazione per la prestazione di servizi di investimento *ex* art. 18 TUF o se, per questi ultimi, sia necessaria una specifica autorizzazione.

Non vi sono dubbi che l'intenzione del legislatore fosse quella di sottoporre gli intermediari del mercato valutario virtuale agli obblighi della normativa antiriciclaggio per porre un freno all'utilizzo delle criptovalute per fini criminosi[138]: l'obbligo di registrazione assolve dunque alla funzione primaria di rendere esperibile i controlli da parte delle Autorità pubbliche di vigilanza. Poiché la procedura non prevede alcun vaglio preventivo sul possesso dei requisiti indicati dal Testo unico finanziario, può ragionevolmente ritenersi che la prestazione di servizi di investimento non rientri tra le attività che tali intermediari sono legittimati a svolgere[139]. La disciplina dei mercati finanziari si muove dunque su un piano parallelo e complementare rispetto a quella dettata dal D. Lgs. 90/2017, di modo che l'applicazione dell'una non esclude l'altra e viceversa.

Per effetto del richiamo generalizzato alle disposizioni dell'art. 17-*bis* del D. Lgs. 141/2010 troverà applicazione anche il quinto comma del medesimo articolo che punisce a titolo di illecito amministrativo l'esercizio abusivo dell'attività, attribuendo al Ministero dell'economia e delle finanze il potere di irrogare le relative sanzioni[140]. Così facendo il legislatore ha previsto una fattispecie di abusivismo applicabile all'attività esercitata dai professionisti del mercato delle valute virtuali. La scelta è sicuramente condivisibile nei fini, ma risulta poco efficace nei mezzi; si tratta infatti di un presidio insufficiente, se paragonato alla previsione di sanzioni di natura penale per l'abusivismo bancario-finanziario.

Esaminando da vicino le disposizioni sanzionatorie del Testo unico bancario, non si rinviene tuttavia alcuna fattispecie di reato applicabile alle condotte di esercizio non autorizzato delle attività degli intermediari sul mercato delle criptovalute.

L'art. 132 TUB dietro la rubrica "abusiva attività finanziaria" punisce che svolge nei confronti del pubblico *«una o più attività finanziarie previste dall'articolo 106, comma 1 in assenza dell'autorizzazione […] o dell'iscrizione»*. L'articolo richiamato

---

[137] Così il nuovo comma 8-*bis* dell'art. 17-*bis* del decreto legislativo 13 agosto 2010, n. 141, come modificato dal D. Lgs. 90/2017 e, successivamente, dal D. Lgs. 125/2019. La disposizione disciplina l'esercizio professionale, nei confronti del pubblico di servizi connessi all'utilizzo delle valute virtuali. Il legislatore ha in sostanza equiparato le attività svolte dai professionisti del mercato delle criptovalute a quella dei cambiavalute, senza effettuare alcuna distinzione tra attività di *trading* (diretto e indiretto), *mining* e *mixing*. Ne consegue che tutti i prestatori di servizi relativi all'utilizzo di valuta virtuale saranno sottoposti alla medesima disciplina, senza distinzioni in base al tipo di attività in concreto svolta.

[138] Sull'irrilevanza della disciplina antiriciclaggio ai fini dell'affermazione della natura finanziaria dei valori virtuali v. GIRINO, *Criptovalute: un problema di legalità funzionale*, cit., 22 ss. Sul tema, v. anche *supra*, 1.2.2.

[139] Sarebbe infatti del tutto illogico sottoporre l'intermediazione finanziaria a regimi autorizzatori differenti a seconda nella tipologia di valori mobiliari offerti o scambiati.

[140] Il comma 5 dell'art. 17-*bis* D. Lgs 141/2010 dispone che *«L'esercizio abusivo dell'attività di cui al comma 1 è punita con una sanzione amministrativa da 2.065 euro a 10.329 euro emanata dal Ministero dell'economia e delle finanze»*.

si riferisce alla attività di concessione di finanziamenti sotto qualsiasi forma a sua volta definita dall'art. 2 della D.M. 6 luglio 1994[141]. Tale riferimento è sufficiente ad escludere dai soggetti attivi del reato gli emittenti e gli intermediari del mercato valutario virtuale, i quali non erogano alcuna forma di finanziamento.

Certamente più pertinente il richiamo ai delitti previsti dagli artt. 130 (abusiva attività di raccolta del risparmio) e 131 (abusiva attività bancaria) del TUB che puniscono, con gradualità sanzionatoria, *«chiunque svolge l'attività di raccolta del risparmio tra il pubblico in violazione dell'art. 11»,* e chi, svolgendo a monte una tale attività, *«esercita il credito»*. L'attività di raccolta del risparmio è definita come *«l'acquisizione di fondi con obbligo di rimborso, sia sotto forma di depositi sia sotto altra forma»* (art. 11, comma 1, TUB). Ciò basta ad 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 valori virtuali.

Il reato di abusiva emissione di moneta elettronica (art. 131-*bis* TUB)[142] sembrerebbe *prima facie* applicabile anche all'emissione non autorizzata di moneta virtuale. La condotta descritta dalla norma[143] fa però riferimento al complesso delle disposizioni del D. Lgs. 385/1993 che disciplinano in modo dettagliato limiti e condizioni di emissione[144]. La definizione di moneta elettronica elimina in radice ogni dubbio circa la possibilità di includervi le valute virtuali: il valore memorizzato nel supporto elettronico è rappresentato da un credito nei confronti dell'emittente pari al controvalore della somma di denaro precedentemente conferita, mentre gli asset DLT sono unità di conto puramente virtuale, privi di valore intrinseco o autoritativamente

---

[141] Il decreto, recante la determinazione, ai sensi dell'art. 106, comma 4, del decreto legislativo 1° settembre 1993, n. 385, del contenuto delle attività indicate nello stesso art. 106, comma 1, nonché in quali circostanze ricorre l'esercizio delle suddette attività nei confronti del pubblico, definisce l'attività di concessione di finanziamenti sotto qualsiasi forma come *«la concessione di crediti ivi compreso il rilascio di garanzie sostitutive del credito e di impegni di firma. Tale attività ricomprende, tra l'altro, ogni tipo di finanziamento connesso con operazioni di: a) locazione finanziaria; b) acquisto di crediti; c) credito al consumo, così come definito dall'art. 121 del testo unico, fatta eccezione per la forma tecnica della dilazione di pagamento; d) credito ipotecario; e) prestito su pegno; f) rilascio di fidejussioni, avalli, aperture di credito documentarie, accettazioni, girate nonché impegni a concedere credito. Fanno eccezione le fideiussioni e altri impegni di firma previsti nell'ambito di contratti di fornitura in esclusiva e rilasciati unicamente a banche e intermediari finanziari»*.

[142] L'emissione di moneta elettronica non è considerata dalla legge come una forma di raccolta del risparmio (art. 11, comma 2-*bis*, TUB); per questo motivo il legislatore ha avvertito la necessità di inserire una autonoma fattispecie di abusivismo che riguarda l'attività degli emittenti di moneta elettronica.

[143] La disposizione recita: «*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 […]»*.

[144] L'art. 1, comma 2, lett *h-ter,* TUB definisce la moneta elettronica come «*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 […] e che sia accettato da persone fisiche e giuridiche diverse dall'emittente»*. Sulle divergenze tra la nozione di "moneta elettronica" e di "valuta virtuale" v. Cap. III, § 2.2.

stabilito, fondati unicamente sulla fiducia degli utenti e sulla formazione del prezzo sulle piattaforme di scambio.

Considerazioni non dissimili valgono per il successivo reato di abusiva attività di prestazione di servizi di pagamento (art. 131-*ter* TUB), la cui condotta esecutiva si esaurisce nella inosservanza delle disposizioni degli artt. 144-*sexies* ss. La definizione di "servizi di pagamento"[145] risulta però difficilmente applicabile all'universo valutario virtuale[146]. La principale differenza risiede nella materiale disponibilità delle somme "depositate" dall'utente: mentre nel caso del conto di pagamento il denaro entra nella piena disponibilità del fornitore del servizio[147], la quantità di valuta virtuale presente nel portafoglio digitale rimane nell'esclusiva sfera di dominio del proprietario, titolare dell'indirizzo e delle chiavi private di criptazione.

3.1.1. Conclusioni in punto di irrilevanza penale dell'esercizio non autorizzato dell'attività di cambiavalute virtuali.

Alla luce dell'indagine finora svolta, non ci sembra cogliere nel segno la sopra richiamata avvertenza della Banca D'Italia secondo cui i prestatori di servizi di cambio di valute virtuali potrebbero incorrere in responsabilità penale per abusivismo bancario. Rimane comunque complesso stabilire se all'esercizio non autorizzato siano applicabili sanzioni ulteriori rispetto a quelle previste per l'inosservanza dell'obbligo di iscrizione di cui all'art. 17-*bis*.

Sicuramente non potrà trovare applicazione la disciplina dettata dal D. Lgs. 31 marzo 1998, n. 114 (c.d. legge sul commercio), che punisce come illecito amministrativo (art. 22) il mancato rispetto delle disposizioni concernenti il preventivo rilascio dell'autorizzazione o la comunicazione di inizio dell'attività. Tale normativa,

[145] Secondo la definizione fornita dall'art. 1, comma 1, lett. b) del D. Lgs. 27 gennaio 2010 n. 11 rientrano tra i 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».*

[146] I fornitori di tali servizi permettono di depositare il contante su un "conto di pagamento" e di effettuare tutte le operazioni richieste per la gestione del conto medesimo. Sebbene le principali piattaforme di *trading* offrano servizi aggiuntivi di portafoglio digitale (*e-wallet)*, mettendo a disposizione un *software* di gestione della valuta virtuale, l'attività difficilmente potrebbe essere paragonata alla gestione di un conto di pagamento. Fanno tuttavia eccezione i servizi di pagamento offerti dai gestori di *blockchain* private che, a determinate condizioni, sembra poter rientrare nel concetto di "servizio di pagamento". A tal fine sarà tuttavia necessario riconoscere pieno valore monetario alle valute virtuali, circostanza che lascia adito a non pochi dubbi (cfr. Cap. III, § 1.2. e 1.5.).

[147] Proprio per questo motivo la prestazione di servizi di pagamento viene disciplinata dal Testo Unico Bancario, essendo finitima rispetto alle forme regolamentate di raccolta del risparmio.

infatti, riguarda soltanto gli esercenti il commercio all'ingrosso e al dettaglio in sede fissa, e coloro che lo esercitano su aree pubbliche[148].

Con l'emanazione del D. Lgs. 9 aprile 2003 n. 70, c.d. Codice del commercio elettronico, adottato in attuazione della direttiva 2000/31/CE, il Legislatore ha regolamentato la materia in modo molto liberale, così da favorire i prestatori di servizi della società dell'informazione. Quest'ultima definizione abbraccia tutte le attività economiche svolte *on line*, tra le quali certamente rientrano le attività svolte dagli operatori professionali sul mercato delle valute virtuali. L'impronta liberista risulta evidente dalla lettura dell'art. 6, rubricato "assenza di autorizzazione preventiva", a mente del quale *«l'accesso all'attività di prestatore di un servizio della società dell'informazione e il suo esercizio non sono soggetti, in quanto tali, ad autorizzazione preventiva o ad altra misura di effetto equivalente»*. Se collocate nel quadro di disciplina relativo al commercio elettronico, le attività in esame non necessiterebbero di alcun provvedimento autorizzatorio.

Da un esame congiunto dei testi normativi finora citati sembra potersi concludere che l'attività dei prestatori di servizi relativi all'utilizzo di valuta virtuale – diversamente dalle attività commerciali "fisiche" o finanziarie in senso stretto – non sia sottoposta ad alcun regime amministrativo di autorizzazione diverso dall'iscrizione nel registro OAM[149]. Risulta infatti evidente la completa assimilazione, ai fini della disciplina amministrativa, dell'attività dei professionisti della valuta virtuale a quella dei cambiavalute della moneta reale, che giustifica l'estensione ai primi della normativa disciplinante l'attività dei secondi.

3.2. Esercizio non autorizzato di "servizi" e le "attività" di investimento. I vasti orizzonti applicativi dell'art. 166 del Testo Unico della Finanza.

La maggiore duttilità applicativa della fattispecie di abusivismo finanziario prevista dal TUF permette di ricondurre nell'area del penalmente l'emissione e l'offerta non autorizzate di valori virtuali.

Nel dettaglio, l'art. 166 del Testo unico punisce tre distinte condotte, precisamente quella di chi senza esservi abilitato: a) svolge servizi o attività di 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.

---

[148] A conferma dell'inapplicabilità delle disposizioni al *trading online* lo stesso decreto prevede future iniziative volte a promuovere l'introduzione e l'uso del commercio elettronico (art. 21).

[149] Il nuovo comma 8-*bis* dell'art. 17-*bis* del D. Lgs. 141/2010 recita: *«Le previsioni di cui al presente articolo si applicano, altresì, ai prestatori di servizi relativi all'utilizzo di valuta virtuale, come definiti nell'articolo 1, comma 2, lettera ff), del decreto legislativo 21 novembre 2007, n. 231, e successive modificazioni tenuti, in forza della presente disposizione, all'iscrizione in una sezione speciale del registro di cui al comma 1».*

Si tratta di un reato di pericolo astratto, che riflette l'esigenza del legislatore di anticipare la tutela apprestata in sede penale prima ancora che si verifichi un effettivo nocumento al pubblico dei risparmiatori e all'integrità del mercato finanziario[150].

Sebbene la disposizione non specifichi che le attività debbano essere esercitate nei confronti del pubblico, un tale elemento può ritenersi assorbito nella descrizione delle condotte esecutive. La prestazione di servizi e di attività di investimento e l'offerta di strumenti o prodotti finanziari implicano infatti una apertura al pubblico dei servizi da intendersi in senso non quantitativo, ma qualitativo, come astratta idoneità a raggiungere un numero non determinato di soggetti[151]. Una parte della giurisprudenza ritiene che si tratti di un reato istantaneo eventualmente permanente, la cui consumazione si protrae per tutto il tempo in cui vengono posti in essere dal soggetto attivo gli atti tipici della funzione di intermediazione finanziaria[152].

Per l'integrazione del delitto è sufficiente la sussistenza del dolo generico, consistente nella coscienza e volontà dell'agente di svolgere le attività sopra indicate con la consapevolezza di non aver acquisito la relativa abilitazione[153].

Dalla lettura della disposizione emerge piuttosto chiaramente la volontà del legislatore ci circoscrivere l'area del penalmente rilevante a un ristretto numero di ipotesi. Ciononostante, non si ravvisano ostacoli significativi all'applicazione della fattispecie laddove siano esercitati attività e servizi collegati all'emissione di valori virtuali al di fuori del regime autorizzatorio previsto dal TUF. Occorrono tuttavia alcune precisazioni.

Quanto alla condotta *sub* a) si è detto che i servizi e le attività di investimento sono definiti elencando una serie di attività[154] aventi per oggetto "strumenti finanziari".

---

[150] In giurisprudenza si è addirittura parlato di *«reato di pericolo presunto che richiede, ai fini della rilevanza oggettiva del fatto, una serie coordinata di atti svolti professionalmente e rivolti a una platea non qualitativamente determinata di soggetti»*. In tal senso Cass. Pen., Sez. V, 29 maggio 2013 n. 27246, in Diritto penale contemporaneo, 9 gennaio 2014, con nota di FERRI F., MIGLIO M., *In tema di abusivismo finanziario*.

[151] Dovrebbe parimenti ritenersi implicito il connotato di professionalità delle condotte penalmente rilevanti. Il pericolo astratto per l'integrità del mercato finanziario sorge infatti soltanto laddove vi sia una organizzazione finalizzata all'esercizio di servizi e attività di investimento in assenza di autorizzazione.

[152] Cass. Pen., Sez. V, 3 febbraio 2015 n. 28157, in *Cass. Pen*., 2017, 306 ss., con nota di PANTANELLA A., *Il bene giuridico nel reato di esercizio abusivo di intermediazione finanziaria*. La tesi è richiamata anche da BASILE E., *Chiaroscuri della Cassazione in tema di abusivismo bancario e finanziario, in Diritto penale contemporaneo,* 15 maggio 2017, § 10. Nello stesso senso per la fattispecie di abusivismo bancario v. CAPRIGLIONE F., *Commentario al Testo Unico delle Leggi in materia bancaria e creditizia*, *sub* Art. 132, Padova, 2018, 2579 ss. Al di là dell'aspetto teorico, la qualificazione come reato eventualmente permanente riveste considerevole importanza pratica per l'individuazione del momento consumativo, come pure allo scopo di stabilire se, in caso di plurime condotte, vi sia spazio per ritenere integrati più fatti uniti dal vincolo della continuazione *ex* art. 81 cpv. c.p.

[153] Cfr. ZANNOTTI, *Il nuovo diritto penale dell'economia*, cit., 371; MONTANI, *La tutela del corretto svolgimento dell'attività di intermediazione e bancaria*, cit., 232.

[154] Vengono elencate, per la precisione, la negoziazione per conto proprio, esecuzione di ordini per conto dei clienti, gestione di portafogli ricezione e trasmissione di ordini, consulenza in materia di investimenti, gestione di sistemi multilaterali di negoziazione. Tali attività di prestano a ricomprendere le attività tipiche dei prestatori di servizi connessi all'utilizzo di valute virtuali. Così, ad esempio, la "gestione di portafogli" potrebbe essere estesa ai fornitori di servizi *e-wallet*, mentre la "negoziazione per conto

Considerato che tra questi ultimi rientrano anche i valori mobiliari di cui all'art. 1, comma 1-*bis* del TUF[155] l'ambito di rilevanza penale dell'abusivismo finanziario si estende a tutte le attività di negoziazione aventi ad oggetto quelle valute virtuali che, oltre ad essere negoziabili su un mercato secondario, presentino un sottostante riferito a valute, indici, merci o *commodities* di altro tipo[156]. Si deve dunque effettuare una distinzione in base alle caratteristiche specifiche dei *token* e/o del contratto di investimento, ammettendo la riconducibilità ai valori mobiliari – e dunque agli strumenti finanziari – delle unità rappresentative di quote di società o di debito oppure di valori reali regolati a pronti.

Anche la seconda condotta, consistente nell'offerta in Italia di quote o azioni di Oicr, può assumere un qualche rilievo nel settore in esame. Come noto, il patrimonio dell'organismo di investimento collettivo è raccolto tra una pluralità di investitori mediante l'emissione e l'offerta di quote o azioni e impiegato per l'acquisto di strumenti finanziari o crediti in base a una politica di investimento predeterminata. Laddove i titoli rappresentativi della partecipazione all'organismo fossero resi disponibili in forma di *token*, la relativa offerta nelle sedi di negoziazione italiane richiederebbe una specifica autorizzazione. Nell'ultimo biennio sono stati creati all'estero numerosi fondi di investimento in criptovaluta che funzionano esattamente come organismi di investimento collettivo[157]. La definizione nazionale di Oicr trova corrispondenza solo parziale nelle disposizioni nella direttiva 2009/65/CE sugli organismi d'investimento collettivo in valori mobiliari (OICVM)[158] che elenca una serie di strumenti di investimento che caratterizzano l'attività svolta da questi soggetti (tra cui valori mobiliari, strumenti del mercato monetario, derivati finanziari e ricevute di deposito). In ogni caso, perché un fondo di investimento possa operare come Oicr, nazionale o straniero, dovrà essere abilitato allo svolgimento dell'attività e osservare le disposizioni sull'offerta delle quote agli investitori. Ciò anche nel caso in cui le attività del fondo siano gestite mediante valori virtuali, circostanza che non esime affatto dal rispetto della normativa pubblicistica; l'inosservanza del regime autorizzatorio per

proprio" ricorda l'attività di *trading* che abbiamo definito "diretto" (*amplius*, § 1.2.). Per "gestione collettiva del risparmio" si intende invece il servizio che si realizza attraverso la gestione di organismi di investimento collettivo e i relativi rischi (art. 1, comma 1, lett. k TUF).

[155] Sulla definizione di valori mobiliari v. *supra*, § 1.2. *sub* nota 24.

[156] È il caso delle c.d. *Stablecoin*, attualmente al centro dell'attenzione mediatica mondiale dopo l'annuncio da parte di Facebook Inc. di aver preso parte alla creazione di Libra, una valuta virtuale il cui prezzo di cambio è ancorato a una riserva di *asset* reali (beni, titoli di debito, moneta avente corso reale).

[157] L'ente raccoglie capitali offrendo agli investitori valute virtuali rappresentative di quote di partecipazione al fondo, per poi impiegare la provvista per l'acquisto di criptovalute o altri asset tokenizzati. Al termine dell'investimento il capitale investito viene remunerato liquidando dividendi o attribuendo agli investitori la disponibilità di un ammontare di valuta virtuale corrispondente al rendimento dei titoli.

[158] Ai sensi dell'art. 1 della direttiva oggetto esclusivo dell'attività svolta da tali soggetti è *«l'investimento collettivo dei capitali raccolti presso il pubblico in valori mobiliari o in altre attività finanziarie liquide di cui all'articolo 50, par. 1, e il cui funzionamento è soggetto al principio della ripartizione dei rischi; le cui quote sono, su richiesta dei detentori, riacquistate o rimborsate, direttamente o indirettamente, a valere sul patrimonio dei suddetti organismi»*.

l'offerta delle quote potrà quindi assumere rilevanza penale ai sensi della disposizione in esame.

Ben più ampio il campo di applicazione dell'ipotesi *sub* c), idonea a ricomprendere tutte le condotte di promozione, offerta e collocamento di cripto-attività finanziarie da parte di soggetti non abilitati[159]. L'oggetto materiale della condotta è qui riferito non solo gli strumenti finanziari ma anche ai prodotti finanziari, cioè a ogni forma di investimento di natura finanziaria. Considerato che in tale categoria rientrano le più varie formule negoziali in cui vi è un impiego di un capitale caratterizzato dall'aspettativa di un rendimento e dall'assunzione di un rischio di natura finanziaria[160], la tutela penale contro l'abusivismo riuscirà a raggiungere anche le attività d'investimento realizzate mediante l'offerta di valori virtuali.

Gli intermediari saranno in particolare tenuti all'osservanza della disciplina del collocamento a distanza di prodotti finanziari[161], sottoposto all'autorizzazione preventiva della Consob in base alle informazioni contenute nel prospetto. Secondo la definizione fornita dall'art. 1, comma 1, lettera t) TUF per "offerta al pubblico di prodotti finanziari" deve intendersi *«ogni comunicazione rivolta a persone, in qualsiasi forma e con qualsiasi mezzo, che presenti sufficienti informazioni sulle condizioni dell'offerta e dei prodotti finanziari offerti così da mettere un investitore in grado di decidere di acquistare o di sottoscrivere tali prodotti finanziari, incluso il collocamento tramite soggetti abilitati»*[162].

Si ritiene che i promotori di criptoattività finanziarie – tali cioè da integrare la nozione domestica di prodotto finanziario – debbano rispettare non solo le regole generali in materia di servizi di investimento, ma anche la stringente disciplina dettata per la sollecitazione[163]. L'inosservanza delle disposizioni autorizzatorie sull'offerta e

[159] La lettera è stata modificata dall'art. 5 del D. Lgs. 3 agosto 2017 n. 129 (Attuazione della direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari) che ha inserito il riferimento ai prodotti finanziari, prima assente. L'art. 31 del Testo unico prevede che per l'offerta fuori sede i soggetti abilitati debbano avvalersi di consulenti finanziari a ciò autorizzati, e che il soggetto abilitato conferente l'incarico sia responsabile in solido dei danni arrecati a terzi dal consulente finanziario abilitato all'offerta fuori sede. Presso l'Organismo di vigilanza è stato istituito un albo unico dei consulenti finanziari, nel quale sono iscritti in tre distinte sezioni i consulenti finanziari abilitati all'offerta fuori sede, i consulenti finanziari autonomi e le società di consulenza finanziaria.

[160] In essa rientra ogni strumento, comunque denominato, che sia rappresentativo dell'impiego di un capitale in misura prevalente rispetto al godimento del bene. Cfr. *supra*, § 1.2.1.

[161] Per tecniche di comunicazione a distanza si intendono «*le tecniche di contatto con la clientela, diverse dalla pubblicità, che non comportano la presenza fisica e simultanea del cliente e del soggetto offerente o di un suo incaricato*». La materia è oggi regolata dalla delibera Consob n. 20307 del 15.2.2018 che ha sostituito la precedente delibera n. 16190 del 29 ottobre 2007 (c.d. Regolamento Intermediari).

[162] Si realizza una offerta al pubblico anche qualora i prodotti finanziari che abbiano costituito oggetto in Italia o all'estero di un collocamento riservato a investitori qualificati siano, nei dodici mesi successivi, sistematicamente rivenduti a soggetti diversi da investitori qualificati (art. 100-*bis*, comma 2, TUF).

[163] Prima della pubblicazione dell'offerta l'intermediario dà comunicazione alla Consob circa le caratteristiche dell'operazione (art. 94, comma 1, TUF) compilando un prospetto informativo che, previa autorizzazione rilasciata dall'Autorità, dovrà essere diffuso affinché i risparmiatori possano *«pervenire a un fondato giudizio sulla situazione patrimoniale, economica e finanziaria e sull'evoluzione dell'attività dell'emittente nonché sui prodotti finanziari e sui relativi diritti»* (art. 94, comma 2). Laddove la proposta d'investimento sia condotta a distanza, l'intermediario sarà assoggettato alla

sul collocamento a distanza potrà assumere rilevanza come esercizio abusivo di attività finanziaria ai sensi della disposizione in esame[164].

Per concludere, la condotta descritta dalla lettera c-*bis*) si riferisce alla prestazione non autorizzata di servizi di comunicazione di dati[165], materia regolata dalle disposizioni della MiFID II[166]. La direttiva attribuisce all'Autorità designata dagli Stati membri il potere autorizzare allo svolgimento dell'attività i soggetti in possesso di determinati requisiti, salva la possibilità di abilitare anche le imprese di investimento e i gestori delle sedi di negoziazione. La comunicazione dei dati riguarda i mercati regolamentati e le operazioni di negoziazione e post-negoziazione di strumenti finanziari, circostanza che rende estremamente limitate le possibilità di applicazione della norma all'attività degli intermediari del mercato valutario virtuale.

3.3. L'ineludibile certezza del diritto. Riflessioni sull'opportunità di regolare l'emissione e lo scambio di criptoattività finanziarie.

L'indagine fin qui svolta consente di affermare che, nell'ordinamento vigente, l'offerta non autorizzata di criptoattività finanziarie è idonea a integrare gli estremi del reato di abusivismo finanziario. Ciò non esonera dal chiedersi se, in un quadro dominato dal rapido sviluppo del Fintech e dalla ampia diffusione di valori virtuali, sia opportuno un intervento del legislatore per disciplinare in modo organico la materia.

---

disciplina prevista per la l'offerta fuori sede regolata da disposizioni specifiche a tutela dell'investitore/consumatore.

[164] L'offerta al pubblico di prodotti finanziari è sottoposta ad una specifica disciplina (Capo I del Titolo II della Parte IV del TUF; Titolo I del Regolamento emittenti, approvato dalla Consob con delibera n.11971 del 14 maggio 1999; Libro VII del Regolamento Intermediari, approvato dalla Consob con delibera n. 16190 del 29 ottobre 2007), volta ad assicurare la correttezza e la completezza delle informazioni da fornirsi ai potenziali investitori e la parità di trattamento dei destinatari dell'offerta. Gli intermediari dovranno rispettare le norme sull'offerta al pubblico di prodotti finanziari (art. 94 ss. TUF) che impongono una serie di obblighi di trasparenza e di informazione nei confronti degli investitori. Nel dettaglio, la proposta dovrà essere accompagnata dalla pubblicazione di un prospetto informativo redatto secondo gli schemi predisposti dalla Consob; in caso di omissione gli interessati saranno esposti alle onerose sanzioni pecuniarie di cui all'art. 191 del TUF, salva la rilevanza penale del fatto in caso di informazione mendace (v. *infra*, § 4.2.).

[165] L'art. 1, comma 6-*undecies*, lett. d) TUF definisce tali servizi come la gestione di un dispositivo di pubblicazione autorizzato (APA) o di un sistema consolidato di pubblicazione (CTP) o di un meccanismo di segnalazione autorizzato (ARM). La fornitura di servizi di comunicazione dati è soggetta ad autorizzazione preventiva da parte della Consob, che vigila sui fornitori di servizi di comunicazione dati e controlla regolarmente che essi rispettino le disposizioni degli artt. 79 ss. TUF.

[166] Il legislatore europeo ha disciplinato l'attività dei data reporting services tra cui i dispositivi di pubblicazione autorizzati (*Approved Publication Arrangement* – APA), i meccanismi di segnalazione autorizzati (*Approved Reporting Mechanism* – ARM) e i sistemi consolidati di pubblicazione (*Consolidated Tape Provider* – CTP). L'intento del legislatore europeo è quello di offrire agli investitori una visione globale dell'attività di negoziazione su tutti i mercati finanziari dell'Unione Europea e le Autorità competenti possano ricevere informazioni accurate ed esaustive sulle operazioni rilevanti. In argomento v. SCACCHI F., ZAGHINI G., *MiFID II. I servizi di comunicazione dati: APA, ARM e CTP, in Rivista di diritto bancario*, 18 settembre 2015, 1 ss.

La risposta positiva appare nettamente preferibile, per evidenti ragioni di prevedibilità e certezza del diritto.

Per quanto l'assimilazione dei valori virtuali ai prodotti finanziari possa ritenersi appropriata, esiste un ineliminabile margine di discrezionalità nella valutazione dei requisiti propri di questi ultimi. Risulta infatti tutt'altro che agevole l'apprezzamento, ad esempio, della negoziabilità su un mercato secondario: occorre la quotazione su una piattaforma di *exchange*, o è sufficiente l'astratta idoneità del *token* ad essere trasferito *peer to peer* mediante registri distribuiti? Lo stesso dicasi a proposito del criterio di prevalenza tra aspettativa finanziaria e utilizzo del bene: *quid iuris* per quei valori che, pur incorporando diritti reali o personali di godimento, siano quotati su piattaforme di *trading*?

In assenza di indicazioni legislative può ben darsi che l'inquadramento delle cripto-attività nelle categorie del diritto finanziario sia, per gli operatori del settore, un esito tutt'altro che prevedibile. Soltanto in tempi recenti la questione è giunta all'attenzione della Consob, che ha sottoposto a consultazione pubblica alcuni lineamenti della futura normativa senza tuttavia chiarire quale forma giuridica essa dovrà rivestire. Gli aspetti tecnici della materia[167] dovranno essere disciplinati con regolamento *ex* art. 3 TUF[168], previa creazione di una base normativa a fondamento dell'azione dell'autorità di settore. Del resto, una compiuta definizione delle caratteristiche proprie delle "cripto-attività" finanziarie all'interno del Testo unico, che sia non limitata al solo impiego per il finanziamento di progetti imprenditoriali, appare decisamente opportuna. Spetterà dunque al legislatore tanto la codificazione di una categoria *ad hoc* – eventualmente distinta dai prodotti finanziari – quanto la decisione sul regime normativo cui essa debba essere soggetta. A ben vedere, soltanto una legge potrebbe accordare deroghe alla disciplina nazionale in materia di prospetto e offerta a distanza, non potendo una scelta così delicata essere attratta ai poteri impliciti dell'autorità di vigilanza.

Ciò non sottrae campo all'adozione di norme di dettaglio sui requisiti tecnici e organizzativi per lo svolgimento dell'attività, sulle procedure da seguire per le comunicazioni prescritte dalla legge e per le informazioni sui rischi dell'investimento. Sarebbe del resto auspicabile che le fonti secondarie fornissero alcuni parametri di valutazione (ad esempio linee guida contenenti indici analitici) o prevedessero procedure di interpello preventivo sull'assoggettamento alla disciplina settore.

---

[167] Quali, ad. esempio, i requisiti e le procedure di registrazione dei gestori di portali per l'offerta e lo scambio di cripto-attività.

[168] Come noto, l'ampiezza dei poteri regolamentari spettanti alla Consob è una questione discussa in dottrina. Le disposizioni del Testo unico assegnano all'autorità il potere di vigilare sulla trasparenza e sulla correttezza dei comportamenti di società d'investimento e di gestione collettiva. Così, ad esempio, l'art. 74 TUF impone il controllo sulla trasparenza dei mercati e sull'ordinato svolgimento delle negoziazioni, mentre l'art. 91 TUF attribuisce alla Commissione un potere regolamentare in relazione agli obiettivi di trasparenza, efficienza e tutela degli investitori. Cfr. RODORORF R., *La Consob come autorità indipendente nella tutela del risparmio*, in *Foro Italiano*, 2000, 147 ss.; DE MINICO G., Lineamenti del potere regolamentare della Consob, in DE SIERVO U. (a cura di), *Osservatorio sulle fonti* 1996, Torino, 1996, 203 ss.

L'opportunità di un intervento del legislatore si avverte in misura anche maggiore sul fronte repressivo. L'applicazione dell'art. 166 TUF alle attività esercitate dagli intermediari del mercato valutario virtuale potrebbe di fatto risultare imprevedibile, a causa degli evidenti difetti redazionali della fattispecie di abusivismo finanziario pocanzi esaminata.

La condotta è descritta mediante la tecnica del rinvio "aperto" alle norme di disciplina senza indicare con precisione le disposizioni di riferimento (*«È punito […] chiunque, senza esservi abilitato ai sensi del presente decreto»*), lasciando all'interprete l'arduo compito di ricostruire il precetto in base al regime amministrativo delle diverse attività di intermediazione finanziaria[169]. Probabilmente il legislatore ha scelto di sacrificare la determinatezza della fattispecie nella consapevolezza delle spasmodiche modifiche e dei continui aggiornamenti al Testo unico finanziario. Se fossero stati inseriti precisi riferimenti alle norme di disciplina, il rischio di lacune di tutela sarebbe stato decisamente elevato. Evidenti sono però le ricadute sul piano della conoscibilità della norma penale che risente tanto dell'indeterminatezza del divieto, quanto dell'assenza di una definizione legislativa dei valori virtuali.

La codificazione della categoria delle "cripto-attività finanziarie" permetterebbe di individuare più facilmente la regola di condotta, evitando il passaggio obbligato sullo scivoloso terreno dei prodotti finanziari. Sarebbe sufficiente che il legislatore aggiungesse all'elenco dell'art. 166 una lettera c-*ter*) del seguente tenore: *«presta servizi o attività di investimento, ovvero offre, promuove o colloca mediante tecniche di comunicazione a distanza, cripto-attività finanziarie in violazione degli articoli […]».* In tal modo il presidio penale sarebbe limitato al solo esercizio non autorizzato di determinate attività (servizi e attività di investimento, offerta al pubblico etc.) aventi ad oggetto una particolare categoria di *asset* virtuali – le cripto-attività finanziarie, caratterizzate dagli elementi tipici degli investimenti di natura finanziaria. Il richiamo a precise norme di disciplina si rende a nostro avviso opportuno al fine di superare la criticabile tecnica redazionale che fino a oggi è stata impiegata per la formulazione dell'art. 166 TUF.

L'auspicio per il futuro è che il legislatore possa fare chiarezza in un panorama dominato da dubbi e incertezze sull'inquadramento giuridico dei valori virtuali che, oltre a nuocere allo sviluppo delle nuove forme di circolazione della ricchezza, rischia di frustrare le esigenze di tutela del mercato finanziario[170].

[169] Come noto la tecnica del rinvio è ampiamente utilizzata in settori caratterizzati dall'elevato tecnicismo della materia (ambiente, beni culturali, tutela dei dati personali). Se da una parte tale tecnica presenta il difetto di non rendere immediatamente intellegibile il precetto penale, dall'altra contribuisce a puntualizzare quali siano le norme di disciplina la cui inosservanza viene sanzionata penalmente. Si ritiene pertanto che il legislatore debba farne buon uso, inserendo un espresso richiamo a norme precise e immediatamente prescrittive.

[170] Se da un lato la stasi normativa pone un freno alle nuove forme di finanziamento, dall'altro non potrebbe non considerarsi il potenziale effetto criminogeno dato dalla mancanza di sanzioni penali contro le nuove forme di abusivismo finanziario.

4. *Trading* di asset virtuali e tutela del mercato finanziario.

Il mercato valutario virtuale è del tutto libero dai vincoli tipici dei mercati regolamentati. Se da un lato ciò alimenta il timore per i rischi associati alla criptomoneta, dall'altro apre le porte al paradiso della speculazione, non essendovi limiti all'aumento del prezzo dei titoli o procedure particolari per la concentrazione di valori nelle mani di pochi investitori. Trattandosi di una piazza di scambio che, a pochi anni dalla sua nascita, vanta una capitalizzazione misurabile in centinaia di miliardi di dollari, si dovrebbe iniziare a pensare all'opportunità di introdurre regole a tutela della fiducia degli investitori, non diversamente da quanto accade per i mercati regolamentati.

Rovesciando ora la prospettiva dell'indagine, fino a questo momento focalizzata sulla permeabilità del mercato mobiliare ai rischi della criptofinanza, ci si domanda se la tutela penale accordata a quest'ultimo possa o debba estendersi anche al *trading* valutario virtuale. A prima vista la questione potrebbe sembrare avanguardista – o forse addirittura pioneristica – se si paragona la quantità di capitali circolante nel mercato borsistico con il volume giornaliero di transazioni in valuta virtuale su scala globale[171]. Andando oltre il mero dato quantitativo – di per sé non indicativo della meritevolezza di tutela – dovrebbe aversi riguardo al bene giuridico da proteggere, ovvero il risparmio. Non vi è chi non veda come l'esigenza di tutela sottesa al mercato finanziario sia unica, a dispetto di ogni distinzione tra sedi rituali di negoziazione e piattaforme di *trading* virtuale.

Che senso avrebbe imporre un prospetto informativo per l'offerta di cripto-attività al fine di tutelare l'interesse patrimoniale degli investitori, se poi questi ultimi sono esposti alle più svariate forme abuso del mercato? Non sarebbe forse coerente con (l'affermazione della) natura finanziaria dei valori virtuali ammettere la necessità di una qualche forma di tutela, presidiando così la trasparenza del mercato degli scambi? Ben presto tali interrogativi giungeranno all'attenzione della prassi, specialmente laddove si verificassero nuovamente condotte riconducibili a vere e proprie forme di abuso di mercato.

La cronaca degli ultimi anni ha messo in luce quanto il mercato valutario virtuale sia esposto a condotte illecite riconducibili a ipotesi di *market abuse*[172]. In un rapporto

[171] Deve comunque darsi atto del fatto che la situazione sta cambiando rapidamente. Guardando ad esempio ai dati di mercato di Piazza Affari (https://borsaitaliana.it) emerge che nel luglio del 2019 la media giornaliera degli scambi è stata di circa 2 miliardi di euro, di gran lunga inferiore rispetto al volume medio giornaliero di transazioni globali in Ethereum nello stesso periodo. Il che vuol dire che il principale mercato italiano scambia quotidianamente titoli per un valore non paragonabile a quello della seconda criptovaluta per capitalizzazione.

[172] Si pensi alla vicenda scaturita dal *listing* di Bitcoin Cash (BCH) su *Coinbase Inc*. Nelle ore che hanno preceduto l'annuncio, il prezzo di cambio del titolo è addirittura raddoppiato per effetto di un improvviso innalzamento della domanda di acquisto. Ciò ha condotto al sospetto di uno sfruttamento da parte degli intranei di *Coinbase,* dell'informazione privilegiata relativa alla quotazione della valuta sulla piattaforma.

del 2016 la Prudential Regulation Authority del Regno Unito ha addirittura stimato che quasi il 30% degli acquisti possa essere l'effetto di *insider trading*[173].

A ben vedere, nella dimensione economico finanziaria attuale, dominata dall'intelligenza artificiale, dai *social media*, e dalla dematerializzazione dei valori, il *market abuse* "ad alto contenuto tecnologico" non è affatto un fenomeno limitato al *trading* virtuale, ben potendo causare la distorsione dei mercati regolamentati. Tuttavia, nell'universo valutario virtuale la realizzazione di abusi di mercato risulta decisamente più agevole poiché non vi è alcun limite all'aumento o al ribasso del prezzo di scambio né esistono autorità di vigilanza in grado di esperire i propri controlli sulla ritualità delle negoziazioni e sul rispetto dei limiti imposti dalla legge[174].

Di certo la presenza di una vasta zona franca da responsabilità – penale e amministrativa – per le condotte di *market abuse* non disincentiva gli operatori da porre in essere comportamenti di questo tipo. Ciò rappresenta un ostacolo significativo alla crescita del Fintech, sul quale dovrebbe iniziarsi a riflettere per non frustrare le esigenze connesse alla tutela degli investitori. Il *core* della questione è dato dalla possibilità di reprimere tali condotte facendo leva sulle vigenti fattispecie di abuso di informazioni privilegiate e di manipolazione del mercato: una opzione senza dubbio affascinante ma allo stato – fatte salve alcune ipotesi – decisamente non percorribile per le ragioni di seguito esposte.

4.1. L'inapplicabilità delle fattispecie di *market abuse*.

L'art. 184 TUF[175] delimita l'area dell'incriminazione al concetto di informazione privilegiata concretamente idonea a influenzare il prezzo degli strumenti finanziari.

[173] Bank of England, Annual Report and Accounts 2016, in https://bankofengland.co.uk

[174] La preoccupazione per la piega assunta dal fenomeno è accresciuta dalla spinta criminogena offerta dalla possibilità di conseguire ingenti profitti mediante la diffusione di informazioni false oppure la compravendita di asset prima che si renda pubblica una notizia in grado di incidere sul prezzo di scambio dei valori virtuali sulle maggiori piattaforme di *exchange.*

[175] La disposizione, di recente modificata dal D. Lgs. n. 10 agosto 2018, n. 107, incrimina chi, essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio: *«a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni medesime; b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio o di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento (UE) n. 596/2014; c) raccomanda o induce altri, sulla base di esse, al compimento di taluna delle operazioni indicate nella lettera a)».*

Parimenti, l'art. 185 TUF[176] descrive le condotte di manipolazione informativa e manipolazione operativa facendo rifermento alla concreta idoneità a provocare una sensibile alterazione del prezzo degli strumenti finanziari[177].

Dalla disamina svolta nei paragrafi precedenti[178] è emerso come la categoria degli strumenti finanziari abbia un campo di applicazione ristretto ai soli valori virtuali suscettibili di essere inquadrati tra i valori mobiliari *ex* art. 1, comma 1-*bis*, lett. c) TUF; per tutte le altre cripto-attività deve escludersi, in ossequio al principio di tassatività, ogni possibilità di estendere analogicamente le fattispecie poste a presidio del mercato finanziario.

L'impiego della locuzione "strumenti finanziari" all'interno degli artt. 184 e 185 TUF va inteso come un elemento normativo della fattispecie che richiama la ben precisa definizione contenuta nel Testo unico[179]. Non si deve quindi cadere nell'errore di confondere gli investimenti di natura finanziaria, che come si è visto possono assumere rilevanza per l'individuazione dei prodotti finanziari, con gli strumenti finanziari *stricto sensu*[180]. A differenza di quanto testé affermato a proposito della fattispecie di abusivismo finanziario, si deve pertanto concludere nel senso dell'impossibilità di estendere il presidio penale contro il *market abuse* alle condotte di *insider trading* e manipolazione del mercato aventi ad oggetto cripto-attività finanziarie idonee ad integrare la nozione domestica di prodotto finanziario[181].

Similmente, anche le sanzioni amministrative previste dall'art. art. 187-*bis* e seguenti del TUF presentano insormontabili ostacoli applicativi. Sebbene l'interprete non sia in questo caso costretto entro gli stretti limiti della interpretazione della legge penale, vi sono validi argomenti per escludere dal raggio d'azione dell'illecito amministrativo le condotte di abuso di informazioni privilegiate commesse sul mercato valutario virtuale. Invero, la disposizione punisce l'inosservanza dell'art. 14 del Regolamento n. 2014/596/UE che a sua volta richiama implicitamente la definizione di informazione privilegiata facente leva ancora una volta sulla nozione di "strumento finanziario".

Rimane, altresì, esclusa l'applicazione delle sanzioni amministrative comminate per la manipolazione del mercato dall'art. 187-*ter* TUF., nel testo risultante dalla recente riforma. L'illecito è oggi descritto mediante il rinvio all'art. 15 del

[176] La disposizione, anch'essa modificata da ultimo dal D. Lgs. n. 10 agosto 2018, n. 107, punisce «*chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari*».

[177] La struttura dell'incriminazione richiama quella dell'aggiotaggio (art. 2637 c.c.), dal quale però si differenzia per avere ad oggetto soltanto strumenti finanziari quotati o per i quali è stata presentata richiesta di negoziazione in un mercato regolamentato.

[178] Si vedano in particolare §§ 1.2. e 1.4.

[179] Art. 1, comma 2, TUF e Sezione C degli allegati al Testo unico.

[180] Come precisato in apertura del capitolo quella degli strumenti finanziari è una *species* del *genus*, dei prodotti finanziari sottoposta a un regime giuridico molto particolareggiato che si caratterizza per la regolazione delle sedi di negoziazione e dei soggetti abilitati a prestare servizi e attività di investimento.

[181] Si tratterebbe infatti di una applicazione elusiva del divieto di analogia in materia penale, non potendo evidentemente sostenersi che nel particolare (novero degli strumenti finanziari) sia compreso anche l'universale (categoria dei prodotti finanziari).

Regolamento 2014/596/UE, indirettamente riferito alla definizione di strumento finanziario fornita dal precedente art. 12, relativa a operazioni che possono incidere sull'offerta, sulla domanda, o sul prezzo di strumenti finanziari.

Al di là dei limiti imposti dal principio di legalità, resta il fatto che, in mancanza di una compiuta disciplina normativa, l'estensione delle sanzioni previste per gli abusi di mercato rappresenta un esito tutt'altro che prevedibile. Sarebbe dunque erroneo far leva sul diritto penale per veicolare nei consociati la consapevolezza della rilevanza finanziaria delle operazioni di emissione e scambio di valori virtuali, irrogando sanzioni esemplari a coloro che, in modo senz'altro deprecabile, hanno saputo profittare dell'inettitudine del legislatore nel regolare il fenomeno.

Decisamente preferibile la strada della regolazione settoriale, con cui si potrebbe facilmente conseguire l'obiettivo di rendere il *trading* valutario virtuale un autonomo mercato regolamentato, dotato di specifiche procedure, norme e sanzioni.

4.2. Omissioni informative e falsità in prospetto.

Il legislatore italiano ha improntato la disciplina applicabile all'offerta al pubblico di prodotti finanziari a quella che la direttiva 2003/71/CE (c.d. direttiva prospetto[182]) prescriveva per i soli strumenti finanziari. In tal modo gli oneri informativi sulla natura e sui rischi dell'investimento sono stati estesi a tutte le forme di sollecitazione del pubblico risparmio, ad esclusione dei depositi bancari o postali.

L'art. 94 TUF prevede che coloro che intendano effettuare un'offerta al pubblico debbano preventivamente pubblicare un prospetto, contenente in una forma facilmente analizzabile e comprensibile, tutte le informazioni che, a seconda delle caratteristiche dell'emittente e dei prodotti finanziari offerti sono necessarie affinché gli investitori possano pervenire ad un fondato giudizio sulla situazione patrimoniale e finanziaria, sui risultati economici e sulle prospettive dell'emittente e degli eventuali garanti, *«nonché sui prodotti finanziari e sui relativi diritti»*[183].

Nella pregressa trattazione è stato illustrato come le criptoattività possiedano spesso le caratteristiche dei prodotti finanziari[184]. L'aspettativa di un incremento di valore del capitale impiegato e la presenza di un rischio connesso all'investimento sono

[182] La direttiva è stata abrogata dal Regolamento 2017/1129/UE relativo al prospetto da pubblicare per l'offerta pubblica o l'ammissione alla negoziazione di titoli in un mercato regolamentato.

[183] Il prospetto contiene altresì una nota di sintesi la quale, concisamente e con linguaggio non tecnico, fornisce le informazioni chiave nella lingua in cui il prospetto è stato in origine redatto. Il formato e il contenuto della nota di sintesi forniscono, unitamente al prospetto, informazioni adeguate circa le caratteristiche fondamentali dei prodotti finanziari che aiutino gli investitori al momento di valutare se investire in tali prodotti (art. 94, comma 2).

[184] La definizione è infatti sufficientemente ampia da ricomprendere ogni strumento che sia idoneo alla raccolta del risparmio, purché rappresentativo di un impiego di capitale e connotato dall'attesa di un ricavo dall'operazione realizzata e dal rischio connesso alla stessa. Cfr. CARRIÈRE, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche*, cit., 34 ss.

gli elementi su cui fondare il giudizio assoggettamento delle operazioni di emissione e scambio[185] alla normativa di settore.

Ebbene, l'inquadramento tra i prodotti finanziari postula il rispetto delle disposizioni di legge – cui sopra si è fatto cenno – in materia di informazioni al pubblico, esponendo gli emittenti e gli intermediari alle conseguenze sanzionatorie connesse all'omissione e al falso in prospetto. Per l'inosservanza della disciplina dettata dall'art. 94 sono previste sanzioni amministrative pecuniarie che, nei casi più gravi, possono giungere fino a cinque milioni di euro[186]. Alcune condotte potranno assumere rilevanza penale ai sensi dell'art. 173-*bis* TUF che punisce la falsità in prospetto[187]. La disposizione, introdotta dalla legge 28 dicembre 2005 n. 262, fu successivamente modificata in sede di recepimento della direttiva 2003/71/CE[188] per includervi anche le falsità commesse nell'offerta al pubblico di prodotti finanziari[189].

Le condotte di falsa esposizione e di occultamento sono punite anche se insistono sui documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio. Queste ultime costituiscono, insieme alla sollecitazione all'investimento, una

---

[185] *Amplius*, § 1.2 e 1.4. In argomento v. anche GIRINO, *Criptovalute un problema di legalità funzionale*, cit., 24 ss. secondo cui le valute virtuali possiedono una endemica connotazione finanziaria.

[186] L'art. 191, comma 1, TUF dispone che: *«Chiunque effettua un'offerta al pubblico in violazione dell'articolo 94, comma 1, è punito con la sanzione amministrativa pecuniaria da euro venticinquemila fino a euro cinque milioni»*. Il secondo comma prevede sanzioni più tenui (da euro cinquemila fino a euro settecentocinquantamila) per chi violi *«gli articoli 94, commi 2, 3, 5, 6 e 7, 96, 97 e 101 […] ovvero le relative disposizioni generali o particolari emanate dalla Consob ai sensi degli articoli 95, commi 1, 2 e 4, 97, comma 2, 99, comma 1 […]».* L'applicazione delle sanzioni importa la perdita temporanea dei requisiti di idoneità previsti dal TUF per gli esponenti aziendali dei soggetti abilitati e dei requisiti previsti per i consulenti finanziari abilitati all'offerta fuori sede, per i consulenti finanziari autonomi e per gli esponenti aziendali delle società di consulenza finanziaria nonché l'incapacità temporanea ad assumere incarichi di amministrazione, direzione e controllo nell'ambito di società aventi titoli quotati nei mercati regolamentati o diffusi tra il pubblico in maniera rilevante e di società appartenenti al medesimo gruppo. La sanzione amministrativa accessoria ha durata non inferiore a due mesi e non superiore a tre anni.

[187] La disposizione punisce con la reclusione da uno a cinque anni chi «*allo scopo di conseguire per sé o per altri un ingiusto profitto, nei prospetti richiesti per la offerta al pubblico di prodotti finanziari o l'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, con l'intenzione di ingannare i destinatari del prospetto, espone false informazioni od occulta dati o notizie in modo idoneo a indurre in errore i suddetti destinatari*». Trattasi di un reato di pericolo concreto posto a presidio della trasparenza finanziaria in via strumentale rispetto alla tutela dell'interesse patrimoniale degli investitori e del risparmio collettivo. In dottrina, v. SGUBBI F., *Il falso in prospetto*, in GALGANO F., ROVERSI MONACO F., *Le nuove regole del mercato finanziario*, Padova, 2009, 649 ss.; ID., *Il falso in prospetto*, in SGUBBI F., FONDAROLI D., TRIPODI A.F., *Diritto penale del mercato finanziario*, Padova, 2013, 277 ss.; SEMINARA S., *Nuovi illeciti penali e amministrativi nella legge sulla tutela del risparmio*, in *Dir. pen. proc*., 2006, 549 ss.; ZANNOTTI R., *Il nuovo diritto penale dell'economia*, Milano, 2017, 380 ss.; SALERNO A., *Il nuovo falso in prospetto*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M., Diritto penale dell'economia, Milano, 2016, 453 ss.

[188] L'art. 4 del D. Lgs. n. 51/2007 ha modificato l'art. 173-*bis* sostituendo l'originario riferimento alla *«sollecitazione all'investimento»* con la locuzione *«offerta al pubblico di prodotti finanziari»*.

[189] Più precisamente per offerta al pubblico di prodotti finanziari deve intendersi «*ogni comunicazione rivolta a persone, in qualsiasi forma e con qualsiasi mezzo, che presenti sufficienti informazioni sulle condizioni dell'offerta e dei prodotti finanziari offerti così da mettere un investitore in grado di decidere di acquistare o di sottoscrivere tali prodotti finanziari, incluso il collocamento tramite soggetti abilitati*» (art. 1, comma, 1, lett. t).

delle due forme dell'appello al pubblico risparmio presenti nel nostro ordinamento. Il Testo unico aveva inizialmente realizzato una netta separazione tra la disciplina delle offerte di vendita e quella delle offerte di acquisto e scambio, escludendo queste ultime dalla definizione di "sollecitazione all'investimento" e formulando in proposito regole del tutto distinte[190]. Con l'emanazione del D. Lgs. 51/2007 la linea di confine si è fatta più labile, poiché l'ampio concetto di "offerta al pubblico di prodotti finanziari" sembrerebbe *prima facie* poter accorpare le due tipologie d'offerta. Ciononostante, l'espresso riferimento al fatto di *«acquistare o di sottoscrivere […] prodotti finanziari»,* contenuto nella definizione sopra citata[191], riconduce la nuova categoria nel perimetro della sollecitazione all'investimento. Sembra dunque ragionevole ammettere che le offerte al pubblico di scambio e di acquisto di prodotti finanziari siano escluse dall'ambito applicativo dell'art. 173-*bis* TUF. Da ciò derivano conseguenze significative in punto di responsabilità degli intermediari del mercato valutario virtuale. La rilevanza penale delle condotte di falso in prospetto andrà circoscritta alle sole offerte pubbliche di vendita (sollecitazione in senso proprio) di cripto-attività finanziarie, mentre andranno esenti da pena quelle commesse nelle comunicazioni che accompagnano le offerte pubbliche di acquisto o di scambio[192].

La precisazione appare tutt'altro che superflua, considerato che le maggiori piattaforme di *exchange* si limitano a prestare servizi di cambio tra valori virtuali e soltanto una esigua minoranza converte moneta avente corso legale per Bitcoin o altra valuta. Anche la vendita di cripto-attività di nuova emissione (ICO) è a stretto rigore una offerta pubblica di scambio: i neo-coniati *token* vengono infatti attribuiti in cambio

[190] Cfr. ANNUNZIATA, *La disciplina del mercato mobiliare*, cit., 294 ss., richiamato da BRUNO F., ROZZI A., *Dalla sollecitazione all'investimento all'offerta al pubblico di prodotti finanziari: una prima riflessione sul recepimento della Prospectus Directive nel mercato dei capitali italiano*, in *Giurisprudenza commerciale*, 2008, 2, 281. Nella sollecitazione all'investimento agli oblati viene proposto di trasferire all'offerente una somma di danaro in cambio di prodotti finanziari già sul mercato (*offerta pubblica di vendita*) o da immettere sul mercato (*offerta pubblica di sottoscrizione*), mentre nell'offerta pubblica di acquisto o scambio viene proposto agli oblati di ricevere danaro in cambio dei prodotti finanziari dagli stessi posseduti (*offerta pubblica d'acquisto*) o di ricevere altri prodotti finanziari in cambio di quelli che l'offerente si impegna ad acquistare (*offerta pubblica di scambio*). Delle due categorie d'offerta la prima presenta un grado di rischio maggiore per l'investitore che trasferisce un valore liquido e certo (una somma di danaro) in cambio di un prodotto finanziario di valore non altrettanto certo; nel secondo caso il risparmiatore riceve invece una prestazione certa in cambio di un prodotto finanziario di più incerto valore (offerta di acquisto) o quanto meno opera uno scambio fra beni di valore non certo.

[191] L'intenzione del legislatore di assoggettare la sola offerta pubblica di vendita all'obblighi informativi di cui al titolo II (art. 94 ss.) emerge chiaramente anche dalla lettura dell'art. 95-*bis* che, riconosce all'oblato il diritto di revoca dell'acquisto o della sottoscrizione, nel caso in cui il prospetto non indichi le condizioni o i criteri in base ai quali il prezzo di offerta definitivo e la quantità dei prodotti da offrirsi al pubblico sono determinati.

[192] L'art. 101-*bis* TUF prevede inoltre che, nelle offerte pubbliche di acquisto o di scambio, le disposizioni che pongono a carico dell'offerente specifici obblighi informativi nei confronti dei dipendenti o dei loro rappresentanti non si applicano alle offerte pubbliche di acquisto o di scambio aventi ad oggetto prodotti finanziari diversi dai titoli. La Consob può inoltre individuare con regolamento le offerte pubbliche di acquisto o di scambio, aventi ad oggetto prodotti finanziari diversi dai titoli, da non sottoporre alla disciplina della OPA e della OPSC, ove ciò non contrasti con l'esigenza di tutela dell'investitore e con efficienza e la trasparenza del mercato.

di valuta virtuale (BTC, ETH etc.), mentre soltanto in rare occasioni l'offerente accetta in pagamento denaro o altro mezzo di pagamento.

L'inquadramento dei valori virtuali nella categoria dei prodotti finanziari non è dunque risolutiva di ogni problema, se solo si considera che le disposizioni del Testo unico in materia di prospetto potrebbero nella maggioranza dei casi – secondo la tesi che qui si sostiene – rivelarsi inefficaci.

Non a caso la Consob ha più volte sottolineato[193], proprio con riferimento alle offerte di scambio, che *«al fine di evitare che la scelta dell'emittente di non predisporre un prospetto/documento di offerta per l'operazione di scambio finisca per tradursi in limitazioni fattuali dei diritti dei portatori dei titoli oggetto dello scambio»* alcune informazioni dovrebbero essere portate all'attenzione degli investitori. Tenuto conto che la relazione tra l'emittente/offerente e l'investitore al dettaglio non è di tipo diretto ma transita di norma per un intermediario che svolge una funzione di filtro nell'interesse del risparmiatore, l'Autorità ritiene che in presenza di un'operazione di scambio per la quale non sia stato pubblicato un prospetto/documento d'offerta sussiste, in ogni caso, il dovere dell'intermediario che svolge per il proprio cliente il servizio accessorio di custodia e amministrazione titoli, di operare in modo che i clienti siano sempre adeguatamente informati[194]. Un simile principio dovrebbe operare, *mutatis mutandis*, anche con riferimento all'attività svolta dai cambiavalute virtuali e dagli operatori di *trading* di cripto-attività; non si vede infatti per quale ragione tali operatori debbano essere sollevati dall'onere informativo in operazioni caratterizzate da un'alta rischiosità dell'investimento e dall'elevata volatilità del prezzo dei valori.

Occorre comunque evidenziare anche in questa sede l'opportunità di un intervento del legislatore al fine di adeguare il quadro normativo vigente alle peculiarità delle nuove frontiere della tecnofinanza; sarebbe del resto decisamente poco auspicabile che una materia così delicata fosse rimessa alla prassi applicativa, in assenza di una solida base legislativa. L'inapplicabilità delle sanzioni per l'inosservanza della disciplina in materia di prospetto suggerisce inoltre prestare attenzione alla predisposizione di fattispecie *ad hoc* per le omissioni e le falsità commesse nelle comunicazioni agli investitori.

5. Prospettive *de iure condendo*. L'assoggettamento dei valori virtuali alla disciplina finanziaria e i riflessi sul versante sanzionatorio.

L'impiego dei valori virtuali come capitale di investimento rappresenta ormai un *leitmotiv* della c.d. economia della *blockchain*. Se si volessero ricercare i motivi per cui

[193] Comunicazione n. DIN/DCG/DSR/11085708 del20-10-2011, *Offerte di scambio non assistite da prospetto e dovere degli intermediari di informare i propri clienti*, in https://consob.it

[194] Così conclude la citata comunicazione: *«Deve, infatti, ritenersi che informare il portatore di un titolo oggetto di un'operazione di scambio dell'esistenza dell'iniziativa stessa, delle sue caratteristiche e delle conseguenze che può comportare per l'investimento interessato, rientri fra i doveri dell'intermediario di protezione dell'interesse del cliente e non determini di per sé alcuna ipotesi di offerta al pubblico»* (pag. 3).

una tecnologia concepita per la disintermediazione dei pagamenti abbia avuto un così grande successo nella dimensione finanziaria, alcune ragioni risulterebbero palesi.

La tendenza deflazionistica dei valori induce gli operatori a trattenere o a cedere le attività in base alle aspettative di andamento del mercato[195]. L'emissione di una quantità predeterminata di circolante rappresenta un chiaro ostacolo all'utilizzo delle valute virtuali come mezzo di pagamento, poiché accresce il connotato finanziario delle operazioni e alimenta le aspettative di un incremento del prezzo di scambio nel breve periodo. Il mercato è tuttavia avvolto da opacità e da profonde asimmetrie informative tra professionisti e consumatori, dovute alla mancanza di requisiti normativi e di controlli da parte delle autorità statali. All'aspettativa degli investitori di un ritorno finanziario dell'investimento si accompagna una ridotta percezione dei rischi per il capitale investito e, soprattutto, la totale assenza di garanzie sul rimborso del capitale, sull'affidabilità dell'intermediario, sull'andamento del progetto finanziato.

La necessità di regolare queste nuove forme di investimento si fa sempre più pressante, di pari passo con la crescita del *trading* valutario virtuale e la creazione di nuovi modelli di *business* basati sulla tecnologia a registro distribuito. L'analisi svolta in questo capitolo ha messo in luce come l'estensione delle categorie e degli istituti tipici del diritto dei mercati finanziari non sia affatto "l'uovo di Colombo" delle svariate criticità sollevate dall'offerta di cripto-attività finanziarie. Che siano esse assimilabili a "prodotti" o "strumenti finanziari", oppure vengano considerate un *quid novi*, si ritiene che un intervento del legislatore per disciplinare in modo organico la materia sia decisamente necessario.

L'assoggettamento alla disciplina dell'intermediazione finanziaria risulta oggi un esito declinabile in via interpretativa secondo parametri decisamente elastici – per non dire discrezionali – con tutto ciò che ne deriva sul piano della certezza del diritto e dell'efficacia conformativa delle scelte imprenditoriali dei privati[196]. Per questo motivo si auspica nella compiuta definizione delle caratteristiche proprie delle "cripto-attività" finanziarie, dei requisiti dei soggetti emittenti e degli intermediari, delle informazioni da rendere pubbliche, e dei poteri delle autorità pubbliche di vigilanza.

L'intervento del legislatore sortirà effetti positivi sulla tutela della stabilità e dell'integrità del mercato finanziario, ampliando gli orizzonti applicativi delle fattispecie di reato previste dal TUF. Risulterebbe anzitutto più chiara e prevedibile la responsabilità per abusivismo finanziario *ex* art 166 nelle ipotesi di esercizio non autorizzato di servizi e attività di investimento. A tal fine sarebbe sufficiente un adeguamento della fattispecie per includervi anche l'inosservanza delle emanande disposizioni sull'emissione e lo scambio di cripto-attività[197].

---

[195] In tal modo gli investitori privati sono portati a detenere per lungo tempo l'*asset* sperando in una sua rivalutazione. *Amplius*, in questo capitolo, § 1

[196] Sulla differenziazione della disciplina applicabile in base alle differenti tipologie di *token*, *supra* § 1.4.

[197] Sul punto, v. § 3.3.

In linea con l'esigenza di tutela degli investitori si pone la necessità di stigmatizzare possibili condotte di abuso commesse sul mercato valutario virtuale. La presenza di una vasta zona franca da responsabilità, penale e amministrativa, dovuta all'inerzia del legislatore nel disciplinare il fenomeno, non giova affatto alla crescita del Fintech. La riconosciuta impossibilità di reprimere le ipotesi di *market abuse* facendo leva sulle vigenti fattispecie di abuso di informazioni privilegiate e di manipolazione del mercato evidenzia l'esistenza di una falla nel sistema, che rende ancor più debole la posizione dell'investitore al cospetto degli operatori del settore. Si auspica dunque che nell'ambito di un più organico intervento riformatore, il legislatore possa dedicare la giusta attenzione alla trasparenza del mercato e alla repressione di condotte di indebita interferenza sul meccanismo della formazione dei prezzi[198].

Risulta parimenti indispensabile la previsione di norme di dettaglio sulle procedure di approvazione e sui contenuti del prospetto informativo. La disciplina dettata dagli artt. 94 ss. TUF per l'offerta al pubblico di prodotti finanziari non pare infatti applicabile *de plano* ai servizi offerti dalle maggiori piattaforme di *exchange*[199]; così anche il presidio sanzionatorio contro le omissioni e le falsità informative viene meno, accrescendo ulteriormente la già vistosa opacità del mercato valutario virtuale.

[198] Si veda, in questo capitolo, § 4.
[199] *Amplius*, § 4.2.

CAPITOLO V

INVESTIGAZIONI INFORMATICHE, *BLOCKCHAIN FORENSICS* E PROCESSO PENALE

SOMMARIO: 1. Introduzione. – 2. La transnazionalità degli illeciti configurabili. La necessità di strategie di cooperazione internazionale e di coordinamento investigativo. – 2.1. Iniziative per una *partnership* pubblico-privato. – 3. Trasferimento illecito di fondi: una esemplificazione operativa. – 4. Mezzi di ricerca della prova e sequestro probatorio di dati e programmi informatici. – 5. *Blockchain forensics* e *Open Source Intelligence*. – 5.1 Tra *publicly available data* e *legitimate expectation of privacy*. Considerazioni in ordine alla necessità di una base normativa per le indagini OSINT. – 5.2. Indagini *open source* e protezione dei dati personali nelle attività di contrasto. – 6. Gestione accentrata di fondi: gli *exchange provider* e l'acquisizione della prova digitale. – 7. Sequestro e confisca di valuta virtuale. 7.1. *Key disclosure laws* e diritto al silenzio. – 7.2. Uno sguardo ai sistemi di *common law*. Il modello britannico. – 7.3. L'esperienza statunitense. – 8. Lo strumentario processuale sul banco di prova delle valute virtuali. Luci, ombre e prospettive di riforma.

1. Introduzione.

La diffusione della tecnologia a registro diffuso e, in particolare, il trasferimento di valuta virtuale per il suo tramite, hanno mutato profondamente la fenomenologia di alcune attività criminose. Ciò pone problemi di grande spessore non solo sul *piano sostanziale* – guardando alla tipicità di alcune condotte e all'individuazione di nuove oggettività meritevoli di tutela penale – ma anche *sul piano processuale*, sotto il profilo della cooperazione investigativa, dell'acquisizione della prova in ambito informatico, delle misure di ablazione patrimoniale aventi ad oggetto valori virtuali. In un quadro normativo del tutto privo di regole, l'interprete è tenuto ad un costante sforzo ermeneutico per far quadrare gli istituti previsti dal codice di rito in una realtà nuova e in costante evoluzione.

Le difficoltà applicative sono riconducibili, in linea di massima, ad un fattore su tutti: la disintermediazione. L'assenza di un una Autorità centrale e di terzi incaricati della gestione del protocollo informatico che regola le transazioni, determina la crisi degli strumenti di indagine che si "adagiano" sulla collaborazione del *service provider*. La ricerca e l'acquisizione della prova digitale passano costantemente per la mano dei fornitori del servizio, gravati da obblighi di *data retention* o di collaborazione con l'autorità giudiziaria. Allo stesso modo, l'imposizione di misure cautelari nel cyberspazio, prima fra tutte il sequestro-oscuramento del sito *web*, è resa possibile dalla presenza degli *access provider* che si frappongono tra il sistema telematico dell'utente e il sito che questi intende visitare.

Nei trasferimenti che avvengono per il tramite di *blockchain* pubbliche totalmente decentralizzate il ricorso a questi strumenti è, sia sul versante probatorio, sia su quello cautelare, tecnicamente impossibile. Manca infatti l'intermediario della gestione delle transazioni, quale che ne sia la natura (trasferimento di valuta virtuale, esecuzione di un contratto *smart*, registrazione del trasferimento di un *asset* etc.). Inoltre, l'utilizzo della crittografia costituisce un serio ostacolo all'individuazione dell'utente persona fisica che ha disposto l'operazione o che ne ha beneficiato.

Nel complesso, si avverte quindi la necessità che lo strumentario investigativo tradizionale sia integrato da nuove e sofisticate tecniche di *intelligence*[1], e che le varie tipologie di sequestro previste dal codice di rito siano eseguite con modalità peculiari. L'insieme delle regole procedimentali e delle tecniche di analisi del registro pubblico delle transazioni prende il nome di *blockchain forensics*. Tale disciplina ha assunto una autonoma dignità scientifica rispetto al *genus* dell'informatica forense, differenziandosene non soltanto per l'oggetto, ma anche per il metodo d'indagine.

In quest'ambito l'attività dell'informatico forense consiste nell'individuare le transazioni oggetto dell'illecito per fare applicazione di regole euristiche che consentano di aggregare più indirizzi e di capire quali di essi appartengono alla stessa persona e quali invece siano controllati dagli *exchange server*, a cui chiedere informazioni sull'identità dell'indagato e sulle attività compiute sulla piattaforma di scambio[2].

L'analisi svolta in questo capitolo vuole fornire al lettore un quadro d'insieme delle questioni più problematiche che la tecnologia a registro diffuso solleva sul piano processuale. Alcune premesse di carattere sostanziale e metodologico ci sembrano indispensabili per una corretta esposizione dei temi oggetto d'indagine.

Una prima riguarda i reati per i quali, più comunemente, si avverte l'esigenza di ricorrere a tecniche di *blockchain forensics*. Si tratta di illeciti caratterizzati da una marcata componente economico-patrimoniale. Un chiaro esempio è dato dalle nuove frontiere del riciclaggio che, come si è avuto modo di esaminare in precedenza, si collocano sempre più spesso nella dimensione dell'economia virtuale[3]. Seguendo lo schema tipico del riciclaggio, l'acquisto e il trasferimento di *token* e *asset* virtuali

[1] Per una applicazione delle tecniche di *intelligence* al Bitcoin v. SPAGNUOLO M – MAGGI F. – ZANERO S., *BitIodine: Extracting Intelligence from the Bitcoin Network,* in AA. VV., *Financial Cryptography and Data Security,* Heidelberg, 2014, 457 ss.; per una applicazione alla *blockchain* di Ripple v. MORENO-SANCHEZ P. – BILAL ZAFAR M., *Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network*, in *Proceedings on Privacy Enhancing Technologies*, 2016, 4, 436 ss.; per una applicazione all'infrastruttura di Monero, MÖSER M. – SOSKA K., *An Empirical Analysis of Traceability in the Monero Blockchain*, in *Proceedings on Privacy Enhancing Technologies*, 2018, 3, 143 ss.

[2] Sul punto, di recente BISTARELLI S., *Bitcoin forensics: le tecniche labeling, clustering e mixnet recognition,* in *Agenda Digitale*, 10 aprile 2018, a proposito delle attività svolte dal cybersecurity Lab istituito presso l'Università degli studi di Perugia. Per una disamina delle tecniche investigative che si basano sull'analisi del registro pubblico delle transazioni, *infra* § 5).

[3] Sul tema di recente PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2018, 3-4, 590 ss.; SICIGNANO G. J., *Bitcoin e riciclaggio*, Torino, 2019, 108 ss. *Supra*, Cap. III, § 3.

possono essere considerate azioni prodromiche al *consolidamento* della ricchezza nelle mani del reo, finalizzate cioè al rientro dei proventi delittuosi nel circuito dell'economia lecita. Le potenzialità criminogenetiche delle valute virtuali[4] derivano anche dal loro utilizzo quale mezzo di pagamento sulla rete per l'acquisto di beni e servizi, accettato da un numero sempre maggiore di utenti[5]. La pseudonimizzazione delle transazioni e l'assenza di intermediari rendono queste valute lo strumento di scambio prediletto dai criminali per ottenere prestazioni illecite[6] o per finanziare attività delittuose.[7]

Da tale assunto conviene partire per circoscrivere il tema oggetto del nostro approfondimento ai crimini informatici determinati da fini di lucro[8]. Non perché, beninteso, la necessità di far uso di tecniche di *blockchain forensics* non si ponga anche per reati che offendono beni diversi dal patrimonio[9], ma soltanto per la dimensione assolutamente preponderante dell'impiego della tecnologia a registro diffuso quale strumento di scambio di valori virtuali.

Una seconda premessa è rivolta al metodo d'indagine. Per ragioni di economia espositiva, ci limiteremo ad esaminare gli istituti processuali assumendo a base del ragionamento una transazione eseguita sulla *blockchain* di Bitcoin. Tale approssimazione – che all'apparenza potrebbe sembrare semplicistica, tenuto conto dell'elevato numero di sistemi decentralizzati esistenti al giorno d'oggi – non sarà d'ostacolo al raggiungimento dell'obiettivo prefissato. *In primis*, perché la rete Bitcoin

[4] Di recente, SEVERINO P., *Sicurezza informatica e prevenzione del cybercrime*, in *LuissOpen*, 8 settembre 2017, 11

[5] Sulle ragioni del crescente impiego delle valute virtuali non pare necessario soffermarsi, essendo stati abbondantemente esposti in precedenza (v. Cap. II, § 1.2.).

[6] Per una indagine sull'impiego delle criptovalute sui *criminal markets* nel *darknet* e sulle forme di finanziamento diretto e indiretto del terrorismo, si veda il nuovo *Internet Organised Crime Threat Assessment* (IOCTA 2018) redatto dall'*European Cybercrime Center* (EC3) e disponibile sul sito istituzionale di Europol. I dati del penultimo ultimo resoconto, relativo all'anno 2017, già evidenziavano un rapporto di diretta proporzionalità tra l'aumento di capitalizzazione del mercato delle criptovalute e lo sviluppo del *cybercrime*, specialmente con riferimento alle condotte di diffusione di *ransomwares* e al dilagare sulla parte oscura della rete di *criminal markets* per la compravendita di droga, armi, materiale pedopornografico etc.

[7] Cfr. BRILL A. – KEENE L., *Cryptocurrencies: The Next Generation of Terrorist Financing?*, in *Defence Against Terrorism Review*, 2014, 6, 7 ss

[8] Sulle recenti evoluzioni della cyber-criminalità economica e sullo sviluppo delle tecniche investigative si veda il report pubblicato dall'Università di Cardiff *«The Implications of Economic Cybercrime for Policing»* disponibile al seguente link http://orca.cf.ac.uk/

[9] Per il tramite della *distributed ledger technology* è possibile commettere qualsiasi reato eventualmente informatico (reato informatico in senso lato). Anzi, è ragionevole ritenere che, con il progressivo ampliamento delle applicazioni pratiche di tale tecnologia, saranno sempre maggiori le fattispecie criminose astrattamente configurabili. Si pensi ad esempio alla condivisione di notizie su una infrastruttura che, tramite un sistema di *rating* decentrato, indicizzi le notizie giornalistiche per distinguerle dalle *fake news*. In un ecosistema di questo tipo si potrebbero diffondere, aumentandone la visibilità, anche notizie di cui sia vietata la divulgazione (artt. 261, 262, 621 c.p.). Sulla distinzione tra reati informatici in senso stretto e in senso lato, PICOTTI L., *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec*., 2011, 4, 827 ss.; FLOR R., *Cyber-criminality: Finding a Balance between Freedom and Security*, nella raccolta di scritti del convegno *Cybercrime: Global Phenomenon and its Challenges*, tenutosi a Courmayeur il 2-4 dicembre 2011, pubblicata sul sito International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC), 13 ss.

vanta il primato indiscusso in termini di volume delle transazioni e di capitalizzazione del mercato. In secondo luogo, perché i principi alla base del funzionamento tecnico del sistema informatico sono gli stessi: ciò significa che, almeno in linea di massima, le tecniche investigative si fondano su basi comuni, salve le divergenze dovute dal protocollo di codifica proprio di ciascuna infrastruttura[10].

Date tali premesse di ordine metodologico, possiamo ora esaminare da vicino le numerose questioni che si pongono sul piano processuale penale. La prima parte della trattazione ha ad oggetto le strategie di coordinamento investigativo e di cooperazione giudiziaria a livello sovranazionale, che appaiono indispensabili per far fronte all'elevato grado di complessità delle indagini e alla dimensione spesso transnazionale della cybercriminalità economica.

La seconda affronta le questioni più spinose, che riguardano il versante probatorio e quello delle misure cautelari reali esperibili in caso di sospetto di commissione degli illeciti *de quibus*.

Riserveremo alla parte finale le considerazioni critiche *de iure condendo*, soffermandoci sull'opportunità di una riforma del codice di procedura penale per far fronte ad alcune criticità emergenti.

2. La transnazionalità degli illeciti configurabili. La necessità di strategie di cooperazione internazionale e di coordinamento investigativo.

Gli illeciti commessi in rete si caratterizzano per la dimensione essenzialmente transnazionale, derivante dalla riconosciuta aterritorialità del cyberspazio[11]. Ciò ha condotto gli Stati e le organizzazioni internazionali a intraprendere numerose iniziative per porre un argine al dilagare della criminalità informatica. Senza entrare nel merito dell'evoluzione normativa, è qui sufficiente ricordare che, sul piano sovranazionale, la lotta contro il crimine informatico si è incardinata su tre fronti: la creazione di un base legale comune nella definizione degli illeciti; la cooperazione tra autorità giudiziarie; il coordinamento investigativo e la mutua assistenza nelle attività d'indagine.

L'armonizzazione delle disposizioni di diritto penale sostanziale garantisce agli Stati una base giuridica comune per la lotta al *cybercrime*. Diversamente, i criminali informatici si gioverebbero dell'esistenza di asimmetrie e di sacche di impunità nelle legislazioni di alcuni Paesi. La creazione di canali di comunicazione tra autorità giudiziarie e agenti di polizia assicura un rapido e costante scambio di informazioni,

[10] Le tecniche di identificazione basate sull'analisi del registro pubblico delle transazioni divengono più complicate per alcune infrastrutture che consentono agli utenti di scambiare valori in modo totalmente anonimo. Sulla deanonimizzazione dei trasferimenti su Monero v. MÖSER – SOSKA, *An Empirical Analysis of Traceability in the Monero Blockchain*, cit., 148

[11] In argomento, SEVERINO P., *Sicurezza informatica e prevenzione del cybercrime*, cit.,11; PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 26; FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc.*, 2015, 10, 1296.

garantisce il rispetto e l'esecuzione delle decisioni giudiziarie, contribuisce alla creazione di *unit* trasversali per lo svolgimento di investigazioni complesse, favorisce lo scambio di *expertise* tecnica.

Tra le istituzioni internazionali, quella che ha raggiunto i traguardi più significativi in quest'ambito è senza dubbio il Consiglio d'Europa. Dopo aver adottato, in tempi ormai passati, una celebre Raccomandazione *«sur la criminalitè avec l'ordinateur»*[12], l'avvento della Convenzione di Budapest sul *cybercrime*[13] ha segnato un nuovo corso nella lotta alla criminalità informatica. Il trattato rappresenta oggi la stella polare dell'armonizzazione legislativa e della cooperazione internazionale a livello globale[14].

Nel delineare i principi del coordinamento investigativo per la raccolta della *digital evidence*, la Convenzione disciplina la mutua assistenza tra Stati, a partire da meccanismi tradizionali come l'estradizione (art. 24) fino a giungere a soluzioni innovative quali la richiesta di conservazione o divulgazione rapida di dati (artt. 29 ss.) e l'accesso transfrontaliero a *files* immagazzinati (art. 32)[15]. Queste ultime due soluzioni si affidano all'attività dei fornitori di servizi telematici (*provider*), sempre più spesso destinatari di obblighi di collaborazione, consegna e conservazione dei dati. Nel prosieguo della trattazione si darà conto importanza centrale che gli *exchange provider* assumono nella raccolta della prova e nel sequestro di valuta virtuale.

A livello eurounitario, l'estensione delle competenze in materia penale *post* Trattato di Lisbona ha gettato le basi per l'adozione della direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione[16]. Sul piano processuale, la direttiva disciplina il solo scambio di informazioni (art. 13), affidando ad altri strumenti

[12] Il riferimento è alla Raccomandazione del Consiglio d'Europa del 13 settembre 1989. In argomento, PECORELLA C., *Diritto penale dell'informatica,* Padova, 2006, 7 ss.; PICOTTI L., *L. 23 dicembre 1993, n. 547. Commento all'art. 8 l. 23 dicembre 1993, n. 547*, in *Leg. pen.*, 1996, 1-2, 129 ss.; ID., *La "Raccomandazione" del XV Congresso Internazionale di diritto penale in tema di criminalità informatica,* in *Riv. trim. dir. pen. econ.*, 1995, 4, 1279 ss.

[13] Per un commento, PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa – Profili sostanziali*, in *Dir. pen. proc.*, 2008, 6, 700 ss.; LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa – Profili processuali*, in *Dir. pen. proc.*, 2008, 6, 717 ss.; SARZANA DI S. IPPOLITO C., *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. proc*, 2008, 12, 1562 ss. Nella letteratura straniera, per tutti, CLOUGH J., *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, in *Monash University Law Review*, 2014, vol. 40, 3, 698 ss.

[14] Al trattato hanno aderito moltissimi Stati che non sono membri del Consiglio d'Europa, tra cui *ex plurimis* Stati Uniti, Canada, Australia, Argentina, Giappone, Sud Africa. Per appronfondimenti, CLOUGH J., *Principles of cybercrime*, Cambridge, 2015, 23 ss.

[15] Cfr. LUPARIA, *La ratifica della Convenzione Cybercrime*, cit., 718

[16] La direttiva 2013/40/UE ha sostituito la decisione quadro 2005/222/GAI del Consiglio. Il catalogo delle condotte da incriminare ricalca la parte sostanziale della convenzione di Budapest, ma fa riferimento ai soli reati informatici in senso stretto (accesso abusivo, interferenza illecita relativamente ai dati e ai sistemi, intercettazione illecita). Sulla evoluzione del diritto penale europeo nel contrasto alla criminalità informatica, si veda SUMMERS S. – SCHWARZENEGGER C. – EGE G. – YOUNG F., *The Emergence of EU Criminal Law. Cyber-crime and the regulation of the information society*, Oxford, 2014, 85 ss.

legislativi la disciplina della cooperazione giudiziaria e del coordinamento investigativo in materia[17].

Tanto premesso, rivolgiamo ora lo sguardo al tema oggetto del presente lavoro. La disintermediazione degli scambi attraverso un sistema di pagamento *peer-to-peer* segna il superamento dello statualismo monetario. In tal senso le valute virtuali sono state concepite, *by design*, come mezzo universale di pagamento, talvolta slegato dai valori e dall'andamento dell'economia reale[18]. Alcuni ecosistemi sono stati progettati – e cominciano ad essere impiegati – per regolare rimesse di dare e avere tra istituzioni finanziarie operanti a livello internazionale[19]. Inoltre, la quasi totalità degli ecosistemi decentralizzati si articola lungo una pluralità di nodi, fisicamente collocati su *server* sparsi in varie parti del globo.

Balza dunque all'evidenza che qualsiasi attività illecita che sfrutti le potenzialità della tecnologia a registro diffuso avrà per definizione una dimensione transnazionale. Lo scenario è assai variegato. Una transazione illecita può intercorrere (i) tra indirizzi appartenenti a utenti residenti in diversi Stati; (ii) tra indirizzi di utenti residenti in diversi Stati o nel medesimo Stato, che si avvalgono dell'intermediazione di piattaforme di scambio che hanno sede legale in uno Stato terzo; (iii) tra indirizzi di utenti residenti nel medesimo Stato, sfruttando un protocollo di codifica che richiede la previa validazione da parte di una qualificata percentuale di nodi dell'ecosistema. In ciascuna di queste ipotesi l'azione delittuosa si realizza almeno in parte all'estero; ma anche laddove l'intero *iter criminis* fosse circoscritto ai confini nazionali[20], gli organi inquirenti non potranno prescindere l'attivazione di canali di cooperazione internazionale per la ricerca della prova o per l'esecuzione misure cautelari (quali il

[17] Tra le più rilevanti, la decisione quadro 2002/584/GAI relativa al mandato di arresto europeo; la decisione 2002/187/GAI modificata dalla decisione 2009/426/GAI sui compiti della l'Agenzia per la cooperazione giudiziaria penale (Eurojust); la direttiva 2014/41/UE relativa all'ordine europeo di indagine penale; il Regolamento 2016/794/UE che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol); la direttiva 2017/1371/UE sul funzionamento dell'Ufficio della Procura europea. Alla data di stesura del presente scritto sembra prossimo all'adozione la proposta di Regolamento sul funzionamento di Eurojust, presentata in prima lettura dalla Commissione nel 2013 (COM/2013/0535- 2013/0256).

[18] Per riflessioni sul rapporto tra economia reale e virtuale, di recente, DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, in *Dir. pen cont. – Riv. trim*, 2018, 9, 87; MAJORANA D., *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in *Corr. Trib*., 2018, 8, 630.

[19] Ad esempio, il protocollo Ripple è stato creato per agevolare le rimesse interbancarie, eliminando i costi di transazione e riducendo a pochi secondi i tempi di accredito. In argomento, ORCUTT M., *No, Ripple Isn't the Next Bitcoin*, in *MIT Technology Review – Web*, 11 gennaio 2018, 1.

[20] Si pensi ad un caso di autoriciclaggio (art. 648-*ter1*. c.p.) che si realizzi mediante l'acquisto di valute virtuali e la successiva conversione in moneta *fiat.* Un individuo, residente in Italia, trasferisce un certo ammontare di Bitcoin, provento di reato, da un indirizzo privato a un indirizzo di cui egli ha il controllo su una piattaforma di scambio. Sull'*exchange* utilizza l'ammontare di Bitcoin depositato per l'acquisto di più valute che, dopo qualche tempo, converte in moneta *fiat* o in Bitcoin per poi reindirizzarli verso in conto corrente o un indirizzo di cui è titolare. In questo caso la condotta autoriciclativa, in base al principio di diritto affermato dalle Sezioni Unite sul luogo di commissione del reato informatico (Cass. Pen., Sez. Un., 24 aprile 2015 n. 17325, in tema di accesso abusivo a sistema informatico), si perfeziona interamente in Italia, anche se il luogo fisico in cui è localizzato il *server* ove sono custodite le chiavi crittografiche, appartenente all'*exchange provider* ma accessibile dall'Italia, si trovi all'estero.

sequestro di valuta virtuale o l'inibitoria di accesso all'*e-wallet*), posto che la quasi totalità dei fornitori di servizi di intermediazione sul mercato delle valute virtuali sono registrati o hanno *server* allocati all'estero.

L'endemica natura transnazionale dei reati che possono essere commessi per mezzo della tecnologia a registro diffuso (*DLT enabled crime*) non è sfuggita all'attenzione degli attori internazionali. Numerose sono le iniziative intraprese per far fronte a rischi connessi, in particolar modo, all'utilizzo delle valute virtuali.

Le Nazioni Unite, pur non avendo mai adottato alcuna risoluzione formale avente ad oggetto l'utilizzo a fini finanziari della *blockchain,* hanno *de facto* recepito tale tecnologia in alcuni programmi di aiuto umanitario[21]. D'altro canto, però, l'*United Nations Office on Drugs and Crime* (UNODC) ha messo in guardia sui rischi di un uso delle valute virtuali per fini di riciclaggio, avviando iniziative di formazione specifica per ufficiali di polizia giudiziaria e membri delle unità di informazione finanziaria[22]. Per supportare l'attività didattica, è stato pubblicato un manuale sulle tecniche di investigative da utilizzare per l'individuazione delle operazioni di riciclaggio commesse mediante valute virtuali[23].

Per il rafforzamento della cooperazione internazionale contro la criminalità informatica, con particolare riguardo alle procedure per l'acquisizione della *electronic evidence*, gli Stati membri del Consiglio d'Europa hanno recentemente iniziato i lavori per elaborare un testo del secondo protocollo addizionale alle Convenzione di Budapest[24]. A livello locale, sono state inoltre avviate alcune iniziative di formazione per giudici e pubblici ministeri aventi ad oggetto la ricerca, il sequestro e la confisca dei proventi del *cybercrime*. Per quel che qui interessa, nell'ambito progetto i-PROCEEDS[25] si dedica una importanza centrale ai poteri di indagine e alle misure

[21] Stando alle notizie pubblicate sul sito internet dedicato (https://un-blockchain.org, notizia del 18 giugno 2017), nell'ambito del World Food Programme per gli aiuti umanitari in Siria, le Nazioni Unite hanno utilizzato l'infrastruttura *Ethereum* per trasferire *vouchers* ad oltre 10.000 rifugiati Siriani. Altrettanto innovativa l'iniziativa dell'Unicef di creare un *software,* chiamato *Claymore* (liberamente scaricabile dal sito ufficiale https://www.chaingers.io) che consente agli utenti di giochi *online* di offrire parte dell'energia e delle risorse computazionali delle proprie schede grafiche per minare Ethereum che, periodicamente, vengono trasmessi all'indirizzo di Unicef in donazione ai bambini siriani.

[22] Di recente, nell'ambito del programma di recupero per alcune zone del Medio Oriente, è stato attivato il corso di formazione «on Investigation of Money Laundering with Cryptocurrencies and Money Transfer Systems and Electronic Money», che prevede alcuni moduli specifici sulle nuove forme di finanziamento al terrorismo islamico tramite valori virtuali.

[23] «Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies», disponibile sul sito Internet dell'*International Money Laundering Information Network* (https://www.imolin.org). Il manuale fornisce le indicazioni essenziali per un inquadramento del funzionamento, delle potenzialità e dei rischi associati alle valute virtuali. Alcuni moduli didattici sono dedicati agli strumenti investigativi e alla descrizione delle operazioni basilari da compiere per eseguire un sequestro di valuta virtuale.

[24] Lo si apprende dal comunicato stampa del 19 marzo 2018, intitolato «Towards a Protocol to the Budapest Convention», nella sezione «Protocols negotiations» del sito Internet istituzionale (https://www.coe.int /cybercrime).

[25] Il riferimento è al progetto «On targeting crime proceeds on the Internet in South-eastern Europe and Turkey» (i-PROCEEDS), per il quale è stato elaborato un manuale didattico rivolto ai magistrati inquirenti e giudicanti. La sezione V dell'opera è dedicata all'utilizzo delle valute virtuali come

cautelari che l'autorità giudiziaria può disporre per raggiungere i proventi dell'attività delittuosa nell'universo virtuale. Nel documento vengono elencate una serie di "sfide" che le autorità procedenti dovranno affrontare, alcune delle quali risultano particolarmente complesse, anche a causa delle lacune legislative presenti negli ordinamenti nazionali.

Con l'adozione della quinta direttiva antiriciclaggio[26] l'Unione Europea ha gettato le basi per l'emersione e per il contrasto delle attività di "ripulitura" commesse mediante l'utilizzo delle valute virtuali. Guardando al piano operativo, un recentissimo studio del Parlamento Europeo[27] ha sottolineato la necessità di implementare strategie di cooperazione tra istituzioni, autorità ed enti per una efficace risposta alle sfide lanciate dalle valute virtuali. Grazie all'attività svolta dall'Ufficio europeo di Polizia (Europol) nella raccolta di informazioni e nel perfezionamento dell'*intelligence analysis*, è stato possibile creare delle *taskforce* di azione per portare al termine operazioni tecnicamente molto complesse sul *darknet*, che hanno condotto alla definitiva chiusura dei mercati neri Alpha Bay e Hansa[28]. In Italia, la Polizia Postale e delle Comunicazioni in collaborazione con Europol ha disposto la chiusura di Babylon[29] e eseguito il sequestro di migliaia di *e-wallet* Bitcoin appartenenti agli utenti del *black market*. Inoltre, a partire dal 2014, l'European Cybercrime Center (EC3) istituito presso Europol esegue annualmente una valutazione sulle evoluzioni della criminalità organizzata in rete (*Internet Organised Crime Threat Assessment*, IOCTA), contribuendo a diffondere dati e statistiche sulle tecniche di attacco di maggiore attualità e diffusione.

2.1. Iniziative per una *partnership* pubblico-privato

La cooperazione tra il settore pubblico e quello privato è divenuta una e*sigenza funzionale*[30] nel campo della sicurezza informatica per almeno due ordini di motivi: la gestione della maggior parte delle infrastrutture critiche nazionali da parte di società

strumento di raccolta e trasferimento dei proventi del crimine informatico. Per approfondimenti si rinvia al sito Internet: https://www.coe.int/en/web/cybercrime/iproceeds

[26] Direttiva 2018/843/UE che modifica la direttiva 2015/849/UE «relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo». (*Amplius*, Cap. III, § 3.4.).

[27] «Virtual currencies and terrorist financing: assessing the risks and evaluating responses», studio del Dipartimento per la tutela dei diritti dei cittadini e gli affari costituzionali per la commissione "Terrorismo", disponibile sul sito Internet http://www.europarl.europa.eu, sezione "Studi", 57 ss.

[28] «Massive blow to criminal Dark Web activities after globally coordinated operation», comunicato stampa del 20 luglio 2017, su https://www.europol.europa.eu.

[29] Il mercato nero Babylon era uno dei *marketplace* più rinomati in Italia. All'atto della "chiusura" gli organi inquirenti hanno individuato oltre 170.000 messaggi relativi a trattative illecite e oltre 14.000 *hot wallet* localizzati sulla piattaforma. Per i dettagli dell'operazione, si visiti il sito Internet http://www.interno.gov.it, sezione Notizie, 31 luglio 2015.

[30] Cosi definita da MELE S., *La cooperazione tra pubblico e privato nella cyber-security*, disponibile nell'archivio del SISR (http://www.sicurezzanazionale.gov.it), 2.

privatizzate; l'utilizzo da parte dei cittadini e delle istituzioni di connessioni e dispositivi progettati e amministrati da enti privati[31].

Da un esame comparativo delle *cyber-strategy* rese pubbliche a livello europeo ed internazionale, risulta ricorrente il riferimento a indirizzi strategici relativi al rafforzamento delle *partnership* internazionali e all'*information sharing* tra il settore pubblico e quello privato[32]. Tale esigenza si manifesta, con particolare enfasi, nell'ambito delle attività di contrasto al *cybercrime*. Difatti, nella maggioranza dei casi, la prova della commissione di un delitto informatico è registrata nell'archivio dei fornitori dei servizi digitali. Di qui la necessità per le autorità inquirenti di concludere accordi con i *provider* privati per disciplinare l'accesso alle informazioni su richiesta e attivare canali di segnalazione delle operazioni sospette.

Avuto riguardo all'oggetto del presente lavoro, la realizzazione di un partenariato pubblico-privato figura tra le priorità di molte istituzioni impegnate nella lotta contro l'utilizzo delle valute virtuali per fini illeciti[33].

Tra le iniziative di maggior rilievo spicca il Progetto TITANIUM[34], istituito al fine di sviluppare strumenti *open source* per il rilevamento delle transazioni "a rischio" di riciclaggio o comunque sintomatiche dell'impiego delle valute virtuali per scopi illeciti, e di addestrare le forze dell'ordine all'uso di programmi di *cross-ledger-analysis*[35]. Un altro progetto sovvenzionato dall'Unione Europea è DANTE (*Detecting and Analisying Terrorist-related Online Content and Financing Activities*)[36] che, pur non essendo specificamente incentrato sul circolante virtuale, ha come obiettivo l'analisi delle attività di raccolta di fondi sul *darknet* per il finanziamento di attività terroristiche.

Per stabilire un contatto diretto tra le autorità inquirenti e l'industria delle criptovalute è stata costituita la Blockchain Alliance[37], un gruppo di lavoro coordinato da Europol che riunisce molti *exchange provider* e alcune società che offrono servizi

---

[31] In argomento, TROPINA T., *Public-Private Collaboration: Cybercrime, Cybersecurity and National Security*, in TROPINA T.– CALLANAN C., *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Berlino, 2015, 8 ss.

[32] Cfr. MELE S., *La cooperazione tra pubblico e privato nella cyber-security*, su https://sicurezzanazionale.gov.it, 1 dicembre 2014.

[33] In tal senso il rapporto «Virtual currencies and terrorist financing: assessing the risks and evaluating responses», cit., 60

[34] Il Progetto, avviato nel maggio 2017, è stato finanziato con i fondi Horizon 2020 dell'Unione Europea. Tra i membri figurano, oltre ai vertici dell'esecutivo di alcuni stati europei (Spagna, Germania, Finlandia), alcune università (UCL di Londra e l'Università di Innsbruck), diverse società private operanti nel settore IT, e INTERPOL.

[35] Si tratta di *software* OSINT che permettono di "incrociare" i dati presenti nei pubblici registri delle transazioni di più infrastrutture, e di seguire le tracce di flussi di valuta virtuale sulle *blockchain* delle più famose Altcoin. Per approfondimenti sulle tecniche di *open source intelligence*, v. *infra* § 5).

[36] Lo scopo del progetto è la creazione di un sistema automatizzato di estrapolazione dei dati per individuare, recuperare, collezionare ed analizzare grandi quantità di contenuti eterogenei, in formato multimediali e in lingue diverse, che siano direttamente o indirettamente collegati al terrorismo, sia nel *surface web* sia nel *dark web*. Il Partenariato ha 18 membri, appartenenti ai settori pubblico e privato, tra cui figurano anche il Ministero della Difesa italiano e l'Arma dei Carabinieri.

[37] Per approfondimenti si rinvia al sito internet istituzionale https://blockchainalliance.org

di *blockchain forensics*. Il team di Europol ha inoltre organizzato una serie di incontri periodici tra gli esponenti del mercato dei valori virtuali, per incentivare uno scambio di informazioni sulle migliori prassi di prevenzione del riciclaggio e del finanziamento del terrorismo (*AML/CFT best practices*).

Tra gli accordi siglati da Europol con il settore privato si ricorda, da ultimo, anche la *partnership* con il Basel Institute on Governance[38] che rappresenta un buon esempio di raccordo e *information sharing* tra autorità investigative e accademia.

Le iniziative finora descritte evidenziano come la realizzazione di un partenariato pubblico-privato sia uno dei primi punti all'agenda delle istituzioni sovranazionali e dei governi nazionali.

Per quanto auspicabile, essa non fornisce però la soluzione a tutti i problemi. In un recente studio del Parlamento Europeo[39] si esprime grande preoccupazione per la mancanza di esperti nel settore *blockchain* nei ranghi delle autorità di polizia, evidenziando come, negli Stati membri, la competenza in materia di valute virtuali sia spesso concentrata tra pochi esperti autodidatti[40]. Pertanto, nel prossimo futuro, ci si attende che la *partnership* tra settore pubblico e privato sia convogliata verso iniziative di formazione e di diffusione della cultura e delle competenze tecnico-gestionali in materia *blockchain*.

3. Trasferimento illecito di fondi: una esemplificazione operativa.

Un trasferimento di fondi *peer to peer* presenta caratteristiche peculiari, che incidono notevolmente sulle tecniche di acquisizione della prova e sulle modalità di apprensione della ricchezza. L'uso della crittografia rende complicato risalire agli autori della transazione, che figurano sul registro con lo "pseudonimo" del loro indirizzo di portafoglio[41].

Prima di entrare nel merito dell'approfondimento, vogliamo fornire al lettore una esemplificazione delle diverse fasi che caratterizzano un trasferimento di valuta virtuale[42]. Ciò renderà più agevole l'illustrazione delle diverse questioni e delle criticità riscontrabili sul piano operativo.

---

[38] Per informazioni di dettaglio, si rinvia alla sezione notizie del sito internet di Europol (https://europol.europa.eu) comunicato stampa del 09 settembre 2016.

[39] «Report on the proposal for a regulation of the European Parliament and of the Council on controls on cash entering or leaving the European Union», studio condotto dalla Commissione affari economici e monetari del Parlamento Europeo (COM-2016-0825 – C8-0001/2017 – 2016/0413-COD), disponibile sul sito internet: http://www.europarl.europa.eu

[40] La relazione (emendamento n. 8) ricorda come le Autorità doganali di tutta l'Unione non dispongono di risorse sufficienti per monitorare la circolazione transfrontaliera di valute virtuali, un divario che potrebbe ulteriormente aumentare la facilità del loro impiego per fini di riciclaggio o evasione fiscale.

[41] In argomento, LEMME G.-PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, in *Riv. Dir. banc.*, 2016, 11, 22 ss.; ROSEMBUJ T., *Bitcoin*, Barcelona, 2016, 30 ss.; D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta*, cit., 15.

[42] Per approfondimenti, si veda il rapporto «Bitcoin and Cryptocurrencies», pubblicato dal Law Enforcement Cyber Center costituito dalla *International Association of Chiefs of Police* (IACP), disponibile sul sito http://www.iacpcybercenter.org, 4 ss.

Assumiamo che Tizio, *hacker* molto esperto, dopo aver messo a disposizione su un portale del *web* profondo una vasta gamma di servizi di danneggiamento di dati e programmi informatici "su commissione", sia stato contattato da Caio, intenzionato ad avvalersi della sua opera per vendicarsi contro Mevio, suo *ex* datore di lavoro. All'esito delle trattative, i due concordano il prezzo della prestazione in 2 Bitcoin, ammontare di valuta che l'acquirente dovrà corrispondere in anticipo rispetto all'esecuzione della prestazione. La transazione è il risultato di un processo tecnico-matematico piuttosto complesso, basato sulla crittografia asimmetrica a doppia chiave, che si articola in tre fasi successive.

Il processo inizia con l'*ordine di pagamento* disposto da una parte in favore dell'altra. Gli interessati hanno un *wallet* Bitcoin installato sul proprio computer o *smartphone*, vale a dire un programma o insieme di *file* che permette l'accesso a uno o più indirizzi Bitcoin. Gli indirizzi sono composti da una stringa alfanumerica di caratteri[43] e sono associati a una differente quantità di valuta; nel portafoglio sono custodite le chiavi private di accesso a ciascun indirizzo. Per ricevere il pagamento Tizio può decidere se avvalersi di uno degli indirizzi già registrati nel portafoglio[44], oppure creare un nuovo indirizzo "dedicato" alla ricezione del dovuto. Dopo aver ricevuto gli estremi dell'indirizzo, Caio inoltra al *client* Bitcoin[45] un ordine di pagamento, che include l'indirizzo di *input* della transazione, quello di *output*, e l'ammontare di valuta da trasferire. Il *client* firma la richiesta di transazione con la chiave privata dell'indirizzo utilizzato come *input*, e lo inoltra alla rete.

A questo punto di apre la fase di *verifica della transazione*. La rete può utilizzare la chiave pubblica per verificare che la richiesta di transazione provenga dal legittimo titolare della chiave privata[46]. Più precisamente, i computer impegnati nel *mining* – configurati per elaborare calcoli di crittografia – raggruppano tutte le transazioni degli ultimi minuti in un blocco[47]. La funzione crittografica di *hash* trasforma i dati del blocco in elaborazione in una stringa alfanumerica di caratteri, di ammontare predeterminato, detto valore di *hash*[48]. Per creare differenti valori finali a partire dai medesimi dati iniziali, rappresentati dall'insieme di transazioni riunite in blocco, il

[43] Si tratta stringhe alfanumeriche di lunghezza variabile, compresa tra i 26 e i 35 caratteri, con il primo carattere rappresentato dal carattere 1 o 3, e, all'interno caratteri non ambigui (O 0 I l) nella codifica utilizzata, denominata base58.

[44] Cfr. BISTARELLI, *Bitcoin forensics: le tecniche labeling, clustering e mixnet recognition*, cit., 3

[45] Il *client* in questione potrebbe essere quello di un *provider* che offre servizi di *storage* o di portafoglio – dunque, un mero intermediario – oppure direttamente il *client* Bitcoin.org. La presenza di intermediari della gestione di servizi di portafoglio assume una importanza centrale sul piano delle investigazioni e dell'esecuzione di misure cautelari (v. *infra*, § 6 e 7)

[46] La richiesta di nuova transazione incorpora anche il riferimento alle precedenti transazioni per consentire una verifica della effettiva titolarità della quantità di valuta che l'ordinante intende trasferire (nel caso di specie, 2 BTC).

[47] *Amplius*, Cap. I, § 2.2.

[48] Anche il più insignificante cambiamento dei dati iniziali (un singolo carattere o byte) cambierà totalmente il valore finale di Hash. Si tratta di un algoritmo matematico che mappa dati di lunghezza variabile in una stringa binaria di dimensione fissa chiamata appunto valore di *hash*. Tale funzione di è progettata per essere unidirezionale (*one-way*), ovvero impossibile da invertire (dal valore finale non è dato risalire ai dati iniziali).

sistema Bitcoin usa un "nonce", cioè un numero casuale che si aggiunge ai dati iniziali prima dell'applicazione della funzione di criptazione. I *miners* cominciano così a calcolare nuovi valori di *hash* basandosi sui dati del blocco che riunisce le transazioni e sul valore numerico casuale. Per i moderni computer la creazione di siffatti valori non sarebbe affatto complessa, ma il sistema Bitcoin richiede che il nuovo valore debba iniziare con un certo numero di zeri. Non essendo possibile stabilire *ex ante* quale sarà il numero che, applicata la funzione di *hash*, darà come risultato un valore che inizi con il valore predeterminato di zeri, i *computer* impegnati nel *mining* dovranno continuare a generare valori di *hash* cambiando di volta in volta, in modo causale, il numero *nonce* finché non verrà trovato il valore che soddisfa i requisiti previsti dal sistema.

L'ultima fase è caratterizzata dalla *chiusura del blocco* sulla *blockchain.* La transazione tra Tizio e Caio sarà ultimata quando, conclusa con successo la verifica degli *input* di transazione e inserita la stessa nel gruppo di *unconfirmed transactions*, verrà trovato il valore di *hash* idoneo a "saldare" questo nuovo blocco agli anelli precedenti della catena[49]. A questo punto Tizio riceverà all'indirizzo di *output* i 2 BTC che potranno essere utilizzati come *input* per nuove transazioni. Con il passare del tempo, la transazione contenuta nel nuovo blocco andrà a stratificarsi sotto il manto delle nuove transazioni, rendendo pressoché impossibile apportare modifiche al registro[50]. Sulla *blockchain* rimarrà dunque impresso in modo tendenzialmente immodificabile e pubblicamente verificabile che: (i) tra i due indirizzi vi è stato uno scambio di valuta di un certo ammontare; (ii) la transazione è avvenuta in una data certa; (iii) che l'ordinante poteva effettivamente disporre del predetto ammontare di valuta[51].

Ammettiamo che, ricevuto il pagamento, Tizio esegua con successo l'attacco informatico commissionato e che, a seguito della denuncia presentata dalla vittima, si apra un procedimento penale contro ignoti. Dalle prime indagini emerge una certa similarità tecnica e contiguità temporale tra il fatto denunciato e altri attacchi informatici verificatisi nelle settimane precedenti, tale da indurre gli organi inquirenti a ipotizzare che ti tratti di un criminale seriale che, verosimilmente, agisce su commissione dietro il pagamento di un corrispettivo in valuta virtuale.

Il caso appena esemplificato fungerà da base per l'esame delle questioni che l'utilizzo della tecnologia a registro diffuso pone sul piano processuale. Quali mezzi di ricerca della prova potranno essere utilizzati per suffragare l'ipotesi investigativa? Quali procedure dovranno essere seguite per acquisire la prova della transazione illecita? Come disporre il sequestro, preventivo o probatorio, del prezzo del reato?

---

[49] NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, in https://bitcoin.org, § 4

[50] Se qualcuno volesse manipolare il pubblico registro delle transazioni dovrebbe rifare al contrario il lavoro di *mining*, trovando un numero-*nonce* per ciascuno dei blocchi già saldati alla *blockchain*, per poi ricostituire tutta l'intera catena. Un tale operazione richiederebbe una potenza computazionale immensa che, allo stato, non sembra possibile raggiungere.

[51] «Basic Manual on the Detection and Investigation of the Laundering of Crime Proceeds Using Virtual Currencies», cit., 33 ss.

Per fornire una risposta a questi interrogativi dovremo focalizzare l'attenzione sulla prima e l'ultima fase della transazione[52], esaminando da vicino le diverse forme che può assumere un ordine di pagamento e le tipologie di analisi che possono compiersi sulla *blockchain* a seguito della chiusura di ciascun blocco.

4. Mezzi di ricerca della prova e sequestro probatorio di dati e programmi informatici.

La disintermediazione degli scambi nel cyberspazio pone problemi di rilievo sul versante probatorio, che scaturiscono dal tramonto della figura del *provider* quale referente principale nell'acquisizione della *digital evidence*. La tecnologia a registro diffuso permette agli utenti di scambiare informazioni – siano esse rappresentative di valori, idee, documenti – basandosi sulla fiducia reciproca nell'ecosistema, senza passare per l'opera di terze parti intermediarie. In un simile contesto, le attività di ricerca della prova dovranno essere condotte sfruttando le potenzialità della *blockchain* e le garanzie che essa offre in termini di immodificabilità e trasparenza del registro pubblico delle transazioni.

Mettendo per un momento da parte le ipotesi in cui gli autori di una transazione illecita si siano avvalsi di fornitori di servizi di portafoglio virtuale[53], vi sono casi[54] in cui lo scambio di realizza realmente *peer to peer* senza il coinvolgimento, neppure indiretto, di terze parti. Per semplificare diremo che la transazione avviene tra *indirizzi privati*, per distinguerla dai casi in cui gli indirizzi siano "depositati" su una piattaforma di scambio o in un portafoglio gestito da un fornitore di servizi. In simili circostanze, la difficolta nell'individuazione dei soggetti responsabili raggiunge l'apice.

L'analisi svolta in questo e nel successivo paragrafo avrà ad oggetto i mezzi di ricerca della prova esperibili nei procedimenti per reati connessi all'utilizzo di valute virtuali, quando il trasferimento sia avvenuto in modo diretto tra indirizzi privati. Per fornire al lettore un quadro esaustivo dei diversi strumenti d'indagine, converrà distinguere le ipotesi in cui la persona indagata sia stata individuata, da quelle in cui il procedimento sia apra contro ignoti.

Nel primo caso l'acquisizione della *digital evidence* potrà seguire i principi dettati dal codice di procedura penale in materia di sequestro probatorio di strumenti informatici[55]. Individuato l'autore di una transazione illecita, le autorità inquirenti

[52] La seconda fase di *verifica della transazione* non è rilevante sul piano investigativo. Coloro che svolgono l'attività di *mining* si limitano a processare dati in modo automatico, senza poter avere cognizione delle parti coinvolte o delle finalità della transazione. Pertanto, essi non potranno mai venire in rilievo, neppure astrattamente, come potenziali concorrenti nel reato (v. Cap. II, § 6.5.).

[53] Il tema sarà oggetto di esame nel prosieguo (v. *infra*, § 6).

[54] I criminali informatici più esperti agiscono nell'anonimato più totale, ed evitano di trasferire valori per mezzo di fornitori di servizi. Il trasferimento diretto di fondi è quindi la forma che si presta più facilmente all'utilizzo per fini illeciti.

[55] A norma dell'art. 253 c.p.p. è sempre possibile il sequestro del corpo del reato e delle cose che servirono a commettere il reato. Il computer (comprensivo di *hardware* e *software*) e le connesse periferiche potrebbero costituire gli strumenti che materialmente sono stati impiegati per effettuare una

potranno procedere a ispezioni o perquisizioni[56] finalizzate alla ricerca, dapprima, delle apparecchiature informatiche (*computer, laptop, smartphone, tablet*), e poi, al loro interno, dei programmi o dati informatici a sostegno dell'ipotesi accusatoria. Le predette attività di ricerca dovranno svolgersi in conformità con le regole procedurali fissate dal codice di procedura penale per assicurare la genuinità e l'immodificabilità dell'evidenza informatica raccolta. Nell'*hard disk* di un computer rinvenuto dalla polizia giudiziaria nel corso di un'ispezione o di una perquisizione potrebbero esservi le tracce digitali utili e significative sul piano probatorio. Per quel che qui interessa, l'attenzione andrà rivolta, in particolare, alla presenza di *software* di gestione degli indirizzi e delle chiavi crittografiche private o di periferiche di archiviazione delle stesse (*cold wallet*).

La disciplina codicistica cui fare riferimento è quella dettata dall'art. 354, comma 2, c.p.p., nella formulazione introdotta dalla legge di ratifica della Convenzione di Budapest[57], che attribuisce alla polizia giudiziaria il potere-dovere[58] in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, di

---

transazione illecita. Il sequestro probatorio è un mezzo tipico di ricerca della prova (artt. 253-265 c.p.p.), che consiste nell'assicurare una cosa mobile o immobile al procedimento per finalità probatorie, mediante lo spossessamento coattivo della cosa o la creazione di un vincolo di indisponibilità sulla *res* medesima. Tale vincolo di indisponibilità serve per conservare immutate le caratteristiche della cosa, per consentire un accertamento oggettivo dei fatti. Occorre, quindi, che vi sia un bene materiale, che si tratti del corpo del reato o di una cosa pertinente al reato (art. 253 c.p.p.), e che la cosa appresa o vincolata sia necessaria per l'accertamento dei fatti. Il sequestro probatorio, infatti, è mantenuto fino a quando sussistono le esigenze probatorie (art. 262, primo comma, c.p.p.) e, in ogni caso, mai può oltrepassare il momento che segna l'irrevocabilità della sentenza, salvo che sia disposta la confisca (art. 262, comma 4, c.p.p.). Per approfondimenti, con particolare riguardo al sequestro probatorio in ambito informatico, VENTURINI S., *Sequestro probatorio e fornitori di servizi telematici*, in LUPÀRIA L., *Internet provider e giustizia penale*, Milano, 2012, 107 ss.; VACIAGO G., *Digital evidence, I mezzi di ricerca della prova nel processo penale e le garanzie dell'indagato*, Torino, 2012, 51 ss.; MACRILLÒ A., *Le nuove disposizioni in materia di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, in *Dir. Internet*, 2008, 5, 503 ss.; BARBIERI A., *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici*, ivi, 516 ss.; LUPÀRIA L., *La disciplina processuale e le garanzie difensive*, in LUPÁRIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, 130 ss.

[56] La ricerca delle apparecchiature informatiche viene eseguita nel domicilio o indosso alla persona sottoposta alle indagini. Una volta rivenuta, sarà necessario esplorare il contenuto del sistema informatico per acquisire elementi di prova del reato per cui si procede. Secondo una condivisibile opinione dottrinale, l'*ispezione* di sistemi informatici è una ipotesi di scuola, configurabile soltanto nei casi in cui gli inquirenti si limitino ad osservare le immagini proiettate su un monitor acceso. L'esplorazione di un *computer* – sia che avvenga contestualmente nel domicilio dell'indagato, sia successivamente in un laboratorio di *forensics* – assume sempre i connotati della perquisizione. Infatti, «*accedendo alle memorie interne del computer ed esplorandone i contenuti informatici e telematici, si entra nella sfera individuale e domiciliare dell'individuo. Si perlustra l'ambiente virtuale dove si svolge la di lui esistenza e se ne scrutano le abitudini. In buona sostanza si effettua una perquisizione sulla persona, sulle cose e sul domicilio dell'indagato*» (così VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, cit., 132). Sulla base a queste premesse, l'Autore ritiene che alla perquisizione informatica si applichino le garanzie di cui agli artt. 247 ss c.p.p. Pertanto, dovrà essere previamente individuato, in maniera specifica e concreta, il *thema probandum* nel cui ambito si effettua la ricerca, poiché, diversamente argomentando, la perquisizione da strumento di ricerca della prova si trasformerebbe in mezzo di acquisizione della *notitia criminis*.

[57] Cfr. Art. 9, comma 3, della legge 18 marzo 2008 n. 48

[58] Così definito da VENTURINI S., *Sequestro probatorio e fornitori di servizi telematici*, cit., 109

adottare le misure tecniche o di impartire le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso, provvedendo, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità[59].

Le *best practice*[60] di settore suggeriscono di procedere alle operazioni di copia mediante la cosiddetta *bit stream image*, anche nota con il nome di *mirror image*, consistente nella realizzazione di una riproduzione fedele *bit-by-bit* del contenuto dell'*hard disk* e delle periferiche[61]. A partire da questa, si potranno realizzare altri duplicati, su cui compiere tutte le operazioni necessarie senza correre il rischio di danneggiare o alterare il contenuto dell'*hardware*[62]. Per assicurare l'immodificabilità della copia-clone e renderla, dunque, pienamente utilizzabile nel processo penale, la polizia giudiziaria provvede alla cifratura dei *file* mediante l'algoritmo crittografico di *hash*[63]. La stringa alfanumerica di caratteri (valore di *hash*) consente alla difesa di verificare la corrispondenza tra i dati contenuti nell'*hard disk* e quelli della copia clone, o tra quest'ultima e gli eventuali duplicati successivi.

La *digital evidence* è contenuta in un documento informatico che, ove legittimamente acquisito, entra a comporre il compendio probatorio secondo la disciplina della prova documentale. Tuttavia, è bene precisare che l'utilizzabilità nel processo è limitata alle prove pervenute integre e inalterate al vaglio dibattimentale. In caso di inosservanza delle procedure pocanzi esaminate – e dunque nell'incertezza circa l'adozione di misure tecniche necessarie ad assicurare la conservazione dei dati e dei programmi informatici ed impedirne l'alterazione o l'accesso, ovvero nel dubbio sulla conformità della copia all'originale e la sua immodificabilità – deve operare la sanzione dell'inutilizzabilità *ex* art. 191 c.p.p.

In procedimenti per reati connessi all'utilizzo di valuta virtuale gli strumenti investigativi finora esaminati potrebbero rivelarsi inadeguati, o comunque insufficienti

---

[59] Gli ufficiali di polizia giudiziaria possono inoltre sequestrare il corpo del reato e le cose a questo pertinenti ai sensi del predetto art. 253. In questi casi il verbale delle operazioni è trasmesso senza ritardo, e comunque non oltre le quarantotto ore al pubblico ministero del luogo dove il sequestro è stato eseguito; questi, nelle successive quarantotto ore, convalida il sequestro con decreto motivato, ove ne ricorrano i presupposti, ovvero dispone la restituzione delle cose sequestrate (art. 355, comma 2, c.p.p.).

[60] «Best Practice Manual for the Forensic Examination of Digital Technology», documento pubblicato dall'European Network of Forensics Science Institutes (ENFSI), disponibile sul sito internet http://enfsi.eu

[61] In argomento, VENTURINI S., *Sequestro probatorio e fornitori di servizi telematici*, cit., 122 il quale descrive la *bit stream image* come una "fotografia digitale", un clone perfettamente identico all'originale, contenente oltre ai file visibili anche quelli nascosti, danneggiati o cancellati, nella loro esatta disposizione.

[62] Dal punto di vista operativo, la duplicazione del contenuto dell'*hard disk* può essere effettuata direttamente *in loco*, oppure in un momento successivo, adottando *medio tempore* le opportune cautele per evitare la perdita di dati. Qualora si proceda nell'immediatezza, sarà possibile estrarre copia anche delle informazioni contenute nella memoria RAM di un computer acceso, le quali, una volta spento l'elaboratore, potrebbero non andare definitivamente perdute.

[63] L'algoritmo di *hash* è utilizzato in *computer forensics* per le stesse ragioni (immodificabilità dei dati, sicurezza nella trasmissione delle informazioni, verificabilità esterna dei valori di *hash*) che abbiamo illustrato a proposito del trasferimento di valuta virtuale tra due indirizzi (v. *supra*, § 3).

ad acquisire la prova di una transazione illecita. Solitamente, i *software* di gestione di portafogli virtuali e gli *hardware wallet* ad essi associati sono protetti da *password* e da sistemi di sicurezza basati su algoritmi di codifica che rendono il contenuto inaccessibile, o comunque non intellegibile per chi non disponga delle chiavi di accesso. Le procedure di autenticazione più evolute utilizzano vere e proprie tecniche di crittografia, che non potrebbero essere superate neppure da un esperto informatico forense[64].

Può dunque accadere che le attività di perquisizione informatica debbano arrestarsi di fronte alle barriere di autenticazione del portafoglio virtuale. Eppure, l'accesso ai dati in esso contenuto si rivela spesso assolutamente necessario ai fini della prosecuzione e della buona riuscita delle indagini. Basti pensare che accedendo allo "storico" delle transazioni di dare e avere di un *e-wallet*, gli investigatori potrebbero ottenere facilmente gli indirizzi di accredito/addebito dei valori virtuali, e confrontare le stesse con le evidenze pubbliche della *blockchain*, riuscendo così a fare breccia nel muro della pseudonimizzazione[65]. Per dar corso alla perquisizione del portafoglio gli investigatori potranno chiedere all'indagato di comunicare la relativa chiave di accesso ai sensi dell'art. 248 c.p.p., che disciplina la richiesta da parte dell'autorità giudiziaria di consegna delle cose ricercate con la perquisizione. La richiesta sarà possibile soltanto quando la perquisizione sia specificamente e *ab origine* rivolta alla ricerca di un portafoglio virtuale. Diversamente, qualora le ricerche riguardino generiche e non meglio note informazioni in formato digitale, si estenderebbe *in malam partem* l'ambito applicativo della disposizione[66]. La questione si profila, dal punto di vista teorico, particolarmente complessa anche per l'indubbia incidenza sul diritto al silenzio[67] della persona sottoposta alle indagini. A ben vedere, la richiesta di comunicazione della *password* è funzionale al rilascio di una dichiarazione che potrebbe essere utilizzata contro l'indagato. Ne deriva che, a stretto rigore, la polizia giudiziaria dovrebbe procedere nei modi indicati dall'art. 350, comma 1, c.p.p. e

[64] Cfr. «Bitcoin and Cryptocurrencies», cit., 13

[65] Quando la transazione sia intercorsa tra indirizzi privati, senza l'intermediazione di alcuna piattaforma o servizio di gestione, l'accesso al portafoglio virtuale dell'indagato può divenire l'unica fonte di prova della commissione del fatto, specie nei casi in cui nel *computer* – o eventualmente sul *cloud* – non vi siano altre tracce (quali, ad esempio, messaggi, file di testo o documenti) del compimento dell'operazione sospetta.

[66] Sul punto, VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, cit., 133 il quale ritiene che la richiesta rivolta all'indagato di comunicare un codice di accesso costituisca in ogni caso una estensione analogica *in malam partem* dell'art. 248 c.p.p., dal momento che, in questi casi *«non gli si chiede di consegnare un determinato oggetto con precise connotazioni spaziali, ma lo si interroga per conoscere un codice d'accesso che altro non è se non un'informazione riservata che la persona sottoposta alle indagini ha diritto a mantenere tale»*.

[67] Nella dottrina processualpenalistica vi è la tendenza a desumere il diritto al silenzio da alcune disposizioni codicistiche che ne rappresentano manifestazioni parziali, quali l'art. 64 (avvertimento sullo *ius tacendi*), l'art. 188 (libertà morale della persona) e 274 (divieto di inferire la sussistenza dell'esigenza cautelare dal silenzio dell'indagato) del codice di procedura penale. La sanzione processuale per la violazione del diritto al silenzio dell'imputato/indagato è la radicale inutilizzabilità ai sensi art. 191 c.p.p. delle informazioni acquisite in sede di indagine. Sul tema, di recente, STANZIONE G., *Autoincriminazione e diritto al silenzio*, Padova, 2017, 71 ss.

formulare gli avvertimenti di cui all'art. 64 c.p.p[68]. Nell'incertezza sulla disciplina codicistica applicabile all'ipotesi *de qua*, dovrebbe comunque valere il principio generale *in dubio pro reo.*

5. *Blockchain forensics* e *Open Source Intelligence*.

L'utilizzo dei mezzi tipici di ricerca della prova presuppone che le indagini siano indirizzate nei confronti di una o più persone, possibili autori di un reato connesso all'utilizzo delle valute virtuali. Non si deve tuttavia dimenticare che l'incentivo all'uso di queste ultime deriva proprio dalle garanzie di anonimato che esse offrono, circostanza che, sul piano investigativo, comporta serie difficoltà nell'individuazione degli autori di una transazione illecita. A tal fine sono state elaborate alcune innovative tecniche di indagine che si basano sull'osservazione delle evidenze disponibili sul registro pubblico delle transazioni[69] e sulle informazioni reperibili in rete, al fine di delineare un profilo dei possibili cyber-criminali. Questi nuovi strumenti investigativi, nati dalla combinazione di espedienti di *intelligence*[70] su informazioni liberamente accessibili, c.d. *Open Source Intelligence*, e di elementi di ingegneria informatica, permettono di associare, a determinate condizioni, gli indirizzi incisi sulla *blockchain* ad utenti particolarmente "attivi" in rete. Il caso che abbiamo addotto come esempio nella pregressa trattazione[71] ci servirà ora da guida per esaminare da vicino lo svolgimento di questo tipo di indagini.

Immaginiamo che gli organi inquirenti, dopo aver ricevuto la denuncia di Mevio, esaminate le risultanze dei registri delle notizie di reato relativi a casi analoghi, ipotizzino che l'attacco informatico di cui questi è stato vittima sia l'opera di un criminale seriale che agisce su commissione dietro il pagamento di un corrispettivo in

---

[68] *Infra*, § 7.1.

[69] Il pubblico registro della *blockchain* è liberamente accessibile; chiunque potrebbe scaricarlo sul proprio computer e cimentarsi in una delle tecniche d'*intelligence* descritte nel prosieguo di questo paragrafo.

[70] L'*intelligence* viene essere definita come l'insieme delle le attività di raccolta, valutazione e analisi delle informazioni al fine di produrre "il sapere" necessario per il raggiungimento di determinati obiettivi. Essa può assumere connotati differenti, in base all'oggetto. Alcuni autori distinguono in particolare, la *Human Intelligence* (HUMINT) che ha per oggetto le fonti umane e si basa sulla raccolta delle informazioni attraverso soggetti che, per vari motivi, posseggono informazioni rilevanti al caso; la *Imagery Intelligence* (IMINT), vale a dire l'attività di raccolta informazioni attraverso l'elaborazione e l'analisi di immagini aeree provenienti da satelliti, aerei spia, droni etc.; la *Measurement and Signature Intelligence* (MASINT), riferita all'analisi scientifica e tecnica di tracce chimiche, spettrografiche e radiologiche riferite a vettori e sistemi strategici militari; la *Signals Intelligence* (SIGINT), basata sull'intercettazione e l'analisi delle comunicazioni sia tra esseri umani, sia tra macchine intelligenti. Ai fini della presente analisi rileva in particolare la *Open Source Intelligence* (OSINT), che si fonda sull'attività di analisi delle fonti "aperte", ovvero le fonti pubbliche, liberamente accessibili, non classificate. Cfr. SAGLIOCCA A., *Open Source Intelligence e Deep Web: scenari moderni delle investigazioni digitali*, in *Ciberspazio e diritto*, 2017, 1, 171 ss.; KOOPS, B.J., *Police investigations in Internet open sources: Procedural-law issues*, in *Computer Law & Security Review*, 2013, fasc. 29, 6, 654 ss.

[71] v. *Supra*, § 3

valuta virtuale. Chiamato a rendere informazioni più dettagliate, l'imprenditore riferisce di poter nutrire sospetti di ritorsione soltanto nei confronti di Caio, licenziato qualche giorno prima all'esito di un litigio furibondo. Dalle prime indagini emerge che l'*ex* dipendente ha un profilo pubblico sul noto *forum* di discussione bitcointalk.org, ove appare in chiaro un indirizzo di portafoglio Bitcoin.

Per seguire le tracce del presunto *hacker* mercenario, gli investigatori possono avvalersi di sofisticati *software* per indicizzare i risultati più pertinenti alla ricerca svolta. L'attività in questione prende il nome di *labeling* e consiste nell'utilizzo di motore di *web crawling*[72], in grado di analizzare interi siti e domini *web* e indicizzarne i contenuti. La ricerca andrà rivolta, in particolare, agli *hidden service* nascosti sulla rete Tor, tra cui vi sono molti forum di discussione o mercati neri dove è possibile acquistare servizi di *crime-as-a-service*[73], cioè attacchi informatici su commissione; ai *crawler* verranno pertanto impartite chiavi di ricerca per individuare annunci correlati a tali servizi[74]. All'esito, potrà essere attivato un processo di *web scraping*, consistente nell'estrazione automatizzata di singoli dati da un insieme di pagine *web*, per collezionarli all'interno di database che li renda intellegibili e facilmente consultabili. Con ogni probabilità, la ricerca condurrà all'individuazione di numerosi annunci, post o messaggi, alcuni dei quali pubblicati in tempo prossimo rispetto alla commissione del reato. Selezionati quelli più rilevanti, si potrà redigere una sorta di "classifica" dei risultati, in base al tipo di servizio offerto, alla lingua utilizzata per l'annuncio, al prezzo richiesto per ciascuna prestazione. Supponiamo che l'attività di *labeling* abbia condotto all'individuazione di un utente di lingua italiana, erogatore di servizi di *hackeraggio* su commissione, e che sia possibile associare[75] uno o più indirizzi Bitcoin al profilo di quest'ultimo.

Gli esperti potranno partire da queste informazioni per ricercare nel registro pubblico delle transazioni le tracce della transazione incriminata. Le attività di *blockchain forensics* rappresentano una nuova forma di *open source intelligence*, basata sull'analisi e sull'aggregazione di indirizzi per cercare di comprendere, tramite metodi euristici specifici, quali indirizzi appartengono alla stessa persona e quali invece

[72] Un *crawler* è un *software* appositamente studiato per prelevare il contenuto di una pagina *web* e seguirne gli hyperlink al fine di analizzare siti *web* collegati o pagine secondarie.
[73] Cfr. «Internet Organised Crime Threat Assessment» (IOCTA 2017), cit., 58 ss.
[74] È possibile inserire come chiave di ricerca anche un indirizzo di portafoglio, qualora questa sia una informazione già nota agli inquirenti. Si pensi al caso in cui venga denunciato un attacco *ransomware* indicando a chiare lettere l'indirizzo a cui far pervenire il pagamento del riscatto.
[75] Gli annunci relativi a prestazioni illecite difficilmente contengono gli estremi dell'indirizzo a cui il proponente intende ricevere pagamenti o altre informazioni di carattere personale. Spesso viene indicato soltanto un contatto di messaggistica istantanea, che gli inquirenti potranno utilizzare per ottenere, sotto copertura, ulteriori informazioni. Un recente studio ha comunque dimostrato che è possibile associare gli utenti di molti *hidden service* su Tor ad uno o più indirizzi grazie ad accurate indagini *open source* sul profilo dell'utente, sul *surface web* (social network, forum di discussione) e sul *deep web*. In argomento, AL JAWAHERI H., *Deanonymizing Tor hidden service users through Bitcoin transactions analysis*, disponibile sul portale dell'Università del Qatar, http://qspace.qu.edu.qa, 17 ss.

sono controllati dagli *exchange provider* a cui chiedere informazioni sull'identità dell'utente[76].

Tra i metodi euristici disponibili, la c.d. *wallet closure analysis* ha una importanza centrale. Essa si fonda sull'assunto secondo cui, qualora due indirizzi figurino nella stessa transazione come *input*, sarà verosimile che siano controllati da uno stesso utente che ha firmato la transazione con la sua chiave privata. Un secondo metodo di analisi, detto *shadow heuristic*, si basa sull'evidenza che la maggior parte dei portafogli virtuali esistenti gestiscono transazioni con resto, generando una nuova coppia di chiavi in *output* per la quantità di valuta non spesa. Laddove vi sia una transazione con un *input* e due *output*, si può supporre che uno sia l'indirizzo di destinazione e l'altro sia il resto[77]. La *consumer heuristic*, derivata dalla precedente, è utilizzata per sciogliere il dubbio su quale dei due indirizzi di *output* sia quello che porta i fondi verso il destinatario e quale il resto, basandosi sul comportamento dell'utente/investitore medio[78]. Al medesimo fine, la *optimal change heuristic* aiuta ad individuare l'indirizzo generato come resto in base alla configurazione di *default* dei portafogli, tendente alla ottimizzazione nella gestione degli indirizzi. andando a cercare i migliori *output* da spendere[79].

La "lettura ragionata" del reticolo di transazioni sul registro pubblico, finalizzata all'accorpamento di più indirizzi controllati dallo stesso proprietario è detta attività di *clustering*. Le euristiche che guidano l'interprete in questo arduo compito, pur non avendo *stricto sensu* validità scientifica, rappresentano il postulato della *blockchain forensics*, concorrendo a rendere fruibili informazioni che, diversamente, risulterebbero inaccessibili e di nessuna utilità pratica. A complicare il quadro, si aggiungono i servizi di *mixing* o *mixnet*, utilizzati al precipuo scopo di ostacolare la ricostruzione della catena delle transazioni[80]. Il loro funzionamento può essere sinteticamente descritto nei termini seguenti: un utente invia un determinato ammontare di valuta da uno o più indirizzi, per poi riprendersi il denaro virtuale su indirizzi in uscita preesistenti o appositamente creati. Il *mixer* farà in modo che non sia

[76] Sul punto, BISTARELLI, *Bitcoin forensics: le tecniche labeling, clustering e mixnet recognition*, cit., 3

[77] In questo senso, DAL CHECCO P. – ZEN L., *Il Clustering come Strumento di Deanonimizzazione dei Wallet Bitcoin,* in *ICT security magazine*, 24 luglio 2017. Seguendo il nostro esempio, se l'indirizzo (o gli indirizzi) utilizzato per remunerare l'*hacker* fossero riferiti a una quantità maggiore di valuta (es. 3 BTC), sulla *blockchain* sarebbero registrati due *output,* uno dell'ammontare di 2 BTC diretto all'indirizzo privato di Tizio, l'altro di 1 BTC come resto diretto a un nuovo indirizzo controllato da Caio.

[78] Si guarda in questo caso, al reticolo di transazioni successive ai due indirizzi di *output*. Se uno dei due indirizzi riversa, a sua volta, la valuta in più *output* – magari prendendolo da più *input*, secondo la prima euristica – verosimilmente sarà quella la transazione di resto, mentre l'altro indirizzo apparterrà al destinatario della prima transazione.

[79] Questa euristica si basa sul seguente assunto: se c'è un *output* con un valore minore dei singoli *input,* allora quello sarà il resto della transazione. Esemplificando, laddove in una transazione vi siano due *input* da 1 BTC ciascuno e due *output* rispettivamente da 1.7 BTC e da 0.3 BTC, allora sapremo con certezza che quest'ultimo è il resto. Difatti, non avrebbe senso il contrario: se l'utente avesse inteso trasferire 0.3 BTC, sarebbe bastato un solo *input* da 1 BTC, con un avanzo di 0.7 BTC. Cfr. DAL CHECCO – ZEN, *Il Clustering come Strumento di Deanonimizzazione dei Wallet Bitcoin,* ibidem

[80] Sui servizi di *mixing* v. *Amplius*, Cap. III § 3.3.2.

possibile associare direttamente l'ammontare di denaro in entrata e quello in uscita, e tratterà – quale corrispettivo della propria intermediazione – una percentuale sul valore della transazione[81].

Per ricostruire la "pista" digitale, gli informatici forensi si servono tecniche di *reverse engineering* e di *machine learning* che aiutano a scompigliare la matassa e a porre in evidenza i veri *input* e *output* delle transazioni[82]. Il potenziamento dei *software* di *mixnet recognition* rientra tra gli obiettivi del partenariato pubblico-privato, cui abbiamo fatto cenno in apertura del capitolo[83]. Lo sviluppo di algoritmi di apprendimento richiede, infatti, una grande quantità di dati e lo studio accurato dei protocolli di *mixing* più diffusi[84].

Infine, tra le tecniche d'indagine più innovative vi è la *pattern analysis*. Metaforicamente assimilabile a una diagnostica per immagini in campo *blockchain*, essa consiste nella trasposizione grafica della direzione e del flusso di determinate transazioni, per valutare l'esistenza di *pattern* ricorrenti ed usuali. Questo strumento si rivela particolarmente utile per supportare le attività di indagine relative al pagamento di riscatti a seguito di diffusione di *ransomware.*

Per concludere, proviamo ad ipotizzare un possibile *exitus* investigativo del caso che abbiamo esemplificato. Grazie alle indagini svolte *open source* gli inquirenti hanno individuato due indirizzi Bitcoin riconducibili ai possibili sospettati. A questo punto l'attenzione dovrà focalizzarsi sul registro pubblico delle transazioni per scoprire se vi siano associazioni tra questi indirizzi in epoca prossima alla commissione del reato. In particolare, l'indirizzo controllato da Tizio, figura più volte negli ultimi mesi come beneficiario, a cadenze periodiche fisse, di pagamenti per importi più o meno uguali (ricompresi tra 2 e 4 BTC). Ciò dimostra, con ogni probabilità, che quello è l'indirizzo a cui l'*hacker* professionista fa pervenire i ricavi della sua attività. Per quanto riguarda l'indirizzo rinvenuto sul profilo di Caio nel *forum* Bitcointalk.org, si scopre che: a quest'ultimo erano pervenuti alcuni pagamenti nel 2015 per l'ammontare complessivo di 1,8 BTC; per oltre due anni l'indirizzo è risultato inattivo, non risultando né in *input* né in *output* di alcuna transazione; che due giorni prima della commissione dell'attacco

[81] I prestatori di servizi di *mixing* utilizzano, tendenzialmente, due espedienti. Una prima tecnica consiste nell'invio "a catena" di moneta da numerosi portafogli, dai quali poi si dipartiranno altre operazioni dirette ad altri conti. L'obiettivo è quello di rendere la rete dei passaggi a tal punto complessa da rendere quasi impossibile la ricostruzione dei singoli passaggi intermedi. Gli indirizzi che partecipano a questa attività sono chiamati "conti di rimbalzo" (conti *bounce*). Una seconda tecnica consiste nel raggruppare i fondi di più utenti che si sono rivolti al servizio di *mixing* in un unico indirizzo, detto conto *pool* o *pot,* e poi spedirli nuovamente a più indirizzi. *Amplius,* Cap. III, § 3.3.2.

[82] In questi termini, BISTARELLI, *Bitcoin forensics: le tecniche labeling, clustering e mixnet recognition*, ibidem

[83] *Supra,* § 2.1.

[84] Alcune importanti iniziative per una *partnership* pubblico-privato sono state siglate con la società «Chainanalysis», specializzata nella produzione di *software* antiriciclaggio per l'ecosistema Bitcoin. Tra gli accordi più importati spicca quello con Europol e altre istituzioni di coordinamento investigativo. Per approfondimenti si rinvia all'articolo «Europol and Chainalysis Reinforce Their Cooperation in The Fight Against Cybercrime», comunicato stampa del 19 febbraio 2016 sul sito istituzionale https://europol.europa.eu

informatico ai danni di Mevio, l'indirizzo figura, insieme a un altro indirizzo, come *input* di una transazione diretta *in output* all'indirizzo di Tizio; gli *input* di transazione (1,8 e 1,2 BTC), debbono essere ritenuti dello stesso proprietario secondo l'euristica *multiaddress*; gli *output* sono facilmente distinguibili, dal momento che l'ammontare di 2 BTC è trasferita a un indirizzo noto agli inquirenti, e che 1 BTC non può che essere il resto, in accordo con la *optimal change heuristic*; che 2 BTC è esattamente il corrispettivo che Tizio richiedeva nel suo prezziario per prestazioni analoghe, come dimostrano i messaggi rinvenuti sul profondo *web*. Gli elementi di prova così raccolti darebbero luogo a un quadro indiziario davvero fragile, se non fossero corroborati da tutti gli altri mezzi di ricerca della prova. L'approfondimento istruttorio sarà possibile ottenendo un provvedimento giudiziale[85] che autorizzi ispezioni e perquisizioni nei confronti di Caio, finalizzati al sequestro probatorio degli strumenti informatici utilizzati per commettere il reato. Gli inquirenti avranno altresì la possibilità di svelare l'identità di Tizio, risalendo a questi tramite i messaggi telefonici o telematici scambiati con il "committente".

Risulta evidente, dalle considerazioni che abbiamo svolto, l'importanza della *blockchain forensics* dell'*open source intelligence* per il buon esito delle indagini in procedimenti collegati all'utilizzo delle valute virtuali. La combinazione di queste innovative tecniche d'indagine con gli ordinari mezzi di ricerca della prova arricchisce lo strumentario processuale, adeguandolo alle nuove tendenze della criminalità economica.

5.1. Tra *publicly available data* e *legitimate expectation of privacy*. Considerazioni in ordine alla necessità di una base normativa per le indagini OSINT.

Le attività di *intelligence* su dati pubblicamente accessibili rischiano di divenire un espediente di sorveglianza massiva "ad alto contenuto tecnologico". Secondo una parte della dottrina il solo fatto che i dati siano pubblicamente accessibili non implica la totale assenza di limiti all'operato dei pubblici agenti[86] e non esonera dal domandarsi quale sia la base giuridica per il compimento delle predette attività e quali le condizioni legittimanti il ricorso alle indagini OSINT.

Guardando in particolare alle interferenze con il diritto alla riservatezza, viene in rilievo non soltanto l'esigenza di una base normativa sufficientemente chiara in funzione di garanzia – per individuare i presupposti e le modalità di esercizio del potere – ma anche la necessità di prevedere misure di protezione dei dati e affidabilità delle procedure di informatica forense.

[85] Gli elementi di prova acquisiti *open source* – specie quando risultano precisi e concordanti, come nel caso in esame – sono un fondato motivo (art. 247 c.p.p.) per ritenere che il corpo del reato o le cose ad esso pertinenti si trovino indosso all'indagato o nel suo domicilio, tale da giustificare l'emissione di un decreto motivato di ispezione, perquisizione o sequestro probatorio

[86] In argomento KOOPS, *Police investigations in Internet open sources,* cit., 655

Esaminata da questa prospettiva, la questione assume una piega del tutto peculiare. In particolare, l'assunto secondo cui la raccolta e l'elaborazione di *open access* si muovono in una zona franca da vincoli e restrizioni si rivela decisamente fragile[87].

Se è vero che l'individuo gode di una legittima aspettativa alla *privacy* anche quando si muove in un contesto pubblico, dovrebbe parimenti ammettersi che l'informazione personale collocata nello spazio virtuale, sebbene pubblicamente accessibile, non possa essere visualizzata e utilizzata dal mondo intero[88]. Applicando un tale principio alle investigazioni *online*, dovrebbe ritenersi legittima l'aspettativa degli utenti a che la polizia non controlli tutto ciò che vaga su Internet, specie laddove l'indagine sia condotta mediante sofisticati *software* di ricerca e analisi dei risultati[89]. A ben vedere, la polizia giudiziaria agisce in veste istituzionale anche quando compie un'attività che qualsiasi cittadino potrebbe svolgere. Sicché, anche il trattamento di dati *open access* dovrebbe essere ricondotto alla normativa processuale che disciplina le condizioni e i limiti per l'esercizio dei pubblici poteri.

Secondo la lettura fornita dalla Corte di Strasburgo, la tutela offerta art. 8 CEDU copre anche gli aspetti della vita privata visibili al pubblico, in relazione all'utilizzo che i pubblici poteri fanno delle informazioni personali. In una pronuncia ormai risalente il collegio aveva ritenuto che la raccolta e la conservazione in modo continuo e sistematico di dati pubblicamente accessibili, in assenza di una adeguata base normativa, integrasse una violazione del diritto alla vita privata[90]. Nel bilanciamento tra i contrapposti interessi può ritenersi che determinate modalità di ricerca e raccolta di dati *open access* interferiscano con il diritto alla *privacy* dell'interessato. Si propone così una distinzione tra le consultazioni effettuare manualmente e *una tantum*, e le indagini ad alto contenuto tecnologico eseguite mediante sofisticati strumenti di indagine. Queste ultime dovrebbero soddisfare i requisiti previsti dall'art. 8, par. 2, CEDU, che postula l'esistenza di una base normativa a fondamento dell'azione della

[87] La pubblicità del dato potrebbe infatti indurre a credere che, come il *quivis de populo*, anche la polizia dovrebbe poter accedere all'informazione in libertà e utilizzarla per nello svolgimento della propria attività istituzionale.

[88] Si richiama ancora una volta la tesi di KOOPS, *Police investigations in Internet open sources*, cit., 657 secondo cui la dottrina sulla *legitimate expectation of privacy* trova piena applicazione anche alle indagini su Internet. Nel prosieguo del paragrafo ci atterremo al pensiero dell'Autore per illustrare i termini della questione.

[89] Sarebbe pertanto erroneo paragonare tali programmi di *data analytics* alla lente d'ingrandimento utilizzata dal *detective* per l'ispezione di luoghi pubblici. In questo secondo caso lo strumento di analisi non consente la profilazione dell'individuo né rischia di comprometterne la riservatezza.

[90] CEDU, 4 May 2000, Rotaru v. Romania, App.no. 28341/95, § 43, in https://hudoc.echr.coe.int. Il ricorrente denunciava la violazione del diritto al rispetto della vita privata a causa dell'utilizzo da parte dei servizi segreti rumeni di un fascicolo contenente informazioni personali sulle proprie opinioni politiche, risalente al periodo della dittatura comunista in Romania, in assenza di una sufficiente base normativa: *«In the applicant's submission, the keeping and use of the file on him were not in accordance with the law, since domestic law was not sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities were empowered to file information on their private life and make use of it. Furthermore, domestic law did not define with sufficient precision the manner of exercise of those powers and did not contain any safeguards against abuses. […] Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past».*

pubblica autorità per fini di prevenzione e repressione dei reati[91]. Negli ordinamenti in cui i servizi di *intelligence* utilizzano complessi programmi e apparecchiature informatiche sarebbe dunque opportuno disciplinare in modo specifico le condizioni e i limiti delle operazioni OSINT[92].

5.2. Indagini *open source* e protezione dei dati personali nelle attività di contrasto.

Nell'ordinamento processuale italiano non esiste alcuna disposizione che disciplini in modo specifico i poteri della polizia giudiziaria e l'utilizzabilità degli elementi di prova acquisiti *open source*. Pur essendo auspicabile, sulla scorta di quanto finora osservato, regolare l'utilizzo degli strumenti più intrusivi per la riservatezza dell'individuo, occorre tuttavia dar conto dell'esistenza di una base normativa che, sia pur indirettamente, ammette il ricorso a detti strumenti.

Sul piano della cooperazione investigativa, la Convenzione di Budapest disciplina l'accesso transfrontaliero ai dati informatici dettando alcune deroghe ai principi generali sull'acquisizione della *digital evidence*. Le autorità investigative devono limitare le ricerche alle fonti disponibili nel territorio dello Stato, salvo che si tratti di «*publicly available (open source) stored computer data, regardless of where the data is located geographically»* oppure sia acquisito il consenso del soggetto che abbia il diritto di comunicarli (art. 32)[93]. In questi casi l'acquisizione della prova non richiederà alcuna autorizzazione preventiva, mancando una, sia pur minima, ingerenza sulla sovranità statale; i paesi firmatari hanno inteso così eliminare ogni aggravio procedimentale nell'accesso ai dati archiviati in *server* stranieri. Il regime di libero accesso non risolve però il *core* del problema, rappresentato dall'incidenza delle attività di *intelligence* sulla vita privata dell'individuo. Tanto la preoccupazione per la mancanza di una base normativa, quanto il rischio di una eccessiva limitazione della *privacy* degli interessati, risultano oggi superati – o quantomeno attenuati –

[91] Cfr. KOOPS, *Police investigations in Internet open sources,* ibidem. Secondo l'Autore le ricerche meno invasive potrebbero anche non richiedere la previa emanazione di una normativa *ad hoc*, ben potendo i cittadini prevedere che la polizia avrà accesso ai dati *open source* sulla base delle disposizioni che regolano l'attività ordinaria di ricerca di fatti e circostanze di reato. Diversamente, per lo svolgimento di indagini a lungo termine che comportano una inevitabile intrusione nella vita privata, sarebbe necessaria una specifica disciplina legale.

[92] Vi sarebbero evidenti implicazioni sul piano dell'utilizzabilità della prova nei procedimenti penali. Sebbene i risultati delle indagini *open source* integrino soltanto degli elementi di prova, la teoria dell'illegittimità derivata dovrebbe precludere l'ingresso nel processo delle evidenze che non sarebbero state *aliunde* acquisite.

[93] La disposizione non chiarisce, tuttavia, cosa si intenda per "dati pubblicamente accessibili". Se da una parte la nozione sembrerebbe far riferimento ai soli dati immediatamente accessibili (ad esempio, sul web senza alcuna restrizione di accesso), dall'altra potrebbe includere anche quelli ad accesso semi ristretto (es. files accessibili ai soli utenti registrati) La specificazione *open source*, utilizzata a complemento della locuzione *publicly available*, rappresenta probabilmente un compromesso raggiunto durante i lavori redazionali. Soltanto in tempi recenti è stato chiarito che l'accesso riguarda tutti i dati a cui il pubblico può accedere, motivo per cui le forze dell'ordine possono anche registrarsi per i servizi offerti al pubblico. Cfr. *Transborder access to data and jurisdiction: Options for further action by the T-CY*, 3 dicembre 2014, in https://rm.coe.int, 17 ss.

dall'esistenza di una disciplina di dettaglio sulla protezione dei dati personali nelle attività di contrasto. Come noto la Direttiva 680/2016/UE, approvata contestualmente al Regolamento Generale, ha armonizzato la materia del trattamento dei dati delle persone fisiche da parte delle autorità competenti *«a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica»* (art. 1), applicando i principi fondamentali in materia di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile acquisite nel corso di un procedimento penale[94].

Non sembra potersi dubitare dell'applicabilità delle disposizioni della direttiva alle operazioni OSINT, dovendo aversi riguardo *«all'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici»*[95], nonché a *«qualsiasi operazione o insieme di operazioni compiute nei confronti di dati personali o insiemi di dati personali per tali finalità, con l'ausilio di strumenti automatizzati o in altro modo»*[96]. La portata garantistica della direttiva emerge dall'affermazione secondo cui il trattamento dei dati personali dovrebbe essere lecito, corretto e trasparente e perseguire unicamente fini specifici previsti dalla legge, dovendo il titolare assicurare che la raccolta dei dati personali non sia eccessiva e che i dati siano conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (considerando n. 26). La nozione di "trattamento" include *inter cetera* anche le attività di raccolta, strutturazione, adattamento, estrazione, consultazione, raffronto e interconnessione[97], con cui solitamente vengono svolte le indagini di *blockchain forensics*.

Con il D. Lgs. 18 maggio 2018 n. 51 il legislatore italiano ha dato attuazione agli obblighi comunitari riproducendo in modo piuttosto fedele il testo della direttiva 680/2016/UE. Occorre peraltro ricordare come qualche mese prima dell'entrata in vigore del decreto è stato emanato il DPR 15/2018[98], che ammette genericamente la

[94] Gli Stati membri sono obbligati al rispetto dei principi secondo cui: i dati personali nell'ambito delle attività di contrasto devono essere raccolti per finalità determinate, esplicite e legittime; trattati in modo lecito e corretto, per finalità pertinenti e non eccedenti rispetto alle finalità indicare all'art. 1; il titolare del trattamento deve adottare misure tecniche e organizzative per impostazione predefinita a tutela del dato. La direttiva offre una serie di tutele all'interessato per quanto riguarda l'accesso, la rettifica e la cancellazione dei dati, oltreché la facoltà di chiedere limitazioni al trattamento in determinati casi. Disposizioni particolari sono infine previste con riferimento al diritto all'indennizzo in caso di danno conseguente a un trattamento che abbia violato le regole in materia di trasferimento a Stati terzi dei dati personali e di incauta gestione.

[95] Così il considerando n. 21 alla direttiva.

[96] Cfr. Considerando n. 34 alla direttiva. A conferma della rilevanza dei principi sul trattamento dei dati alle attività di OSINT il precedente considerando n. 27 stabilisce una sorta di fondamento legale per la raccolta ai fini di prevenzione, indagine, accertamento o perseguimento di specifici reati al fine di *«sviluppare conoscenze delle attività criminali e mettere in collegamento i diversi reati accertati»*.

[97] Cfr. Art. 3 n. 2 della Direttiva; Art. 2 lett. b) D. Lgs. 51/2018.

[98] Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15 (Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati

raccolta e il trattamento dei dati personali quando ciò sia necessario per un'attività informativa, di sicurezza o di indagine di polizia giudiziaria o di tutela dell'ordine e della sicurezza[99].

Nell'ordinamento vigente le operazioni di *open source intelligence* sono dunque sottoposte ai vincoli dalla normativa di settore, frutto di un razionale bilanciamento delle contrapposte esigenze. Le limitazioni al trattamento dei dati non eliminano però del tutto la preoccupazione di una generalizzata *mass surveillance*, né rendono superflua l'emanazione di una disciplina *ad hoc* sull'utilizzo degli strumenti tecnologici di più significativo impatto sulla vita privata dei cittadini. In una società sempre più digitalizzata e interconnessa, in cui il dominio pubblico dell'informazione diviene la regola – anziché l'eccezione – non può che guardarsi con favore l'eventualità di un intervento del legislatore in chiave garantistica, al fine di individuare i presupposti oggettivi e soggettivi per la raccolta e l'analisi continua e sistematica dei dati personali dispersi nella rete[100].

6. Gestione accentrata di fondi: gli *exchange provider* e l'acquisizione della prova digitale.

In molti casi i trasferimenti in valuta virtuale vengono gestite dagli utenti grazie ai servizi offerti dalle piattaforme di scambio (*exchange provider*) o dai gestori di portafogli virtuali (*hot wallet*). Questi operatori mettono a disposizione alcuni *software* di semplice utilizzo per inviare, ricevere e scambiare valori virtuali, a fronte del pagamento di ridotte commissioni su ciascuna transazione. Negli ultimi tempi, anche a causa della proliferazione di nuovi *token* virtuali, sono entrati sul mercato molti nuovi fornitori di servizi. Il legislatore europeo ha colto l'occasione per estendere a detti operatori professionali gli obblighi previsti dalla normativa antiriciclaggio[101], nella consapevolezza del ruolo fondamentale che essi rivestono nell'economia virtuale.

---

effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia). Ai sensi dell'art. 49, comma, 3 del D. Lgs. 51/2018 i decreti adottati in attuazione degli articoli 53 e 57 del Codice della *privacy* continuano ad applicarsi fino all'adozione di diversa disciplina.

[99] Il Decreto prevede, peraltro, una serie di limiti e condizioni quali ad esempio il fatto che i sistemi informativi e i programmi informatici debbano essere configurati in modo da ridurre al minimo l'utilizzo di dati personali e identificativi (art. 5); che i dati raccolti per esigenze temporanee o in relazione a situazioni particolari direttamente correlate all'esercizio dei compiti di polizia di prevenzione dei reati, possano essere conservati per un periodo di tempo non superiore a quello necessario e, comunque, non oltre 10 anni dalla cessazione dell'esigenza o della situazione particolare che ne hanno reso necessario il trattamento (art. 8).

[100] Si condivide, sul punto, il pensiero di SORO A., *Tra privacy e open data intesa possibile*, in *Il Sole24Ore*, 13 ottobre 2014, di «*definire un punto di equilibrio tra apertura del patrimonio informativo pubblico e protezione dei dati personali e al contempo suggerire, in modo costruttivo, alcune possibili modalità perché tale obiettivo venga concretamente perseguito, consapevoli che anche investendo su soluzioni tecnologiche, c'è spazio per contemperare le esigenze di tutela della privacy e di accesso pubblico alle informazioni*».

[101] *Amplius*, Cap. III, § 3.2.

A nostro avviso, i prestatori di servizi connessi all'utilizzo delle valute virtuali costituiscono un *centro di recupero* dell'intermediazione in un mercato tendente alla decentralizzazione degli scambi e rappresentano una *figura-ponte* tra le logiche del vecchio sistema e la rivoluzione innescata dall'impiego della tecnologia a registro diffuso. Sul versante processuale, l'esistenza di un intermediario negli scambi e nella tenuta dello storico delle operazioni accresce notevolmente i poteri di indagine e, al contempo, offre una occasione aurea per fare breccia nell'egida dell'anonimato che difende i criminali informatici. Tanto premesso, soffermeremo ora la nostra attenzione sulle questioni relative all'acquisizione della prova, rinviando al paragrafo seguente quelle concernenti l'esecuzione di misure cautelari reali su valori virtuali.

Il riferimento normativo da cui partire è indubbiamente l'art. 254-*bis* c.p.p., introdotto dalla legge di ratifica della Convenzione di Budapest[102] per adeguare l'ordinamento processuale interno agli obblighi indicati dall'art. 18, comma 2, della Convenzione, secondo cui ciascuno Stato aderente deve adottare «*le misure legislative e di altra natura che dovessero essere necessarie per consentire alle autorità competenti di ordinare […] a un fornitore di servizi che offre le proprie prestazioni nel territorio della Parte di fornire i dati in proprio possesso o sotto il suo controllo relativi ai propri abbonati e concernenti tali servizi*», con la precisazione che con l'espressione *informazioni relative agli abbonati* si intende ogni informazione detenuta in forma di dato informatico attraverso la quale è possibile stabilire *«l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento».*

La norma attribuisce all'autorità giudiziaria il potere di disporre[103] il sequestro (probatorio) presso fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, e di stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi[104], che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti agli originali e la loro immodificabilità.

Ai fini della nostra analisi, si tratta anzitutto di comprendere se la locuzione «fornitori di servizi informatici, telematici o di telecomunicazioni» possa ricomprendere anche i prestatori di servizi connessi all'utilizzo delle valute virtuali. Sul piano testuale, la formulazione è molto ampia, e non circoscrive entro limiti precisi l'ambito di operativo della disposizione. In particolare, il riferimento ai fornitori di

[102] Cfr. Art. 8, comma 5, della legge 18 marzo 2008 n. 48

[103] Secondo MACRILLÒ, *Le nuove disposizioni in materia di sequestro probatorio e di custodia ed assicurazione dei dati informatici*, cit. 512 il legislatore, con la disposizione in commento, ha voluto ribadire espressamente l'utilizzabilità del sequestro probatorio per apprendere tutti i dati informatici in possesso dei gestori, ed ha altresì indicato mediante l'utilizzo della locuzione «quando dispone» le precise modalità con cui tale operazione, già concepita dall'art. 254 con riferimento alla corrispondenza, debba avvenire.

[104] Cfr. VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, cit., 112, secondo cui la disposizione mira a contemperare l'esigenza di ricerca della prova con la necessità di garantire ai *provider* la possibilità di continuare ad assicurarne la regolare fornitura dei servizi informatici, telematici e di telecomunicazione.

servizi informatici sembra estendere il raggio d'azione della norma a tutti quei servizi relativi alla *società dell'informazione*, offrendo un argomento decisivo per l'inclusione degli *exchange provider* nella macrocategoria dei fornitori di servizi informatici o telematici. Non essendovi alcuna nozione valida a fini penalistici, si dovrà giocoforza fare riferimento alla normativa extrapenale, e in particolare alle definizioni contenute nella normativa sulla fornitura di servizi nella società dell'informazione[105], che confermano l'assunto di partenza. Difatti, i prestatori di servizi connessi all'utilizzo delle valute virtuali svolgono una attività dietro retribuzione (sia pur sotto forma di commissioni di transazione), a distanza, per via elettronica, *online* e a richiesta individuale di un destinatario.

Una seconda questione riguarda l'oggetto del sequestro probatorio, che la norma riferisce ai dati informatici detenuti dai *provider*, compresi quelli di traffico o di ubicazione. *Nulla quaestio* rispetto ai dati identificativi dell'utente, allo storico delle transazioni e delle operazioni compiute sulla piattaforma, sia in moneta *fiat* sia in moneta virtuale, che indubbiamente rientrano nell'ambito oggettivo della disposizione. Più complesso è invece l'inquadramento della criptomoneta come oggetto del sequestro probatorio di cui all'art. 254-*bis*. Al fine di scongiurare il rischio di interpretazioni estensive, ci si chiede se nel concetto di dato informatico rientri o meno la moneta virtuale. All'interrogativo non può che darsi risposta affermativa. A ben vedere, il *provider* di servizi di cambio o portafoglio virtuale non possiede, in senso tecnico, la moneta virtuale, ma si limita a custodire le chiavi crittografiche private dell'utente e a offrire una interfaccia grafica per la relativa gestione. Una chiave di criptazione non è altro che una stringa alfanumerica complessa, un insieme di bit che costituisce un dato informatico secondo la definizione corrente[106]. Il generico riferimento ai «dati» detenuti dai *provider* appare dunque sufficiente a fondare il potere dell'autorità giudiziaria di disporre il sequestro presso le piattaforme di scambio, a fini probatori, della valuta virtuale. La natura provvisoria del *sequestro de qua* (art. 262 c.p.p.), finalizzato all'acquisizione di una prova rilevante ai fini delle indagini, ammette che siano sottoposte alla misura anche valori virtuali appartenenti a terzi, non concorrenti nel reato. Così, nel caso in cui una transazione sia illecita soltanto *ex latere mittentis* (si pensi alla consumazione di un autoriciclaggio mediante l'acquisto di beni di consumo pagati con un ammontare di moneta virtuale proveniente da reato), il

[105] L'art. 1, comma 1, lett b) della legge 21 giugno 1986, n. 317 definisce «servizio: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»; successivamente, l'art. 2, comma 1, del D. Lgs. 70/2003 (Codice del commercio elettronico) ha definito i servizi della società dell'informazione come «le attività economiche svolte in linea - *online* - nonché i servizi definiti dall'articolo 1, comma 1, lettera b), della legge 21 giugno 1986, n. 317», e il prestatore come «la persona fisica o giuridica che presta un servizio della società dell'informazione».

[106] L'art. 1, par. 1, lett. b) della Convenzione di Budapest definisce dato informatico «qualunque rappresentazione 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». In informatica, il dato è una informazione elementare, codificabile o codificata (così l'Enciclopedia Treccani online, voce «Dato»). Per approfondimenti, BORRUSO R. – RUSSO S. TIBERI C, *L'informatica per il giurista. Dal bit a internet*, Milano, 2009, 36 ss.

sequestro probatorio potrà essere ordinato anche al fornitore di servizi del ricevente, fermo il dovere di restituzione quando non sarà più necessario mantenere il sequestro ai fini della prova.

L'acquisizione dei dati informatici dovrà avvenire «*mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*»[107]. A tal fine i prestatori di servizi potranno avvalersi delle tecniche di copiatura (*mirroring*) e di criptazione (*hashing*) in precedenza esaminate.

Si deve tuttavia precisare che sequestro avente ad oggetto la valuta virtuale dovrà essere disposto con modalità tali da garantire altresì la *indisponibilità* da parte dell'utente. La semplice copiatura e consegna dei dati relativi alle chiavi private non vale di per sé a privare l'utente della disponibilità del denaro, poiché questi potrebbe in ogni momento accedere al conto per inviare su altro indirizzo i propri averi virtuali, frustrando così le esigenze probatorie. Per questo motivo, sarà bene che il decreto di sequestro disciplini in modo preciso le modalità esecutive della misura, specificando, ad esempio, che l'accesso all'area personale dell'utente destinatario del provvedimento dovrà essere bloccato. L'art. 254-*bis* fornisce una copertura normativa anche a questi obblighi, prevedendo, all'ultimo periodo, che l'autorità debba comunque ordinare «*al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali*». L'adozione di misure di protezione non esaurisce però tutti i problemi legati all'indisponibilità del denaro, tema a cui dedicheremo ampio spazio nel paragrafo che segue.

Nel caso in cui i fornitori di servizi abbiano sede legale o *server* collocati all'estero, l'accesso transfrontaliero ai dati sarà ammesso in modo diretto soltanto nei casi previsti dall'art. 32 della Convenzione di Budapest[108]; in tutti gli altri casi si farà riferimento alla procedura di mutua assistenza per l'accesso a dati informatici, basata sugli ordinari strumenti di cooperazione internazionale (art. 31)[109] e, in caso di urgenza, a quella relativa alla rapida conservazione dei dati (art. 29)[110]. Tra Stati membri dell'Unione

[107] Della genuinità e della immodificabilità della prova digitale abbiamo già parlato a proposito della perquisizione (v. *supra*, § 4).

[108] *Supra*, § 5.2. Di recente gli stati membri del Consiglio d'Europa hanno avviato le negoziazioni per un protocollo addizionale alla Convenzione di Budapest. La commissione incaricata ha reso preannunciato che ci saranno delle novità significative per quel che riguarda la cooperazione diretta con i *provider*. Per approfondimenti, si rinvia al sito Internet istituzionale: https://www.coe.int/web/cybercrime/t-cy-drafting-group

[109] La norma prevede che uno Stato possa richiedere la perquisizione, il sequestro o la comunicazione dei dati immagazzinati in un sistema informatico situato nel territorio della Parte richiesta. Quest'ultima è tenuta ad onorare la richiesta osservando gli accordi internazionali e in conformità alle disposizioni della Convenzione stessa. La richiesta deve essere soddisfatta al più presto possibile quando vi sia motivo di ritenere che i dati siano particolarmente a rischio di perdita modificazioni, o quando gli accordi fissino un termine breve per il compimento delle predette operazioni.

[110] Ai sensi dell'art. 29 della Convenzione ciascuno stato può presentare una richiesta, rivolta ad altro Stato, per far sì che questi ordini o ottenga in altro modo la conservazione rapida di dati immagazzinati in un sistema informatico, situato nel territorio della parte destinatari. La richiesta deve specificare: l'autorità che richiede la conservazione; il reato che costituisce oggetto di indagine e una breve esposizione dei fatti relativi; i dati informatici immagazzinati da conservare e il loro legame con il reato;

Europea la materia è disciplinata dagli artt. 82 ss. TFUE; troveranno quindi applicazione le più snelle procedure di cooperazione giudiziaria previste dalla Direttiva 2014/41/UE relativa all'ordine europeo di indagine penale, o dal Regolamento (UE) 2016/794 che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol).

7. Sequestro e confisca di valuta virtuale.

Nella trattazione pregressa l'attenzione è stata rivolta all'utilizzo del sequestro come mezzo tipico di ricerca della prova, esaminando le varie questioni che potrebbero profilarsi quando esso abbia ad oggetto sistemi, dati o programmi informatici utilizzati per il trasferimento e lo scambio di valute virtuali. Vi sono altri casi in cui la necessità di sottrarre all'indagato il possesso delle valute derivi dal pericolo che la libera disponibilità di queste possa aggravare o protrarre le conseguenze del reato o agevolare la commissione di altri reati (art. 321, comma 1, c.p.p.), oppure dall'opportunità di creare un vincolo in vista della futura confisca (art. 321, comma 2, c.p.p.).

Ai sensi dell'art. 240 c.p., in caso di condanna il giudice può ordinare la confisca delle cose che servirono o furono destinate a commettere il reato, e delle cose che ne sono il prodotto o il profitto (confisca c.d. facoltativa). La misura di sicurezza è sempre ordinata quando sia stato pagato un prezzo per la commissione del reato (c.d. confisca obbligatoria). Inoltre, con una recente modifica è stato aggiunto alla disposizione un nuovo comma 1-*bis*, in forza del quale è prevista la confisca obbligatoria dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione di reati informatici ivi indicati, nonché dei beni che ne costituiscono il profitto o il prodotto, anche per equivalente[111]. In tutti gli altri casi, invero piuttosto residuali, la confisca sarà soltanto *facoltativa*.

---

tutte le informazioni utili ad identificare il custode dei dati informatici immagazzinati o il luogo dove si trova il sistema informatico; gli elementi da cui ricavare la necessità della conservazione; l'allegazione che la Parte intende avanzare una richiesta di mutua assistenza per la perquisizione, il sequestro o altro strumento similare. Dopo aver ricevuto la richiesta, la Parte richiesta dovrà prendere tutte le misure appropriate per conservare rapidamente i dati, agendo in conformità alla propria legge nazionale. Per rispondere ad una tale richiesta, la doppia incriminazione non è richiesta come condizione per provvedere alla conservazione, salvo il diritto di rifiutare la richiesta di conservazione qualora il reato non rientri tra quelli indicati nella parte sostanziale della Convenzione.
La conservazione dovrà essere imposta per un periodo non inferiore a sessanta giorni, al fine di permettere alla Parte richiedente di attivare gli strumenti di mutua assistenza.

[111] Pertanto, ogniqualvolta il reato sia connesso all'utilizzo di valuta virtuale, sarà *obbligatoria* la confisca: (i) del prezzo del reato, cioè del corrispettivo dato o pagato per la commissione del reato (es. acquisto di una partita di droga; corrispettivo per la realizzazione di un crimine su commissione); (ii) del prodotto o del profitto, anche per equivalente, di un reato necessariamente informatico, intendendosi per tali ogni utilità economica che derivi in via diretta dalla commissione dell'illecito (es. Bitcoin ottenuti a seguito del pagamento del riscatto di un *ransomware*); (iii) per i reati di riciclaggio, reimpiego e autoriciclaggio (es. *cyberlaudering*), ovvero di danneggiamento informatico che riguardi tre o più sistemi (es. creazione di una *botnet* su larga scala per sfruttare potenza computazionale di sistemi altrui), dei beni di cui il condannato non può giustificare la provenienza e di cui abbia la disponibilità personalmente o per interposta persona, anche per equivalente. *Ampius,* Cap. III, § 7 ss.

A diverse esigenze risponde il sequestro conservativo, che sarà disposto quando vi sia fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della pena pecuniaria, delle spese del procedimento o di altre somme dovute (art. 316 c.p.p.).

Quale che sia la forma giuridica del sequestro cautelare avente ad oggetto la valuta virtuale, è necessario sottolineare le notevolissime criticità che si pongono sul piano esecutivo per la creazione di un reale vincolo di indisponibilità e per la conservazione dei valori. Inoltre, l'esecuzione della misura seguirà procedure differenti a seconda che la criptovaluta sia depositata su una piattaforma di scambio, ovvero sia contenuta in portafogli privati. Per esigenze di coerenza espositiva, ci occuperemo dapprima di quest'ultimo caso, assai più complesso.

Il punto di partenza per un corretto inquadramento della questione risiede nella definizione di sequestro rilevante nell'universo delle valute virtuali come «*movement of bitcoins or altcoins from a suspect's address to an address controlled by law enforcement*»[112]. Il dirottamento dei valori virtuali su un indirizzo controllato dall'autorità giudiziaria è l'unico modo per assicurare il definitivo spossessamento della ricchezza dalle mani del reo. Il sequestro dell'apparecchiatura informatica (*smartphone*, *laptop*, *personal computer*) su cui sono registrati i *software* di gestione è facilmente eludibile grazie all'utilizzo di una chiave di recupero (*backup recovery seed*)[113], che molti servizi di *storage* offrono per rimediare alla perdita o alla distruzione accidentale dell'*hardware.* Ciò consente all'interessato di recuperare in ogni momento la disponibilità delle somme, facendo cadere nel vuoto il vincolo reale imposto dall'autorità.

A differenza della moneta elettronica, che è registrata su circuiti gestiti da terzi intermediari, la creazione di un vincolo di indisponibilità definitiva sulla moneta virtuale richiederà un atteggiamento collaborativo da parte del reo. Eccezion fatta per quei rari casi in cui il portafoglio non è protetto da misure di sicurezza, di regola gli inquirenti si troveranno di fronte a *software applicativi* custoditi da una o anche più password crittografiche di accesso (*two-identifaction factor*), che neppure un esperto informatico forense potrebbe superare senza correre il rischio di un *backup* delle chiavi durante il tempo necessario per le operazioni di decifratura[114]. Quando sussistano le esigenze cautelari di cui agli artt. 316 e 321 c.p.p., la sottrazione della disponibilità del denaro virtuale dovrebbe avvenire nell'immediatezza delle operazioni di perquisizione, o comunque in tempo prossimo, dal momento che una dilazione eccessiva potrebbe

[112] «Advanced Course on the Search, Seizure, and Confiscation of Online Crime Proceeds», manuale didattico elaborato nell'ambito del progetto i-PROCEEDS del Consiglio d'Europa, cit., 59

[113] Cfr. «Bitcoin and Cryptocurrencies», rapport pubblicato dal Law Enforcement Cyber Center, cit., 12; KING D. – WARRACK P., *Real considerations for law enforcement in seizing virtual currency,* June 26 2016, in https://acamstoday.org

[114] Vi sono casi in cui il sistema di cifratura è così complesso da non poter essere tecnicamente superato; altri in cui, pur essendo in astratto possibile, richiederebbe dei tempi di lavorazione sufficientemente lunghi da permettere al reo di ripristinare le chiavi su un altro dispositivo e di dirottare le somme verso un nuovo indirizzo.

pregiudicare la possibilità di disporre il sequestro, per le ragioni anzidette. Per far fronte a questo pericolo, la volontaria *disclosure* delle chiavi di accesso da parte dell'interessato rappresenta la soluzione più rapida ed efficace per eseguire la misura, se non addirittura l'unica possibile. Nel caso in cui questi si rifiuti di collaborare e vi sia fondato motivo si ritenere che disponga di un chiave di recupero, ci si chiede se il silenzio dell'imputato possa giustificare l'emissione a suo carico di una misura cautelare personale, per evitare l'inquinamento probatorio o la commissione di reati della stessa specie di quello per cui si procede. Per espressa previsione dell'ultimo periodo dell'art. 274, comma 1, lett. a), le situazioni di attuale e concreto pericolo per l'acquisizione e la genuinità della prova[115] non possono essere desunte dal rifiuto dell'indagato di rendere dichiarazioni; nel caso *de quo* si potrebbe tuttavia argomentare che il pericolo derivi non tanto dal rifiuto di comunicare le chiavi di accesso, quanto piuttosto dal fondato timore dell'esistenza di una chiave di *backup*. Inoltre, l'impossibilità di disporre il sequestro a causa dell'atteggiamento non collaborativo dell'indagato, potrebbe concretizzare il pericolo di una recidiva nel reato nelle ipotesi previste dal secondo periodo dell'art. 274, comma 1, lett. c) c.p.p. Basti pensare ad un procedimento per riciclaggio, in cui vi sia motivo di ritenere che il reo disporrà nuovamente dei valori virtuali, ostacolando ulteriormente l'individuazione della provenienza delittuosa dei beni. Sembra quindi verosimile ritenere che il soggetto destinatario del sequestro sarà indotto a collaborare per il timore che vengano applicate nei suoi confronti misure di tipo custodiale.

Venendo alle modalità esecutive del sequestro, il vincolo si perfezionerà con l'invio della valuta su un indirizzo controllato dall'autorità giudiziaria o da un custode all'uopo nominato[116]. Ciò solleva ulteriori criticità relative alla conservazione delle valute oggetto del sequestro, che dovrebbero essere custodite in modo sicuro e con procedure che assicurino una non eccessiva svalutazione del loro valore nominale. Sul fronte della sicurezza, le *best practise*[117] consigliano di utilizzare *cold wallet* non connessi alla rete[118], oppure *hardware wallet* cifrati da custodire in cassaforte. Pur osservando le migliori cautele, rimane aperto il problema della volatilità del prezzo

[115] Il discorso vale anche quando il vincolo di indisponibilità sia imposto per esigenze probatorie ai sensi dell'art. 253 (si pensi all'ipotesi in cui l'accesso al *wallet* dell'indagato sia assolutamente necessario per prendere conoscenza dello storico delle transazioni).

[116] Nella recente vicenda collegata al fallimento dell'*exchange* italiano BitGrail, il Tribunale di Firenze ha disposto il sequestro oltre 2 mila Bitcoin (per un valore di quasi 15 milioni di Euro) che è stato eseguito dai coadiutori tecnici mediante l'invio del denaro su un portafoglio appositamente creato per la procedura fallimentare. In precedenza, già i pubblici ministeri presso il medesimo tribunale avevano disposto il sequestro dei valori virtuali del creatore della piattaforma, affidati a un duratore. Per la cronaca, FREDIANI C., *Così sono stati sequestrati 15 milioni di Euro di Bitcoin*, 09 giugno 2018, su https://agi.it; SELVATICI F., *Sequestrati i beni finanziari e virtuali del creatore di Bitgrail.com,* in *Repubblica.it,* 29 maggio 2018. La polizia postale aveva già eseguito con le stesse modalità il sequestro degli oltre 14.000 *wallet* localizzati sul mercato nero Babylon. Per i dettagli dell'operazione, http://www.interno.gov.it, sezione Notizie, 31 luglio 2015.

[117] Cfr. «Bitcoin and Cryptocurrencies», cit., 14

[118] Il deposito dei valori sequestrati in un portafoglio aperto su una piattaforma di scambio (*hot wallet*) alimenta il rischio di perdita accidentale per caso fortuito o per fatto illecito di terzi.

della criptomoneta, che, alla data di svincolo delle somme, potrebbe aver subito variazioni molto significative, sia verso l'alto sia verso il basso. In linea di principio, la misura cautelare dovrebbe essere eseguita con procedure che assicurano il "congelamento" del prezzo, in attesa della conclusione della decisione definitiva sulla responsabilità dell'imputato. A tale tesi si potrebbe obiettare che anche nelle ipotesi di sequestro di moneta avente corso legale non è prevista alcuna misura per rivalutare il *quantum* in base all'aumento o decremento dei prezzi al consumo. L'obiezione ci sembra tuttavia poco convincente. Tra le caratteristiche essenziali della moneta figura la stabilità del relativo prezzo[119], che si contrappone alla volatilità del valore nominale delle valute virtuali. Sarebbe dunque opportuno disciplinare a livello regolamentare le procedure che i pubblici ufficiali incaricati della custodia dovranno osservare per mantenere inalterato il prezzo dei valori sequestrati. Una possibile soluzione potrebbe essere quella di disporre la conversione forzosa della criptomoneta in *stablecoin* che abbiano un valore stabilmente ancorato al prezzo della moneta avente corso legale[120], ovvero, nei casi in cui ciò risulti concretamente impossibile[121], disporre la vendita dei beni sottoposto a sequestro al prezzo medio praticato sul mercato alla data del sequestro, mantenendo gli effetti del sequestro sul ricavato della vendita. Quest'ultima soluzione, che potrebbe risultare abnorme, costituisce in realtà voce di un principio generale dell'ordinamento processuale italiano, evincibile dagli artt. 260, comma 3, c.p.p. e 685, comma 1, c.p.c., che attribuiscono il potere al giudice competente di disporre l'alienazione dei beni deteriorabili sottoposti a sequestro.

In caso di condanna o di applicazione della pena ai sensi dell'art. 444 – qualora sia disposta la confisca dei valori preventivamente sottoposti a sequestro e nelle more non convertiti in moneta *fiat* – la vendita delle valute virtuali sarà l'espediente migliore per incamerare il ricavato e devolverlo ai capi di bilancio dello Stato individuati per legge[122].

Un caso indubbiamente particolare è quello dei *paper wallet,* vale a dire dei semplici fogli di carta con sopra appuntato l'indirizzo di portafoglio e la chiave privata ad esso associata, oppure un *QR code* da scannerizzare per ottenere i medesimi dati. I

[119] In argomento, LEMME G. – PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso Botcoin*, in *Rivista di diritto bancario*, 2016, 11, 36 ss.; VARDI N., *Criptovalute e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. inf.*, 2015, 2, 446.

[120] Ad esempio, la valuta Tether (USDT) ha un valore nominale legato in misura stabile al prezzo del dollaro americano e conta una grossa quantità circolante. Dalla data della sua emissione (inizio 2015) il prezzo ha avuto oscillazioni episodiche mai superiori al 10%; il tasso di cambio si è stabilizzato intorno ad Euro 0.87 per quasi tutto il periodo.

[121] Quando il sequestro è disposto su una ingente quantità di moneta virtuale, l'operazione di conversione in valuta stabile risulterebbe troppo complessa. Nessun acquirente, neanche le più grosse piattaforme di scambio, disporrebbero provvista sufficiente per concludere l'operazione.

[122] Cfr. Art. 2, comma 2, del decreto legge 16 settembre 2008, n. 143, convertito con modificazioni dalla legge 13 novembre 2008, n. 181. Negli Stati Uniti vi sono stati molti casi di vendita all'asta di Bitcoin sequestrati, in applicazione della legge federale che disciplina la vendita di strumenti finanziari sottoposti ad ablazione definitiva. Nella cronaca recente, SOLDAVINI P., *Il governo Usa non ci ha creduto: svenduti all'asta i bitcoin sequestrati*, in *IlSole24Ore*, 29 maggio 2017.

portafogli cartacei assolvono alla stessa funzione di una azione al portatore[123], consentendo a chi ne abbia il possesso di disporre dell'ammontare di moneta virtuale oppure di cederla per un corrispettivo in denaro avente corso legale. L'incorporazione dei dati digitali in un supporto cartaceo rende ancora più complesso individuare l'esistenza di valori da sottoporre a vincolo reale, ma agevola notevolmente l'esecuzione del sequestro. Una volta che il documento sarà nelle mani degli inquirenti basterà scansionare il codice per prendere controllo della valuta e indirizzarla verso il conto di destinazione.

Per quel che riguarda, infine, l'esecuzione della misura ablativa su valori affidati a fornitori di servizi di *storage online* (*hot wallet*) o di *exchange*, l'autorità giudiziaria potrà ordinare il blocco dell'*account* della persona sospettata e disporre che somme in esso contenute siano immediatamente dirottate su un indirizzo controllato dall'autorità; qualora il trasferimento non sia tecnicamente possibile a causa dell'attivazione di particolari misure di sicurezza[124], l'*exchange provider* si limiterà ad impedire l'accesso al conto, per tutto il tempo necessario ad ottenere la collaborazione dell'indagato.

7.1. *Key disclosure laws* e diritto al silenzio.

L'utilizzo della crittografia per l'archiviazione e la trasmissione dei dati informatici va di pari passo con la rilevanza che questi ultimi assumono nella moderna società dell'informazione. Esaminando il fenomeno dalla prospettiva del processo penale è stato acutamente osservato come la diffusione degli algoritmi di cifratura sia in realtà un'arma "a doppio taglio"[125], che ben di presta ad essere utilizzata dai cybercriminali per eludere qualsiasi possibilità di controllo statale.

I *software* di criptazione attualmente sul mercato, alcuni anche in versione gratuita, sono in grado di rendere le informazioni totalmente indecifrabili a chiunque non sia in possesso della chiave segreta. Non sorprende quindi che perfino le forze dell'ordine siano costrette a rinunciare all'acquisizione della prova digitale tutte le volte in cui la tecnica di cifratura assicuri un elevato livello di sicurezza[126]. Ne derivano non pochi problemi in termini di speditezza ed efficienza delle indagini poiché, in mancanza della collaborazione del titolare del sistema o del proprietario del dispositivo, il braccio

[123]Cfr. KING – WARRACK, *Real considerations for law enforcement in seizing virtual currency,* cit., che assimilano un portafoglio cartaceo ad una azione al portatore, esprimendosi nei termini seguenti. «Astute readers may realize that a paper wallet performs the same function as a bearer share, identified many years ago as being a money laundering risk. The person in possession of the paper owns the shares, or in this example, the virtual currency».

[124] Vi potrebbero essere dei casi in cui l'attivazione di un secondo fattore di autenticazione, i cui estremi non sono conosciuti dal *provider* (es. *Google Authenticator*), rende impossibile perfino al fornitore del servizio l'accesso all'area personale.

[125] Cfr. PALFREYMAN B. M., *Lessons from the British and American Approaches to Compelled Decryption*, in *Brooklyn Law Review*, 2009, 75, 1, 346

[126] FAKHOURY H., *A combination or a key? The Fifth Amendment and privilege against compelled decryption,* in *Digital Evidence and Electronic Signature Law Review*, 2012, 9, 81 ss.

armato dello Stato diverrebbe del tutto incapace di raccogliere le prove e provare in giudizio la colpevolezza dei responsabili.

Con la creazione della moneta *peer-to-peer* le difficoltà nel superamento delle barriere crittografiche assumono una portata ben più estesa, inverando uno scenario di totale dipendenza dalle scelte difensive dell'imputato.

Trattando dell'esecuzione delle misure ablative sui valori virtuali si è detto che tanto la possibilità di apprendere la ricchezza, quanto la buona riuscita delle indagini dipende spesso dalla volontà dell'indagato di cooperare con la giustizia mediante la consegna/rivelazione della chiave di criptazione. L'esito delle investigazioni informatiche risulta in tal modo condizionato dalla strategia processuale adottata dal destinatario della misura coercitiva. Visto che in questi casi la collaborazione dell'indagato potrebbe risultare decisiva, non è peregrino chiedersi se questi sia tenuto o meno a fornire le informazioni richieste dalla polizia giudiziaria.

Solitamente il primo contatto tra gli organi inquirenti e l'indagato avviene nel momento in cui viene eseguita la perquisizione e/o il sequestro delle apparecchiature informatiche[127]. Ipotizziamo che la polizia giudiziaria proceda all'acquisizione della prova in presenza del destinatario della misura e che, trovandosi di fronte a file cifrati, faccia richiesta del codice segreto. La dottrina[128] che ha affrontato la questione ritiene che la soluzione al quesito vada ricercata nei fondamentali canoni del processo penale e, in particolare, dal *principio nemo tenetur se detegere*, che porta ad escludere ogni onere collaborativo dell'indagato durante le indagini[129]. In tal senso, la richiesta da parte degli inquirenti di comunicazione della chiave segreta dovrà essere preceduta dall'avviso di cui all'art. 64, comma 3, lett. b) c.p.p., dovendo a tutti gli effetti essere considerata una dichiarazione resa durante l'acquisizione di sommarie informazioni dalla persona nei cui confronti vengono svolte le indagini (art. 350 c.p.p.). Sulla medesima lunghezza d'onda, altra parte della dottrina ritiene che la richiesta rivolta all'indagato di comunicare un codice di accesso non sia riconducibile alla disciplina dell'art. 248 c.p.p., dal momento che, in questi casi non vi è alcuna un bene materiale da consegnare, bensì una vera e propria domanda volta a conoscere l'informazione riservata che la persona sottoposta alle indagini ha diritto a mantenere segreta[130].

Occorre tuttavia riconoscere che in Italia lo stato del dell'arte sul tema risulta piuttosto immaturo se paragonato all'esperienza di altri ordinamenti. Nei sistemi di tradizione anglosassone le *key disclosure laws* indicano quelle norme di legge – previste in via statutaria o di creazione pretoria – che obbligano i destinatari di

[127] *Supra*, §§ 6 e 7

[128] BELLUTA H., *Cybercrime e responsabilità degli enti*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, 106; LUPARIA L., *Processo penale e tecnologia informatica*, in *Diritto dell'internet,* 2008, 226; PITTIRUTI M., Digital evidence *e procedimento penale*, Torino, 2017, 103 ss.

[129] PITTIRUTI, Digital evidence *e procedimento penale*, cit., 104, secondo cui, in assenza dell'avviso relativo alla facoltà di non rispondere, saranno inutilizzabili sia il dato raccolto, sia i successivi accertamenti operati sul sistema informatico.

[130] VENTURINI, *Sequestro probatorio e fornitori di servizi telematici*, cit., 133 (v. *supra*, § 4).

determinati provvedimenti giurisdizionali o di pubblica sicurezza a comunicare le chiavi crittografiche alle forze dell'ordine[131]. La *ratio* delle disposizioni è ovviamente quella di rendere il materiale fruibile per le operazioni di diagnostica forense e la successiva utilizzabilità in giudizio. L'obbligo gravante sul destinatario della misura – che potrà consistere nella rivelazione del codice segreto, oppure nella consegna di una copia non cifrata del *file* – è assistito da sanzioni penali in caso di inottemperanza[132].

Le leggi sulla *disclosure* delle chiavi di cifratura sono guardate con sfavore dalla dottrina più autorevole che non ha tardato a denunciarne l'inconciliabilità con il *privilege against self incrimination*[133] e, più in generale, con il diritto di silenzio[134]. La sacralità del principio è stata ribadita anche dalla Corte Europea dei diritti dell'uomo che in un noto *leading case* ha ricondotto la sua essenza alle garanzie del giusto processo di cui all'art. 6 CEDU[135].

Che il dovere di collaborazione con l'autorità si scontri frontalmente contro il principio *nemo tenetur se detegere,* è un dato difficilmente contestabile. Le *key disclosure laws* tentano infatti di risolvere quei casi in cui la polizia giudiziaria non potrebbe in alcun modo venire a conoscenza del contenuto dell'informazione criptata, se non attraverso la collaborazione dell'imputato[136].

Negli ordinamenti di *common law* il dibattito si è incardinato sulla natura testimoniale o meno delle dichiarazioni che l'imputato è tenuto a rendere per rivelare il codice di accesso[137]. Da un lato la comunicazione della password presenta forti similitudini con la consegna di una chiave fisica, poiché non riguarda fatti o circostante di natura valutativa. L'imputato non ha il potere di modificare l'informazione o

---

[131] In argomento v. KOOPS B.J., *The Crypto Controversy:A Key Conflict in the Information Society*, The Hague, 1999, 168 ss.; ID., *Commanding decryption and the privilege against self-incrimination*, in BREUR, M., KOMMER, J. F. *et al*. (editors), *New trends in criminal investigation and evidence*, Volume II, Antwerpen-Groningen, 2000, 431 ss.; SERGIENKO G., *Self Incrimination and Cryptographic Keys*, in *Richmond Journal of Law & Technology*, 1996, 2.

[132] HOLT D.T. BOSSLER A., SEIGFRIED-SPELLAR K., *Cybercrime and Digital Forensics: An Introduction*, London, 2015, 405 ss.

[133] Il privilegio contro l'autoincriminazione esprime il principio – internazionalmente riconosciuto – secondo cui la persona accusata di un delitto non può essere costretta ad autoaccusarsi o a fornire prove contro se medesimo. Ad esso fanno riferimento sia l'Accordo sui diritti civili e politici (articolo 14 par. 3, lett. g), sia lo Statuto della Corte penale internazionale (art. 55 par. 1, lett. a).

[134] Per approfondimenti v. KOOPS, *Commanding decryption and the privilege against self-incrimination*, cit., 434

[135] CEDU, *Saunders vs United Kingdom*, December 17th 1996, Application no. 19187/91 in cui la Corte ha ribadito che, sebbene non espressamente richiamati nell'art. 6, *«the right to silence and right not to incriminate oneself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6. Their rationale lies, inter alia, in the protection of the accused against improper compulsion by the authorities thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6».* Secondo i giudici di Strasburgo il fatto di poter rimanere in silenzio e non contribuire ad autoincriminarsi rappresenta il cuore pulsante della garanzia convenzionale.

[136] Nella maggior parte dei casi la prova diretta della responsabilità penale dei soggetti coinvolti sarà contenuta nel dispositivo protetto da crittografia; in tal caso il rifiuto di collaborare potrebbe segnare il *discrimen* tra la condanna e l'assoluzione.

[137] KOOPS, *Commanding decryption and the privilege against self-incrimination*, ibidem

immutare artificiosamente la realtà: il codice o funziona o non funziona, *tertium non datur*.

D'altro canto, però, il codice ha una esistenza che dipende dalla mente dell'indagato, tanto che se questi l'ha dimenticata o non ricorda il luogo di conservazione della *password*, non potrà in alcun modo cooperare con la polizia.

Si ritiene dunque che, indipendentemente dalla forma orale o materiale della delazione richiesta all'indagato, l'atto di rivelazione avrà in ogni caso natura testimoniale. Per stabilire se l'obbligo di *disclosure* violi o meno il diritto al silenzio occorre esaminare la tradizione giuridica di ciascun ordinamento ed esaminare la *ratio* e l'estensione di un tale principio.

7.2. Uno sguardo ai sistemi di *common law*. Il modello britannico.

Il Regno Unito ha adottato un approccio regolatorio molto rigoroso di fronte all'evoluzione della crittografia, tentando in più occasioni di risolvere il problema dell'accesso ai file protetti[138]. Nel 2000 con l'emanazione del *Regulation of Investigatory Powers Act* (RIPA) si è provveduto a un riordino delle disposizioni statutarie che disciplinano i poteri d'indagine; a qualche anno dall'entrata in vigore della legge il legislatore è intervenuto per modificare le disposizioni di decrittazione forzata, per rafforzare i presidi contro il rifiuto di collaborare con le autorità investigative[139].

La Parte III del RIPA, rubricata "Investigation of Electronic Data Protected by Encryption etc.", definisce una chiave crittografica come *«any key, code, password, algorithm or other data the use of which (with or without other keys) allows access to the electronic data, or facilitates the putting of the data into an intelligible form»*[140], dettando specifiche condizioni in presenza delle quali il governo può costringere i cittadini a consegnare il testo in chiaro dei documenti crittografati richiesti.

Occorre, anzitutto, che il testo cifrato sia ottenuto in modo legittimo, ad esempio a seguito del fruttuoso esperimento dei mezzi ordinari di ricerca della prova, previa autorizzazione dell'autorità giudiziaria, o nel corso della legittima intercettazione di

[138] Il governo britannico ha avviato varie procedure di consultazione e elaborato, a partire dal 1996, diverse proposte per regolamentare l'utilizzo della crittografia. Nei primi disegni di legge si tentava di risolvere il problema dell'accesso ai file criptati mediante l'istituzione *ex lege* di procedure di deposito delle chiavi presso terzi fornitori di servizi fiduciari, a cui le forze dell'ordine avrebbero potuto far riferimento per l'esecuzione dei mandati di perquisizione. Date le numerose proteste e le numerose criticità cui un simile approccio avrebbe dato luogo, la procedura di deposito delle chiavi è stata resa volontaria, imponendo però ai cittadini l'obbligo di decifrare i documenti in caso di ispezione da parte della polizia giudiziaria. Cfr. KOOPS, *Commanding decryption and the privilege against self-incrimination*, cit., 432.

[139] Lo statuto autorizza alcuni attori governativi, come la magistratura, la polizia di alto livello, i funzionari doganali e delle accise e gli ufficiali militari di costringere la decrittazione con minaccia di reclusione e multe per inosservanza.

[140] RIPA, § 56. Le disposizioni sull'interpretazione della legge definiscono l'informazione criptata come *«any electronic data which, without the key to the data cannot, or cannot readily, be accessed, or cannot, or cannot readily, be put into an intelligible form»*.

flussi di comunicazione (§ 49). Ad avviso della dottrina si tratta un presidio garantistico di estrema importanza poiché pone un limite contro possibili abusi di potere[141]. La misura potrà essere disposta nel solo caso in cui la chiave sia effettivamente in possesso della persona a cui viene notificato l'avviso e sussistano gravi motivi per imporre l'obbligo di decriptazione[142]. Deve inoltre essere rispettato il criterio di proporzionalità, nel senso che la limitazione alla libertà domiciliare e alla segretezza delle informazioni private deve poter essere bilanciata con il concreto interesse per l'amministrazione della giustizia[143]. *Last but non least*, la decriptazione forzata viene concepita come *extrema ratio*, a cui ricorrere soltanto nei casi in cui non vi siano alternative "ragionevolmente praticabili" per ottenere il testo in chiaro.

Al destinatario dell'avviso viene data la possibilità di consegnare la chiave crittografica anziché ostendere il testo chiaro (§ 50)[144]. Nel caso in cui l'indagato dichiari di aver smarrito il codice di accesso sarà tenuto a fornire tutte le informazioni utili affinché le forze dell'ordine riescano a recuperarne il possesso; laddove invece la polizia giudiziaria abbia un interesse specifico ad ottenere la chiave crittografica dovranno essere soddisfatte alcune condizioni ulteriori[145].

La sezione § 53 del RIPA criminalizza l'inottemperanza all'obbligo di decriptazione, comminando una pena fino a due anni di reclusione e la multa[146]. Sono tuttavia previste alcune *special defenses* per chi dimostri di non aver potuto rispettare l'obbligo di *disclosure* nel tempo stabilito o di non essere effettivamente in possesso della chiave. In questo secondo si aprirà un accertamento incidentale, nel quale la pubblica accusa dovrà dimostrare, al di là di un ragionevole dubbio, che l'indagato fosse effettivamente il possesso della *password*.

---

[141] PALFREYMAN, *Lessons from the British and American Approaches to Compelled Decryption*, cit., 364. Ad esempio, se un agente di polizia avesse sequestrato un *computer* in assenza di mandato, il governo non avrebbe il possesso legale di tale computer, e quindi non potrebbe costringere il destinatario della misura alla consegna del testo in chiaro. Viceversa, nel caso in cui l'ablazione sia legittima, l'indagato dovrà consegnare il testo in chiaro entro un ragionevole lasso di tempo. La mancata comunicazione costituisce reato, punito con la reclusione fino a due anni di carcere, che raggiunge i cinque anni nei casi che coinvolgono la sicurezza nazionale o la pornografia minorile. v. *Infra* .

[142] La sottosezione 3 della § 49 prevede, con formula molto ampia, che l'obbligo di disclosure possa esse imposto soltanto nell'interesse della sicurezza nazionale, al fine di prevenire o reprimere reati, o per il benessere economico del Regno Unito.

[143] L'interesse governativo ad ottenere il testo in chiaro dovrà pertanto essere uguale o superiore alla legittima aspettativa del cittadino a mantenere segrete le informazioni criptate.

[144] La facoltà dell'indagato di liberarsi dall'obbligo consegnando la *password* potrebbe dar luogo a criticità di non poco conto nel caso in cui l'ordine abbia ad oggetto un portafoglio digitale protetto da misure di sicurezza. Spesso questi ultimi hanno una chiave di accesso secondaria (*backup recovery key*) attraverso la quale il destinatario della misura potrebbe rientrare in possesso dei valori virtuali, facendo cadere nel vuoto l'attività di ricerca finalizzata al sequestro (*amplius,* §§ 4 e 7).

[145] La § 51 prevede che gli agenti di polizia possano richiedere la consegna della chiave soltanto quando ricorrono circostanze speciali, vale a dire quando lo scopo che si persegue con la misura sarebbe altrimenti frustrato. A tal fine gli organi inquirenti dovranno ponderare il rischio che le informazioni segrete possano essere divulgate con gli effetti negativi sull'attività esercitata dal destinatario della misura.

[146] *«A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice»* (§ 53, par.1).

La sezione successiva attribuisce rilevanza penale alle condotte di *tipping off*, consistenti nella violazione dell'obbligo di segretezza sul contenuto delle informazioni e sulla avvenuta ricezione dell'avviso *ex* § 49 nel caso in cui ciò possa pregiudicare le indagini oppure gli interessi e il benessere individuali[147].

La *key disclosure law* britannica ha trovato seguito anche in altri ordinamenti a tradizione giuridica anglosassone. In India la materia è regolata dalla sezione § 69 dell'Information Technology Act, introdotta nel 2008 nell'ambito di un più ampio intervento riformatore[148], che pone in capo a qualsiasi persona responsabile delle risorse informatiche l'obbligo di fornire l'accesso alle informazioni cifrate e di prestare alle forze dell'ordine tutta l'assistenza tecnica necessaria per acquisire copia dei dati informatici. Anche in questo caso l'inosservanza dell'obbligo di *disclosure* e il rifiuto di collaborare costituiscono reato e soggiacciono a sanzioni molto severe[149].

In Australia il Cybercrime Act del 2001 riconosce agli organi inquirenti il potere di ordinare ai privati la rivelazione dei codici di accesso ai sistemi informatici da utilizzare come prova in procedimenti giudiziari, e di imporre misure come la decriptazione forzosa. In caso di inottemperanza il destinatario del provvedimento è punito con la reclusione fino a sei mesi[150].

Le normative fin qui considerate tentano di ammorbidire la tensione con il privilegio contro l'autoincriminazione, disciplinando le condizioni in presenza delle quali la polizia giudiziaria può imporre l'obbligo di decriptazione. Ciò non risolve però il problema di fondo, dato dallo stridente binomio tra l'autoincriminazione in caso di confessione e la minaccia della pena in caso di rifiuto, che ha portato i primi commentatori a parlare di legge armate (*sledgehammer law*) progettata per rafforzare la sicurezza nazionale a scapito delle libertà civili[151].

---

147 *«A person who makes a disclosure to any other person of anything that he is required by a section 49 notice to keep secret shall be guilty of an offence and liable – (a) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both; (b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both»* (§ 54, par. 4).

148 SARVANKAR S., *Key Disclosure Laws and the Right Against Self-Incrimination in India*, 3 novembre 2017, in https://ssrn.com

149 *«The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall be liable to fine»* (§ 69, par. 4).

150 Cybercrime Act n. 161/2001 (8 Subsection 3L) che modifica il Crimes Act del 1914: *«The executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following: (a) access data held in, or accessible from, a computer that is on warrant premises; (b) copy the data to a data storage device; (c) convert the data into documentary form. […] A person commits an offence if the person fails to comply with the order. Penalty: 6 months imprisonment»*.

151 MCINTOSH N., *Curbing our Right to Online Freedom*, in *The Guardian*, 18 aprile 2001, http://www.guardian.co.uk; PALFREYMAN, *Lessons from the British and American Approaches to Compelled Decryption*, cit., 372.

7.3. L'esperienza statunitense.

Gli Stati Uniti hanno finora resistito alla tentazione di introdurre in via statutaria l'istituto della decriptazione forzata. Nel silenzio del legislatore, la materia è stata lasciata all'azione plasmante della giurisprudenza.

La questione è stata per lo più affrontata dalla prospettiva della legittimità costituzionale dei decreti con cui l'autorità giudiziaria ha talvolta imposto la disclosure dei codici di accesso a *file* criptati[152]. Nel riconoscere alcuni importanti diritti processuali, il quinto emendamento alla Costituzione statunitense sancisce che «*no person shall be compelled in any criminal case to be a witness against himself*». Il *leading case* in materia è rappresentato dal caso *Boucher* [153] in cui la corte di appello del Vermont ha applicato la teoria della *foregone conclusion* alla richiesta di accesso a un computer portatile, negando che nel caso di specie ricorresse una testimonianza forzata[154]. Nel caso sottoposto all'attenzione della Corte il governo sapeva dell'esistenza e della posizione in cui erano archiviati i *file* sospetti, sicché l'accesso ai dati crittografati avrebbe potuto aggiungere poco o nulla al compendio informativo in possesso degli inquirenti. Il signor Boucher non avrebbe pertanto potuto invocare la protezione offerta dal Quinto Emendamento per rifiutarsi di collaborare, poiché, secondo l'orientamento espresso dalla Suprema Corte nel noto caso *Fisher*, nessun diritto costituzionale viene violato nel caso in cui la dichiarazione non abbia, al tempo stesso, natura testimoniale e incriminante[155].

Facendo applicazione degli stessi principi, nel caso *Fricosu*[156] i giudici del distretto del Colorado hanno ritenuto legittimo la *subpoena* diretta all'imputata di decifrare i

---

[152] AJELLO N. J., *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination*, in *Brooklyn Law Review*, 2015, vol. 80, 2, 435 ss.

[153] *In re* Grand Jury Subpoena to Sebastien Boucher, 2009 WL 424718 (Vermount District, 2009)

[154] Di seguito una sintetica esposizione dei fatti all'origine della vicenda processuale. Nel 2006 il Sig. Boucher attraversò il confine con il Canada a Derby Line, nel Vermont, quando un ispettore della dogana notò un computer portatile in macchina che il conducente riconosceva come proprio. Ad un sommario esame del contenuto, disposto in conformità con le leggi doganali, un agente notava dei *file* che sembravano contenere pornografia infantile. Boucher ammetteva di scaricare pornografia dichiarando che, occasionalmente e involontariamente, poteva aver salvato anche materiale pedopornografico. Dopo aver disposto il sequestro del dispositivo, gli informatici forensi tentavano di duplicare il contenuto del portatile, accorgendosi che la directory nel quale erano contenute i file sospetti era protetta da crittografia. Il governo ottenne pertanto un ordine giudiziario di produzione della *password*, che Boucher impugnò lamentando la violazione dei diritti riconosciuti dal Quinto Emendamento, e in particolare del *privilege against self-incrimination*. Nel dettaglio il mandato richiedeva di fornire al governo una versione non crittografata della cartella contenente le immagini; il giudice di prime cure accoglieva la mozione dell'imputato con provvedimento prontamente appellato dal governo.

[155] In applicazione della *foregone conclusion doctrine* il governo sosteneva di poter già provare in giudizio i tre c.d. *Fisher elements* ossia *«that the documents exist, that they are in the control of the accused, and that the papers are authentic»*, per cui la dichiarazione non poteva recare alcun pregiudizio all'imputato. Cfr. *Fisher v. United States*, US Supreme Court, 1976, 391, 408 secondo cui *«Fifth Amendment applies only when the accused is compelled to make a testimonial communication that is incriminating»*.

[156] *United States v. Fricosu*, 841 F. Supp. 2d 1232 (Colorado District, 2012).

dati contenuti in un *hard disk*[157]. Nell'ordinare la decrittazione del dispositivo il tribunale valorizzava anche in questo caso la circostanza che gli organi inquirenti fossero già a conoscenza dell'esistenza e della posizione dei *file* sospetti, superando la censura dell'imputato sull'impossibilità di conoscerne il contenuto.

In un caso più recente la divulgazione della *password* è stata considerata a tutti gli effetti una forma di testimonianza. L'imputato, tratto in giudizio con l'accusa di pornografia infantile, impugnava l'ordine di produzione dei file contenuti nel proprio computer, invocando la tutela offerta dal quinto emendamento contro l'autoincriminazione. I giudici dell'Undicesimo circuito accoglievano la mozione dell'imputato, motivando sulla mancanza di prove in ordine alla *foregone conclusion* eccepita dal governo[158].

Sarà curioso osservare in che modo la giurisprudenza d'oltreoceano farà applicazione di questi principi alla rivelazione contenuto *wallet* digitali protetti da crittografia in procedimenti per riciclaggio o altri reati a sfondo economico. La dottrina della *foregone conclusion* potrebbe qui rivelarsi insufficiente a giustificare l'emanazione di ordini di *disclosure*, a causa nella natura non intrinsecamente illecita delle informazioni rilevabili sul dispositivo. L'apertura forzata del portafoglio potrebbe rappresentare l'unica fonte di prova del possesso di una determinata quantità di criptomoneta, che la pubblica accusa non è in grado di dimostrare in altro modo.

Come poter conciliare allora gli interessi dell'amministrazione della giustizia con il fondamentale diritto al silenzio e alla non autoincriminazione? È probabile che la giurisprudenza affronterà la questione facendo leva sul binomio della natura testimoniale o meno dell'atto di rivelazione della chiave privata. Non può comunque escludersi che il legislatore, mosso dal timore di un eccessivo indebolimento delle prerogative di controllo pubblico, intervenga sulla falsariga del modello britannico per disciplinare la materia a livello federale[159].

---

[157] Nel caso di specie l'FBI aveva eseguito un mandato di perquisizione nella residenza dell'imputata, Ramona Fricosu, rinvenendo sei computer, uno dei quali era protetto da un programma di crittografia. Poco dopo gli inquirenti avevano intercettato una telefonata tra la Fricosu e il suo ex marito. Durante la telefonata l'imputata affermava di essere proprietaria del computer e alludeva alla presenza di file incriminanti sul disco rigido criptato. Il governo ottenne dunque un mandato di ostensione dei contenuti non crittografati, ma la signora Fricosu si rifiutava di ottemperare, invocando a propria difesa la protezione offerta dal quinto emendamento.

[158] *Grand Jury Subpoena Duces Tecum*, March 25, 2011, 670 F.3d 1335 (11th Circuit, 2012). Nel corso di una indagine sotto copertura sulla pornografia infantile, l'FBI aveva rintracciato un sospettato che agiva da una camera d'albergo. Ottenuto un mandato di perquisizione, la polizia sequestrava sette dispositivi diversi, senza tuttavia potere accedere a determinati contenuti protetti da crittografia. Il governo ottenne anche qui una *subpoena* che imponeva all'indagato di produrre il contenuto dei *file.* Nell'accogliere la mozione dell'imputato i giudici hanno ritenuto che, in questo caso, l'ordine di decrittazione integrasse a tutti gli effetti una testimonianza sulla esistenza e sulla posizione dei file sospetti. La dichiarazione richiesta conduceva infatti a un esito nient'affatto scontato. Dagli atti d'indagine non risultava infatti alcun elemento a sostegno dell'ipotesi accusatoria che la cartella contenesse file multimediali pedopornografici e che l'imputato vi avesse accesso.

[159] PALFREYMAN., *Lessons from the British and American Approaches to Compelled Decryption,* cit., 370

8. Lo strumentario processuale sul banco di prova delle valute virtuali. Luci, ombre e prospettive di riforma.

La trattazione finora svolta evidenzia come l'impiego a fini delittuosi delle valute virtuali sollevi numerose questioni sul piano processuale penale. Alcune di queste riguardano la diffusione di innovative tecniche d'indagine, che all'apparenza sembrano distanziarsi dai mezzi tipici di ricerca della prova. Altre sorgono a causa delle peculiarità delle valute virtuali come mezzo di circolazione della ricchezza, che rischiano di mettere in crisi gli ordinari strumenti di ablazione patrimoniale.

Giunti a conclusione di questo percorso, ci domandiamo se l'attuale strumentario processuale sia adeguato a far fronte alle sfide lanciate dalla tecnologia a registro diffuso, ovvero necessiti qualche intervento correttivo per mano del legislatore. Per fornire una risposta esaustiva converrà ripercorre in breve i capisaldi della trattazione.

Nel contrasto alla cybercriminalità economica una importanza crescente è attribuita all'*Open Source Intelligence*, intesa come la raccolta e l'analisi incrociata di dati acquisiti da fonti liberamente accessibili. Nello scenario attuale, caratterizzato da dallo *sharing* massivo di informazioni personali e dall'utilizzo di potenti algoritmi di ricerca, essa può condurre a risultati preziosi per le indagini. Sul piano processuale il valore indiziario delle risultanze acquisite *open source* potrà essere rafforzato mediante l'utilizzo di mezzi di prova come la perizia o la testimonianza esperta. La giurisprudenza di legittimità[160] più recente tende infatti ad escludere che le predette risultanze diano luogo a un fatto notorio, a cui il giudice può far riferimento per superare le prove legittimamente acquisite in dibattimento nel contraddittorio tra le parti. Sarà quindi onere della pubblica accusa far confluire in dibattimento i risultati dell'*intelligence* mediante i canali tipici di formazione della prova.

La medesima efficacia probatoria deve attribuirsi alle tecniche di *blockchain intelligence* che si fondano su euristiche dotate di alta credibilità razionale. Il *clustering* (associazione di indirizzi, *mixnet recognition*, confronto i dati acquisiti *open source*) può essere considerato un accertamento tecnico ripetibile (art. 359 c.p.p.), i cui esiti potranno entrare nel processo attraverso la perizia o la testimonianza esperta. Le risultanze del registro pubblico delle transazioni dovrebbero invece essere inquadrate nella categoria dei fatti notori, potendo allo stato essere assunto a postulato l'immodificabilità della catena dei blocchi, la certezza della data sulla stessa impressa (*time stamping*) e l'oggetto del trasferimento. La notorietà del fatto-transazione non si estende, ovviamente, alla titolarità dell'indirizzo e all'individuazione dell'autore del trasferimento, circostanze rispetto alle quali opera principio generale della formazione della prova in dibattimento nel contraddittorio delle parti.

[160] Cfr. Cass. Pen., Sez. I, 20 maggio 2016, n. 36315, in *Cass. Pen*., 2017, 4, 1550 ss. secondo cui «non sono utilizzabili ai fini della deliberazione informazioni tratte in camera di consiglio dal sito internet *google maps*, in quanto trattasi di acquisizione unilaterale di elementi conoscitivi che determina l'impiego a fini decisori di prove diverse da quelle legittimamente acquisite in dibattimento nel contraddittorio tra le parti».

I nuovi strumenti d'indagine *open source* potrebbero ricavarsi uno spazio significativo tra i mezzi di ricerca della prova. Si tratta di una questione tanto innovativa quanto complessa: una parte della dottrina ritiene infatti che l'utilizzo di particolari *software* e, in generale, di *Internet* costituisca un mezzo di ricerca della prova atipico "a contenuto tecnologico", che si scontra con il fondamentale diritto alla riservatezza[161]. La tesi è certamente condivisibile per quel che concerne gli strumenti più invasivi per la vita privata dell'individuo, il cui utilizzo dovrebbe dar luogo a elementi di prova inutilizzabili. Le garanzie costituzionali non sembrano tuttavia d'ostacolo al compimento di attività d'*intelligence* su dati pubblicamente accessibili tra cui rientra, ad esempio, la consultazione di siti *web* e il raffronto con le risultanze della *blockchain.*

Occorre tuttavia dar conto dell'opportunità, in prospettiva futura, di un intervento del legislatore per dettare limiti e condizioni delle operazioni OSINT "ad alto contenuto tecnologico" che presentano rischi specifici per la riservatezza dell'individuo; la conclusione appare in linea con i principi desumibili dalla nota vicenda relativa all'annullamento della direttiva sulla *data retention*[162], da cui può desumersi la ineludibile necessità della predeterminazione legislativa di limiti e condizioni per "fare ingresso" nella vita privata dei cittadini[163]. Non pare infatti del tutto infondato il timore di una eccessiva compressione della *privacy* dell'individuo per effetto della diffusione di potenti strumenti di *open data analytics,* il cui utilizzo andrebbe regolato e ricondotto alle garanzie della riserva di legge e di giurisdizione.

Altrettanto può dirsi per la disciplina delle perquisizioni informatiche di cui all'art. 247, comma 1-*bis* e del sequestro probatorio di cui all'art. 354, comma 2, c.p.p. che rappresentano una base normativa indispensabile per la corretta acquisizione della *digital evidence.* Nei procedimenti per reati connessi all'utilizzo delle valute virtuali debbono infatti essere assicurate le stesse garanzie di genuinità e di immodificabilità previste in generale per ogni prova informatica. Rimane tuttavia il dubbio sulla procedura da seguire nel caso in cui l'accesso al portafoglio digitale sia impedito da misure crittografiche di protezione. Si auspica che la giurisprudenza possa ricondurre l'eventuale richiesta di decriptazione rivolta all'indagato nell'alveo delle garanzie previste dagli artt. 64 e 350 c.p.p., rifuggendo ogni tentativo di aggiramento del privilegio contro l'autoincriminazione.

Evidenti lacune normative si registrano invece sul piano della disciplina applicabile agli strumenti di ablazione patrimoniale per finalità probatorie o cautelari. Quando

---

[161] MARCOLINI S., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. Pen.*, 2015, 2, 768.

[162] Corte di Giustizia UE, 8 aprile 2014, *Digital Rights Ireland Ltd* (C-293/12 e C-594/12). Cfr. FLOR R., *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in Diritto penale contemporaneo – Riv. trim, 2014, 2, 178 ss.; ID., *Dalla "data retention" al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive "de jure condendo"?,* in *Dir. Inf.*, 2014, 4-5, 775 ss.

[163] Cfr. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale,* cit., 787

l'oggetto del sequestro probatorio, conservativo o preventivo, è rappresentato da un ammontare di valuta virtuale, dovrebbero essere adottate misure idonee a garantire la reale indisponibilità della somma da parte del destinatario del provvedimento; per far fronte a questa esigenza, non è sufficiente privare quest'ultimo della disponibilità di programmi o strumenti informatici di gestione del portafoglio digitale. Diversamente, sarà indispensabile trasferire i valori su un indirizzo controllato dall'autorità giudiziaria, qualora ciò risulti tecnicamente possibile. Al medesimo scopo, dovrà essere ordinato ai fornitori di servizi connessi all'utilizzo del circolante virtuale, destinatari del provvedimento di cui all'art. 254-*bis* c.p.p., di adottare le misure necessarie ad impedire l'accesso dell'utente alla propria area personale, prevedendo la possibilità anche in questo caso di trasferire i valori su un conto *ad hoc*. I valori sottoposti a sequestro dovranno essere custoditi con modalità tali da assicurare un elevato grado di sicurezza nella conservazione e minimizzare il rischio di perdita accidentale o di sottrazione fraudolenta.

Inoltre, la volatilità del prezzo della moneta virtuale mal si concilia con la natura interinale degli effetti del sequestro; la legge processuale dovrebbe pertanto prevedere la possibilità di adottare misure dirette a prevenire l'alterazione del prezzo delle valute sottoposte a sequestro. Tali misure potranno, a seconda dei casi, consistere nella conversione in valute più stabili, o nella vendita al prezzo medio praticato sul mercato.

Questi principi dovrebbero trovare una espressa tipizzazione normativa per evidenti ragioni di uniformità della prassi applicativa, di legalità delle procedure, e di sicurezza della custodia. Tanto premesso, riteniamo che il legislatore dovrebbe mettere mano all'impianto del codice, per disciplinare le modalità esecutive e i principi ispiratori delle misure di ablazione patrimoniale aventi ad oggetto le valute virtuali. Di seguito una possibile proposta di riforma, elaborata tenendo a mente le necessità che abbiamo pocanzi evidenziato.

All'art. 354, comma 2, del codice di procedura penale, in materia di accertamenti compiuti dalla polizia giudiziaria, si potrebbe aggiungere un comma 2-*bis*, del seguente tenore: «Nei casi previsti dal secondo comma, quando il sequestro abbia ad oggetto le valute di cui all'art. 1, comma 2, lett. qq) del decreto legislativo 21 novembre 2007, n. 231[164], il sequestro è eseguito mediante trasferimento dei valori su un conto controllato dall'autorità giudiziaria, adottando le opportune misure tecniche di sicurezza nella conservazione dei dati».

L'art. 254-*bis* del codice, avente ad oggetto il sequestro di dati presso fornitori di servizi informatici, potrebbe essere modificato con l'aggiunta di un comma 1-*bis*, che disponga: «L'autorità giudiziaria, quando dispone il sequestro di valute virtuali presso fornitori di servizi di cui all'art. 1, comma 2, lett. ff) del decreto legislativo 21

[164] La norma definisce la valuta virtuale ai fini della normativa antiriciclaggio come *«la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente»* (v. *amplius*, Cap. III, § 1).

novembre 2007, n. 231[165]può stabilire che la loro acquisizione sia eseguita mediante trasferimento dei valori su un indirizzo controllato dall'autorità giudiziaria. In questo caso è, comunque, ordinato al fornitore dei servizi di inibire immediatamente l'accesso al conto su cui sono registrate le valute virtuali oggetto del sequestro».

La disciplina del sequestro preventivo di cui all'art. 321 del codice potrebbe essere integrata da un comma 3-*quater*, così formulato: «Quando il provvedimento di cui ai commi 1, 2 e 3-*bis* del presente articolo abbia ad oggetto le valute di cui all'art. 1, comma 2, lett. qq) del decreto legislativo 21 novembre 2007, n. 231, il sequestro è eseguito mediante trasferimento dei valori su un conto controllato dall'autorità giudiziaria, adottando le opportune misure tecniche di sicurezza nella conservazione dei dati. Il giudice o, nel corso delle indagini preliminari, il pubblico ministero, possono nominare un consulente tecnico per coadiuvare lo svolgimento delle operazioni, disponendo che siano adottate idonee misure per impedire l'alterazione del prezzo dei valori sottoposti a sequestro».

Infine, all'art. 316 c.p.p. in tema di sequestro conservativo, sarebbe sufficiente aggiungere un comma 1-*ter*, che preveda: «Quando è chiesto il sequestro conservativo di valute virtuali, si applicano, in quanto compatibili, le disposizioni del comma 3-*quater* dell'art. 321».

[165] È considerato prestatore di servizi connessi all'utilizzo di valuta virtuale «ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale».

BIBLIOGRAFIA

A

ABBADESSA G., *Ricettazione e dolo eventuale*, in *Diritto penale contemporaneo*, 20 dicembre 2010

ACCILI SABATINI M. A., BALSAMO A., *Verso un nuovo ruolo della convenzione di Palermo nel contrasto alla criminalità transnazionale*, in *Diritto Penale Contemporaneo – Rivista trimestrale*, 2018, 1, 113 ss.

ACCINNI G.P., *Profili di responsabilità penale dell'*hosting provider *"attivo*", in *Arch. Pen. Web*, 2017, 2, 1 ss.

ACCINNI G.P., *Profili di rilevanza penale delle "criptovalute*", in *Arch. Pen. Web*, 2018, 1, 1 ss.

AJELLO N. J., *Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination*, in *Brooklyn Law Review*, 2015, vol. 80, 2, 435 ss.

ALBANESE D., *Partecipazione all'associazione con finalità di terrorismo 'Stato Islamico': una pronuncia di condanna della Corte d'Assise di Milano*, in *Diritto penale contemporaneo*, 21 ottobre 2016

ALBRECHT M., *Die Kriminalisierung von Dual-Use-Software*, Berlin, 2014

ALESSANDRI A., *Diritto penale e attività economiche*, Bologna, 2010

ALESSANDRI A., *Criminalità economica e confisca del profitto*, in DOLCINI E., PALIERO C.E. (a cura di), *Studi in onore di Giorgio Marinucci*, Milano, 2006, 203 ss.

ALESSANDRI A., *La confisca*, in ID. (a cura di), *Il nuovo diritto penale delle società*, Milano, 2002

ALESSANDRI A., *Un esercizio di diritto penale simbolico: la tutela penale del risparmio*, in ABBADESSA P., CESARINI F. (a cura di), *La legge per la tutela del risparmio*, Bologna, 2007, 169 ss.

AL JAWAHERI H., *Deanonymizing Tor hidden service users through Bitcoin transactions analysis*, University of Qatar, in http://qspace.qu.edu.qa

AMATO M., FANTACCI L., *Per un pugno di Bitcoin*, Milano, 2016

AMBROSETTI E. M., *La frode fiscale mediante altri artifici: vecchi e nuovi aspetti problematici*, in *Archivio Penale*, 2017, 1, 4 ss.

AMBROSETTI E.M., *I reati tributari*, in AMBROSETTI E.M., MEZZETTI E., RONCO M., *Diritto penale dell'impresa*, Bologna, 2016, 505 ss.

ANNUNZIATA F., *Distributed Ledger Technology e mercato finanziario: le prime posizioni dell'ESMA*, in PARACAMPO M.T. (a cura di), *FinTech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2017, 229 ss.

ANNUNZIATA F., *La disciplina del mercato mobiliare*, Torino, 2014, 94 ss.

ANNUNZIATA F., *Speak if you can: what are you? An alternative approach to the qualification of token and ICOs*, Bocconi legal studies research paper, n. 2636561, in attesa di pubblicazione in *European Company and Financial Law Review*

ANTOLISEI F., *Manuale di diritto penale – Parte generale*, Milano, 2003

ANTOLISEI F., *Manuale di diritto penale – Parte speciale*, Vol. I, Milano, 2016

ANTOLISEI F., *Manuale di diritto penale. Parte speciale*, Vol. II, Milano, 2016

ARAGONA V., *Il contrasto al finanziamento del terrorismo*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2017, 1, 101 ss.

ARCELLI M., DONGILI P., *Economia monetaria*, Padova, 1977

B

BALSAMO, A., DE AMICIS, G., *L'art. 12-quinquies della legge n. 356/1992 e la tutela del sistema economico contro le nuove strategie delle organizzazioni criminali: repressione penale "anticipata" e prospettive di collaborazione internazionale*, in *Cass. Pen.*, 2005, 5, 2075 ss.

BARBIERI A., *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici*, in in *Dir. Internet*, 2008, 5, 516 ss.

BARRDEAR J., KUMHOF M., *The macroeconomics of central bank issued digitalcurrencies*, Bank of England Staff Working Paper No. 605, in https://bankofengland.co.uk

BARTOLI R., *Legislazione e prassi in tema di contrasto al terrorismo internazionale: un nuovo paradigma emergenziale?*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2017, 3, 233 ss.

BARTOLI R., *Il problema della causalità penale*, Torino, 2010

BASILE E., *Brevi note sulla nuova Direttiva PIF. Luci ed ombre del processo di integrazione europea in materia penale*, in *Diritto penale contemporaneo*, 12 dicembre 2017

BASILE E., *Chiaroscuri della Cassazione in tema di abusivismo bancario e finanziario, in Diritto penale contemporaneo*, 15 maggio 2017

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

BATTAGLINI G., CRIFÒ G., voce *Imputabilità*, in *Noviss. Dig.*, 1962, VIII, 455

BELLACOSA M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *Diritto Penale Contemporaneo*, 2 febbraio 2015

BELLUTA H., *Cybercrime e responsabilità degli enti*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, 106 ss.

BENUSSI C., *Il pubblico funzionario che fa uso del cellulare di servizio per fini privati risponde di peculato d'uso*, in *Diritto penale contemporaneo*, 12 maggio 2013

BERENTSEN A., *On the private provision of fiat currency*, in *European Economic Review*, 2006, 7, 1683 ss.

BEVILACQUA F.C., *Le previsioni sanzionatorie della normativa antiriciclaggio*, in ALESSANDRI A. (a cura di), *Reati in materia economica*, Torino, 2017, 375 ss.

BLAIOTTA R., *Causalità giuridica*, Torino, 2010

BISTARELLI S., *Bitcoin forensics: le tecniche labeling, clustering e mixnet recognition*, in *Agenda Digitale*, 10 aprile 2018

BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. Inf.*, 2017, 1, 27 ss.

BORRUSO R. – RUSSO S. TIBERI C, *L'informatica per il giurista. Dal bit a internet*, Milano, 2009

BOURQUE S. – FUNG LING TSUI S., *A lawyer's introduction to smart contract*, in *Scientia Nobilitat – Review of legal studies*, 2014, 4

BONFIGLIO A., *Monitoraggio fiscale e regime sanzionatorio*, in *Corriere Tributario*, 2002, 27, 2439 ss.

BRICHETTI R., *Riciclaggio e autoriciclaggio*, in *Riv. it. dir. proc. pen.*, 2014, 2, 684 ss.

BRILL A. – KEENE L., *Cryptocurrencies: The Next Generation of Terrorist Financing?*, in *Defence Against Terrorism Review*, 2014, 6, 7 ss.

BRITO J. (a cura di)., *The law of Bitcoin*, Bloomington, 2015

BRICHETTI R, VENEZIANI P. (a cura di), *I reati tributari*, Torino, 2017

BRUNELLI D., *Autoriciclaggio e divieto di retroattività: brevi note a margine del dibattito sulla nuova incriminazione*, in *Diritto penale contemporaneo – Rivista trimestrale*, 1, 2015, 86 ss.

BRUNELLI D., *Autoriciclaggio: profili del concorso di persone*, in MEZZETTI E.-PIVA D., *Punire l'autoriciclaggio: come, quando e perché*, Torino, 2016, 19 ss.

BRUNO F., ROZZI A., *Dalla sollecitazione all'investimento all'offerta al pubblico di prodotti finanziari: una prima riflessione sul recepimento della Prospectus Directive nel mercato dei capitali italiano*, in *Giurisprudenza commerciale*, 2008, 2, 281 ss.

BUFFA F., *Responsabilità del gestore di sito Internet*, in *Questionegiustizia.it*, 9 gennaio 2017

BURCHARD C., *Artificial intelligence and law*, in WOLFF B., *Whiter artificial intelligence? Debating the policy challenges of the upcoming transformation*, Science Policy Fellowship Program Paper 03/2018, Frankfurt am Main, 14 ss.

C

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

CANTARELLA M., *Il Bitcoin e la dottrina della deflazione*, 13 maggio 2015, in https://rethinkecon.it

CANTONE R., *Abusivismo finanziario: esperienze da un'indagine giudiziaria*, in *Cass. Pen.*, 1996, 3122 ss.

CAPACCIOLI S., *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015

CAPACCIOLI S., *Regime impositivo delle monete virtuali: poche luci e molte ombre*, in *Il Fisco*, 2016, 37, 3538 ss.

CAPOGNA A. *et al.*, *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione*, in *Diritto, mercato e tecnologia*, 2015, 3, 44 ss.

CAPONERA A., GOLA C., *Questioni di Economia e Finanza – Aspetti economici e regolamentari delle 'cripto-attività'*, Paper 484 – Marzo 2019, in https://www.bancaditalia.it;

CAPPELLINI A., *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 762 ss.

CAPRIGLIONE F., *Commentario al Testo Unico delle Leggi in materia bancaria e creditizia*, *sub* Art. 132, Padova, 2018, 2579 ss.

CAPRIGLIONE, F., *Finalità della supervisione ed articolazione dei controlli pubblici*, in ID. (a cura di), *Manuale di diritto bancario e finanziario*, Padova, 2015, 143 ss.

CARACCIOLI I., *L'incerta definizione del reato di riciclaggio*, in *Il Fisco*, 2015, 4

CARMONA A., *I reati contro il patrimonio*, in FIORELLA A. (a cura di), *Questioni fondamentali della parte speciale del diritto penale*, Torino, 2016, 7 ss.

CARRIÈRE P, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche di "strumenti finanziari", "valori mobiliari" e "prodotti finanziari"; tra tradizione e innovazione*, in *Rivista di diritto bancario*, 2019, 2

CASSELLA S. D., *Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete?,* in *Journal of Money Laundering Control*, Vol. 21, 4, 494 ss.

CASTALDO A., *Accesso all'attività bancaria e strategie penalistiche di controllo*, in *Riv. it. dir. proc. pen.*, 1996, 81 ss.

CASTALDO A. R. – NADDEO M., *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio*, Padova, 2010, 92 ss.

CAVALLINI S., TROYER L., *Apocalittici o integrati? Il nuovo reato di auto riciclaggio: ragionevoli sentieri ermeneutici all'ombra del "vicino ingombrante"*, in *Diritto penale contemporaneo – Rivista trimestrale*, 1, 2015, 95 ss.

CAUTERUCCIO R., *I nuovi reati contro la fede pubblica: il falso in documento informatico pubblico o privato*, in *Rivista penale*, 2007, 965 ss.

CENTONZE F., *Causalità attiva e causalità omissiva: tre rivoluzionarie sentenze della giurisprudenza di legittimità*, in *Riv. it. dir. proc. pen*, 2001, 1, 289 ss.

CENTONZE F., *Controlli societari e responsabilità penale*, Milano, 2009

CERQUA L.D., *Il delitto di riciclaggio nel sistema penale italiano*, in *Revista brasileira de estudios politicos*, 2015, 1, 12 ss.

CERQUA L.D., CAPPA E., *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*, Milano, 2012

CHAUM D., *Blind Signatures for Untraceable Payments*, in CHAUM D., RIVEST R.L., SHERMAN A.T. (eds), *Advances in Cryptology*, Boston, 1983, 199 ss**.**

CLAPS P. – PIGNATELLI M., *L'acquisto e la vendita per conto terzi di "bitcoin" non sconta l'IVA ma rileva ai fini IRES ed IRAP*, in *Corriere Tributario*, 2016, 40, 3073 ss.

CLARKE R., *The Digital Persona and its Application to Data Surveillance*, in *The information Society*, 1994 10, 77 ss.

CLOUGH J., *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, in *Monash University Law Review*, 2014, vol. 40, 3, 698 ss.

CLOUGH J., *Principles of cybercrime*, Cambridge, 2015

CHIBBARO S. BECHINI U., *Dal documento all'evento: bollo e documento informatico*, in *Rivista del notariato*, 2013, 2, 273 ss.

CINGARI F., *La dichiarazione fraudolenta mediante altri artifici*, in BRICHETTI R, VENEZIANI P. (a cura di), *I reati tributari*, Torino, 2017, 205 ss.

COLOMBO G., *Il riciclaggio*, Milano, 1990

CONSO A., DI GIORGIO A., MARTINOTTI L., *Un caso recente: divieto di offerta al pubblico di "portafogli di investimento" in criptovalute*", in *Rivista di diritto bancario*, 29 ottobre 2018

CONSULICH F., *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca, borsa e titoli di credito*, 2018, 2, 195 ss.

CONSULICH F., *Poteri di fatto ed obblighi di diritto nella distribuzione delle responsabilità penali societarie*, in *Le società*, 2012, 5, 555 ss.

CONTI L., *Profili penalistici del testo unico sull'intermediazione finanziaria*, in *Dir. pen. proc.*, 1998, 548 ss.

CORRIAS LUCENTE G., *La pretesa responsabilità penale degli intermediari di contenuti in internet*, in *Dir. inf..*, 2009, 1, 91 ss.

CORSO P., *Il declino di un "privilegio": l'autoriciclaggio (anche da reato tributario) ha rilievo penale autonomo*, in *Corriere tributario*, 2015, 3, 159 ss.

CORVINO G., *La tutela penale del documento informatico*, in PLANTAMURA V., MANNA A., *Diritto penale e informatica*, Bari, 2007, 26 ss.

COSTI R., *Il mercato mobiliare*, Giappichelli, Torino, 2016

CRESPI A., voce *Imputabilità (dir. pen.)*, in *Enc. Dir*., 1970, XX, 781 ss.

CRESPI A., *Studi di diritto penale societario*, Milano, 2010

CONTALDO A., GORGA M., *Le novità della disciplina del Processo Civile Telematico (PTC) anche con riguardo alla recente disciplina del Codice dell'Amministrazione Digitale (CAD)*, in *Rassegna dell'Avvocatura dello Stato*, 2016, 4, 166 ss.

CUCCURU P., *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *Nuova Giurisprudenza Civile Commentata*, 2017, 1, 107 ss.

CUÈLLAR M.F., *The Tenuous Relationship between the Fight against Money Laundering and the Disruption of Criminal Finance*, in *The Journal of Criminal Law and Criminology*, 2003, vol. 93, 2, 311 ss.

D

DAL CHECCO P. – ZEN L., *Il Clustering come Strumento di Deanonimizzazione dei Wallet Bitcoin*, in *ICT security magazine*, 24 luglio 2017

D'AIETTI G., *La frode informatica*, in BORRUSO R., BUONOMO G., CORASANTI G., D'AIETTI G., *Profili penali dell'informatica*, Milano, 1994, 39 ss.

D'AGOSTINO L., *Cybersecurity, (auto)regolazione e governance del rischio. Quid de iure poenali*?, in *Luiss Law Review*, 2017, 1, 129 ss.

D'AGOSTINO L., *La nuova disciplina sanzionatoria del monitoraggio fiscale tra limiti eurounitari e controlimiti costituzionali: la parola alla Corte di giustizia*, in *Diritto e pratica tributaria internazionale*, 2017, 3, 957 ss.

D'AGOSTINO L., *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D. Lgs. 10 agosto 2018, n. 101*, in *Archivio penale*, 2019, 1, 2 ss.

D'AGOSTINO L., *L'operatività della confisca e le sorti del sequestro preventivo in presenza di impegno al pagamento del debito tributario: in dubio pro reo?*, in *Rivista Trimestrale di diritto tributario*, 2017, 2, 367 ss.

D'AGOSTINO L., *I margini applicativi della condotta di partecipazione all'associazione terroristica: adesione psicologica e contributo causale all'esecuzione del programma criminoso*, in *Diritto Penale Contemporaneo – Rivista Trimestrale*, 2017, 1, 81 ss.

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*, 2018, 1,

D'AGOSTINO L., PISELLI R., *La definizione di tecnologia a registro distribuito e di smart contract nella legge di conversione del "Decreto semplificazioni". Un primo commento*

critico, in NUZZO A. (a cura di), *Blockchain e autonomia privata. Fondamenti giuridici*, Roma, 2019, 15 ss.

D'ANGLEJAN-CHATILLON A. *et a*, *The Virtual Currency Regulation Review – Canada*, novembre 2018, in https://thelawreviews.co.uk

D'ARCANGELO F., *Gli effetti penali della voluntary disclosure e la responsabilità da reato degli enti*, in *Responsabilità amministrativa delle società e degli enti*, 2015, 2, 9 ss.

D'AVIRRO A., GIGLIOLI M., *Autoriciclaggio e reati tributari*, in *Diritto penale e processo*, 2015, 145 ss.

DE BELLIS M., voce *Mercati finanziari (disciplina pubblicistica)*, in *Enciclopedia Treccani Online*, 2018, 1 ss.

DE FILIPPI P. - HASSAN S., *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, in *First Monday*, 2016, 21, 12 ss.

DE FILIPPI P., WRIGHT A., *Blockchain and the law, The Rule of Code*, Harvard, 2018

DE FILIPPI P., WRIGHT A., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 10 marzo 2015, in https://ssrn.com, 16 ss.

DE FRANCESCO G., *Riciclaggio ed autoriciclaggio: dai rapporti tra le fattispecie ai problemi di concorso nel reato*, in *Dir. pen. proc*., 2017, 7, 944 ss.

DE MASI M., *Le criptovalute entrano nel quadro RW*, in *Il Fisco*, 2018, 20, 1929 ss.

DELOGU T., *Lo 'strumento' nella teoria generale del reato*, in *Riv. it. dir. proc. pen.*, 1974, 273 ss.

DELSIGNORE F., *Il delitto di sottrazione fraudolenta al pagamento di imposte in sede di riscossione coattiva*, in in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Diritto penale dell'economia*, vol. I, Vicenza, 2017, 1009 ss.

DE MARTINO P., *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico*, in *Diritto penale contemporaneo*, 11 maggio 2015

DE MINICO G., *Lineamenti del potere regolamentare della Consob*, in DE SIERVO U. (a cura di), *Osservatorio sulle fonti* 1996, Torino, 1996, 203 ss.

DE NATALE D., *Responsabilità penale dell'internet service provider per omesso impedimento e per concorso nel reato di pedopornografia*, in GRASSO G., PICOTTI L., SICURELLA R., *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, 295 ss.

DINACCI E., voce *Trasferimento fraudolento di valori*, in *Enciclopedia giuridica Treccani*, 2018, 1 ss.

DI GIOVINE O., *Lineamenti sostanziali del nuovo illecito punitivo*, in LATTANZI G., (a cura di), *Reati e responsabilità degli enti*, Milano, 2010, 40 ss.

DI TULLIO D'ELISIIS A., *Autoriciclaggio. Applicazione e strategie difensive*, Rimini, 2015

DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, in *Dir. pen cont. – Riv. trim*, 2018, 9, 87 ss.

DI VIZIO F., *Il delitto di sottrazione fraudolenta del pagamento delle imposte ed i rapporti con i reati di bancarotta fraudolenta per distrazione e di riciclaggio*, in *Discrimen*, 1 ottobre 2018

DONINI M., *Il diritto penale di fronte a "nemico",* in *Cass. Pen*., 2006, 737 ss.

DONINI M., *Imputazione oggettiva dell'evento. "Nesso di rischio" e responsabilità per fatto proprio*, Torino, 2007.

DORIGO S., *Nuovi confini giurisprudenziali del reato di sottrazione fraudolenta al pagamento di imposte*, in *Giurisprudenza penale web*, 2017, 7-8, 6 ss.

DORN J. A., *The future of money in the information age*, (trad. it.), Milano, 1998

E- F

EPIDENDIO T.E., *La confisca nel diritto penale e nel sistema delle responsabilità degli enti*, Padova, 2011

FAKHOURY H., *A combination or a key? The Fifth Amendment and privilege against compelled decryption,* in *Digital Evidence and Electronic Signature Law Review,* 2012, 9, 81 ss.

FASANI F., *I martiri invisibili. Quale ruolo per il diritto penale nella lotta al terrorismo Islamico?* in *Criminalia*, 2015, 485 ss.

FASANI F., *Un nuovo intervento di contrasto al terrorismo internazionale,* in *Dir. Pen. Proc*., 2016, 12, 1555 ss.

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

FERRELL M., *Bitcoin prices surge post-Cyprus bailout,* 28 marzo 2013, in https://money.cnn.com

FERRI F., MIGLIO M., *In tema di abusivismo finanziario*, in *Diritto penale contemporaneo*, 9 gennaio 2014

FIANDACA G., *Il reato commissivo mediante omissione*, Milano, 1979

FIANDACA G., MUSCO E., *Diritto penale – Parte speciale,* vol. II, Bologna, 2014

FIORELLA A., *Il trasferimento di funzioni nel diritto penale d'impresa,* Firenze, 1985

FIORELLA A., *Le strutture del diritto penale,* Torino, 2018

FIORELLA A., *Ufficiale pubblico, incaricato di un pubblico servizio, o di un servizio di pubblica necessità*, in *Enc. dir.,* 1992, XLV, 563 ss.

FLICK G. M., *La repressione del riciclaggio ed il controllo della intermediazione finanziaria. Problemi attuali e prospettive*, in *Riv. it. dir. proc. pen*. 1990, 1264 ss.

FLOR R., *Cyber-criminality: Finding a Balance between Freedom and Security*, nella raccolta di scritti del convegno *Cybercrime: Global Phenomenon and its Challenges*, International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC)

FLOR R., *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de iure condendo?*, in *Diritto dell'informazione e dell'informatica*, 2014, 1-2, 775 ss.

FLOR R., *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Diritto penale contemporaneo*, 2014, 2, 178 ss.;

FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc.*, 2015, 10, 1296 ss.

FLOR R., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention*, in *Ciberspazio e diritto*, 11, 2, 2010, 359 ss.

FONDAROLI D., *Le ipotesi speciali di confisca nel sistema penale. Ablazione patrimoniale, criminalità economica, responsabilità delle persone fisiche e giuridiche*, Bologna, 2007

FONDAROLI D., *Splendori e miserie della confisca obbligatoria del profitto*, in ID. (a cura di), *Principi costituzionali in materia penale e fonti sovranazionali*, Padova, 2008, 117 ss.;

FRANZA E., *Le valute virtuali e prodotti finanziari con sottostanti valute virtuali. Una prima indagine sugli interventi*, in http://foroeuropa.it

FULVI F. R., *L'unità virtuale del diritto penale dell'informatica*, in PICOTTI L, RUGGIERI F. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, Torino, 2011, 167 ss.

FUX A., *Ulteriori precisazioni sui confini della nozione di profitto: è necessaria l'"esternalità"*, in *Cass. pen.*, 2014, 5, 3253 ss.

G

GALLO M., *La legge penale (Appunti di diritto penale)*, Torino, 1965, 74

GALMARINI S., *Monete virtuali e antiriciclaggio: terreni dai confini incerti*, *www.dirittobancario.it*, 11 ottobre 2018

GAMBARDELLA M., *Art. 357*, in LATTANZI G., LUPO E. (a cura di), *I delitti contro la pubblica amministrazione*, Milano, 2010, 913 ss.

GANS J.S., HALABURDA H., *Some Economics of Private Digital Currency*, in GOLDFARB A., GREENSTEIN S., TUCKER C. (eds.), *Economic Analysis of the Digital Economy*, Chicago, 2015

GAREGNANI G.-GALLI G.-TROYER L., *Brevi note sull'introduzione del nuovo delitto di autoriciclaggio nel novero dei reati presupposto della responsabilità amministrativa da reato di cui al D.Lgs. 231/01*, in *Rivista dei dottori commercialisti*, 2015, 3, 467 ss.

GASPARRI G., *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?,* in *Dir. Inf.*, 2015, 1, 429 ss.

GIACONA I., *Il concetto d'idoneità nella struttura del delitto tentato,* Torino, 2000

GIANNITI F., *L'oggetto materiale del reato,* Milano, 1966

GIRINO E., *Criptovalute: un problema di legalità funzionale*, in *Rivista di Diritto Bancario*, 2018, 55, 2 ss.

GIUNTA F., *La posizione di garanzia nel contesto della fattispecie omissiva impropria*, in *Diritto penale e processo.*, 1999, 169 ss.

GIUSTOZZI C., MONTI A., ZIMUEL E., *Segreti Spie Codici cifrati. Crittografia: la storia, le tecniche, gli aspetti giuridici*, Milano, 1999

GOWRISANKARAN, G., STAVINS, J., *Network externalities and technology adoption: lessons from electronic payments*, in *Rand Journal of Economics*, 2004, vol. 35, 2, 260 ss.

GRASSO G., *Il reato omissivo improprio,* Milano, 1983

GRASSO G., sub *Art. 240*, in ROMANO M., GRASSO G., PADOVANI T. (diretto da), *Commentario sistematico del codice penale*, vol. III, Milano, 2011, 611 ss.

GRASSO P., BELLAVIA E., *Soldi sporchi. Come le mafie riciclano miliardi e inquinano l'economia mondiale*, Milano, 2011

GROTTO M., *Regime giuridico del falso informatico dubbi sulla funzione interpretativa dell'art. 491 bis c.p.*, in *Dir. Inf.*, 2006, 589 ss.

GUIDI D., *Una nuova ipotesi di abusivismo finanziario,* in GIUNTA F., MICHELETTI D. (a cura di), *La disciplina penale del risparmio*, Milano, 2008, 173 ss.

GULLO A., *Autoriciclaggio e reati tributari,* in *Diritto penale contemporaneo*, 13 marzo 2018

GULLO A., voce *Autoriciclaggio*, in *Il libro dell'anno del diritto* 2016, in https://treccani.it

GULLO A., *Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato*, in *Dir. Pen. Cont. – Riv. Trim*, 2018, 6, 262 ss.

GUTTMANN B., *The Bitcoin Bible. Gold edition.*, Norderstedt, 2013

H

HACKER, P., THOMALE C., *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*, in *European Company and Financial Law Review*, 2018, 645 ss.

HALLEVY G., *The criminal liability of artificial intelligence entities – from science fiction to legal social control*, in *Akron Intellectual Property Journa*l, 2010, 4, 171 ss.

HAYEK F. A., *Denationalisation of Money*, London, 1976

HILDEBRANDT M., *Criminal liability in smart environments*, in DUFF R. A., GREEN S., *Philosophical foundations of criminal law*, Oxford, 2011, 212 ss.

HILDEBRANDT M., *Smart technologies and the end(s) of the law*, Cheltenham, 2016

HOLT D.T. BOSSLER A., SEIGFRIED-SPELLAR K., *Cybercrime and Digital Forensics: An Introduction*, London, 2015, 405 ss.

I

IEMMA P., CUPPINI N., *La Qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, in *Rivista di diritto bancario*, 08 marzo 2018

IMBRIANI C. – LOPES A., *Teorie macroeconomiche e sistema finanziario*, Novara, 2011

INGRASSIA A., *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine?* in LUPARIA L. (a cura di), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, 15 ss.

INGRASSIA A., *La Suprema Corte e il superamento di una responsabilità di posizione per amministratori e sindaci: una decisione apripista?* in *Diritto penale contemporaneo*, 14 febbraio 2013

INGRASSIA A., *Le diverse forme di sottrazione fraudolenta al pagamento delle imposte*, in BRICHETTI R, VENEZIANI P. (a cura di), *I reati tributari*, Torino, 2017, 378 ss.

INGRASSIA A., *Responsabilità penale degli internet service provider: attualità e prospettive*, in *Dir. pen. Proc.*, 2017, 12, 1621 ss.

ISHMAEV G., *Blockchain technology as an institution of property*, in *Metaphilosophy*, 2017, vol. 48, 5, 665 ss.

J – K

JUELS A., KOSBA A., SHI E., *The Ring of Gyges: Investigating the Future of Criminal Smart Contracts, Conference Paper on Computer and Communication Security*, Vienna, 2016, 2 ss.

KAWAI K., NAGASE T., *The Virtual Currency Regulation Review – Japan*, novembre 2018, in https://thelawreviews.co.uk

KEATINGE T., CARLISLE D., KEEN F., *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, Bruxelles, 2018, in https://europarl.europa.eu

KEYNES J. M., *The General Theory of Employment, Interest, and Money*, New York, 1936

KING D. – WARRACK P., *Real considerations for law enforcement in seizing virtual currency*, June 26 2016, in https://acamstoday.org

KLEIN B., *The competitive supply of money*, in *Journal of Money, Credit and Banking*, 1974, vol. 6, 4, 423 ss.

KOOPS B.J.., *Commanding decryption and the privilege against self-incrimination*, in BREUR, M., KOMMER, J. F. *et al*. (editors), *New trends in criminal investigation and evidence*, Volume II, Antwerpen-Groningen, 2000, 431 ss.

KOOPS, B.J., *Police investigations in Internet open sources: Procedural-law issues*, in *Computer Law & Security Review*, 2013, fasc. 29, 6, 654 ss.

KOOPS B.J., *The Crypto Controversy:A Key Conflict in the Information Society*, The Hague, 1999, 168 ss.;

KRISTOUFEK L., *What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis*, 15 aprile 2015, in https://journals.plos.org

L

LAMBIN J., *A Distributed and Collaborative Economy*, in ID., *Rethinking the market economy*, London, 2014, 164 ss.

LEE D. KUO CHEN, *Handbook of Digital Currency. Bitcoin innovations, financial instruments and big data*, San Diego, 2015

LEMME G., PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, in *Rivista di diritto bancario*, 2016, 11, 27 ss.

LEMME G., *La rivoluzione copernicana della cassazione: la moneta legale, dunque, non coincide con la moneta fisica*, in *Banca, borsa e titoli di credito*, 2008, 2, 553 ss.

LEMME G., *Moneta scritturale e moneta elettronica*, Torino, 2003;

LEONCINI I., *L'obbligo di impedire l'infortunio*, in GIUNTA F., MICHELETTI D., *Il nuovo diritto penale della sicurezza nei luoghi di lavoro*, Milano, 2010, 112 ss.

LEONCINI I., *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza*, Torino, 1999

LESSIG L., *The Law of the Horse. What Cyberlaw Might Teach*, in *Harvard Law Review*, 1999, 4, 501 ss.

LIU Z., CONG LUONG N. *et al*., *A Survey on Applications of Game Theory in Blockchain*, 15 marzo 2019, in https://arxiv.org

LOSAPPIO G., *Risparmio, funzioni di vigilanza e diritto penale. Lineamenti di un sotto sistema*, Bari, 2004

LOTIERZO R., *Il caso* Google-Vivi Down *quale emblema del difficile rapporto degli* internet providers *con il codice della* privacy, in *Cass. Pen*., 2010, 11, 4003 ss.

LUCEV R., BONCOMPAGNI F., *Criptovalute e profili di rischio penale nella attività degli exchanger*, in *Giurisprudenza penale web*, 2018, 3, 1 ss.

LUPÀRIA L., *La disciplina processuale e le garanzie difensive*, in LUPÁRIA L., ZICCARDI G., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, 130 ss.

LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa – Profili processuali,* in *Dir. pen. proc.*, 2008, 6, 717 ss.

LUPARIA L., *Processo penale e tecnologia informatica,* in *Diritto dell'internet,* 2008, 226 ss.

M

MACRILLÒ A., *Le nuove disposizioni in materia di sequestro probatorio e di custodia ed assicurazione dei dati informatici,* in *Dir. Internet*, 2008, 5, 503 ss.

MAGLIOCCO A., *Bitcoin e tassazione*, in *Strumenti finanziari e fiscalità*, 2016, 1, 34 ss.

MAGRI P., *I delitti contro il patrimonio mediante frode*, in MARINUCCI G., DOLCINI E. (diretto da), *Trattato di diritto penale – Parte speciale,* Padova, 2007, 468 ss.

MAJORANA D., *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in *Corriere Tributario*, 2018, 8, 630 ss.

MANES V., *L'ultimo imperativo della politica criminale: nullum crimen sine confiscatione,* in *Riv. it. dir. proc. pen*., 2015, 3, 1260 ss.

MANES V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, in *Riv. trim. dir. pen. econ*., 2004, 1-2, 39 ss.

MANGIONE A., *Mercati finanziari e criminalità organizzata: spunti problematici sui recenti interventi normativi di contrasto al riciclaggio,* in *Riv. it. dir. proc. pen.*, 2000, 3, 1136 ss.

MANNA A., *Colpa cosciente e dolo eventuale: l'indistinto confine ed il principio di stretta legalità*, in *Indice penale*, 2010, 1-2, 9 ss.

MANNA A., *Il bene giuridico tutelato nei delitti di riciclaggio e reimpiego: dal patrimonio all'amministrazione della giustizia, sino all'ordine pubblico ed all'ordine economico*, in ID. (a cura di), *Riciclaggio e reati connessi all'intermediazione mobiliare*, Torino, 2000, 64 ss.

MANNA A., *I soggetti in posizione di garanzia*, in *Dir. Inf.*, 2010, 6, 786 ss.

MANNA A, DI FLORIO M., *Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime,* Milano, 2019, 892 ss.

MANTOVANI F., *Diritto penale – Parte generale,* Padova, 2017

MANTOVANI F., *Diritto penale – Parte speciale*, Vol. II, Padova, 2018

MANTOVANI F., *L'obbligo di garanzia ricostruito alla luce dei principi di legalità, di solidarietà, di libertà e di responsabilità personale*, in *Riv. it. dir. proc. pen*, 2001, 2, 337

MANTOVANI F., *Principi di diritto penale*, Padova, 2002

MARCOLINI S., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. Pen.*, 2015, 2, 761 ss.

MASARONE V., *La responsabilità delle persone giuridiche in rapporto ai delitti di terrorismo tra obblighi internazionali e normativa interna di attuazione,* in *Crit. Dir.* 2014, 3, pp. 225 ss.

MASCIANDRO D., MANTICA A., *Evoluzione dei sistemi di pagamento, internet e cybericiclaggio: prime riflessioni*, in BRUNI E., MASCIANDRO D. (a cura di), *Mercati finanziari e riciclaggio*, Milano 1998

MAUGERI A.M., *La confisca per equivalente ex art. 322-ter tra obblighi di interpretazione conforme ed esigenze di razionalizzazione*, in *Riv. it. dir. proc. pen*., 2011, 2, 783 ss.

MAUGERI A.M., *La lotta all'evasione fiscale tra confisca di prevenzione e autoriciclaggio La confisca dei proventi dell'evasione fiscale o dei redditi leciti non dichiarati fiscalmente?*, in *Diritto penale contemporaneo*, 2 marzo 2015

MAUGERI A.M., *Le moderne sanzioni patrimoniali tra funzionalità e garantismo*, Milano, 2001

MAUGERI A.M., voce *Confisca (diritto penale*), in *Enc. Dir.*, Annali VIII, 2015, § 7

MAY T. C., *The Crypto Anarchist Manifesto*, 1992, in https://activism.net

MAZZACUVA F., *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico*, Torino, 2017, 95 ss.

MAZZACUVA F.., *Il nuovo delitto di dichiarazione fraudolenta mediante altri artifici*, in AA. VV., *Scritti in onore di Luigi Stortoni*, Bologna, 2016, 585 ss.

MAZZOCCHI S., *Esenti da IVA le operazioni di cambio nella valuta virtuale "bitcoin"*, in *Iltributario.it*, 22 dicembre 2015

MCINTOSH N., *Curbing our Right to Online Freedom*, in *The Guardian*, 18 aprile 2001, http://www.guardian.co.uk

MCKINNEY R. E., SHAO L. P., SHAO D. H., ROSENLIEB D. C., *The evolution of financial instruments and the legal protection against counterfeiting: a look at coin, paper, and virtual currencies*, in *Journal of Law, Technology & Policy*, 2015, 2, 273 ss.

MELE S., *La cooperazione tra pubblico e privato nella cyber-security*, in http://www.sicurezzanazionale.gov.it

MENDELSON M., *From Initial Coin Offerings to Security Tokens*: *U.S. Federal Securities Law Analysis*, in *Stanford Technology Law Review*, 2019, vol. 22, 52 ss.

MENDITTO F., *Le confische di prevenzione e penali*, Milano, 2015

MENGHINI A., *Actio libera in causa*, Padova, 2015

MERUSI F., *Profili pubblicistici dell'attività parabancaria e dell'innovazione finanziaria*, in AA. VV., *Studi in onore di Massimo Severo Giannini*, Milano, 1988, 437 ss.

METJAHIC L., *Deconstructing the Dao: the Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations*, in *Cardozo Law Review*, 2018, vol. 39, 1550 ss.

MEZZETTI E., *Reati contro il patrimonio*, Milano, 2013

MICHELINI G., POLIMENI G., *Il fenomeno del crimine transnazionale e la Convenzione della Nazioni Unite contro il crimine organizzato transnazionale*, in ROSI E. (a cura di), *Criminalità organizzata transnazionale e sistema penale italiano: la Convenzione ONU di Palermo*, Milano, 2007

MICHELETTI D., *La posizione di garanzia nel diritto penale del lavoro*, in *Riv. trim. dir. pen. econom.*, 1 - 2, 2011, 155 ss.

MINICUCCI G. *Le frodi informatiche*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 827 ss.

MOLINARO G., *Sono tassabili le manifestazioni di capacità economica emergenti nelle operazioni relative a Bitcoin?*, in *Il Fisco*, 2014, 25, 2447 ss.

MONTANI E., *La tutela del corretto svolgimento dell'attività di intermediazione e bancaria*, in ALESSANDRI A. (a cura di), *Reati in materia economica*, Torino, 2017, 237 ss.

MORENO-SANCHEZ P. – BILAL ZAFAR M., *Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network*, in *Proceedings on Privacy Enhancing Technologies*, 2016, 4, 436 ss.

MÖSER M. – SOSKA K., *An Empirical Analysis of Traceability in the Monero Blockchain*, in *Proceedings on Privacy Enhancing Technologies*, 2018, 3, 143 ss.

MUCCIARELLI F., *Commento all'art.10 della legge 547 del 1993*, in *Leg. Pen.*, 1996, 136 ss.

MUCCIARELLI F, *Qualche nota sul delitto di autoriciclaggio*, in *Diritto penale contemporaneo – Rivista trimestrale*, 1, 2015, 159 ss.

MUCCIARELLI F., PALIERO C.E., *Le Sezioni Unite e il profitto confiscabile: forzature semantiche e distorsioni ermeneutiche*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2015, 4, 246 ss.

MULINARI S., *Cyberlaundering*, Torino, 2003

MUSCO E., ARDITO F., *Diritto penale fallimentare*, Bologna, 2018

MUSCO E., ARDITO F., *Diritto penale tributario*, Bologna, 2016

N - O

NADDEO M., MONTEMURRO D., *Autoriciclaggio e teoria degli insiemi: un "privilegio" matematicamente sostenibile*, in *Riv. trim. dir. pen. econ.*, 2011, 237 ss.

NAKAMOTO S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, in https://bitcoin.org

NAPOLI P., *The Algorithm as Institution: Toward a Theoretical framework for automated Media Production and Consumption*, in https://papers.ssrn.com

NAVONE G., *La data del documento informatico: osservazioni in materia di validazione temporale*, in *Obbligazioni e contratti*, 2009, 4, 364 ss.

NICOSIA E., *La confisca, le confische. Funzioni politico-criminali, natura giuridica e problemi ricostruttivo-applicativi*, Torino, 2012

OLIVARI A., *Santi Romano ontologo del diritto*, Milano, 2016, 103

ORCUTT M., *No, Ripple Isn't the Next Bitcoin*, in *MIT Technology Review – Web*, 11 gennaio 2018, 1 ss.

P

PACCAGNELLA L., *La comunicazione al computer. Sociologia delle reti telematiche*, Bologna, 2000

PACCAGNELLA L., *Il potere dei codici: crittografia, cypherpunk e movimenti sociali*, in *Quaderni di sociologia*, 2000, 23

PAGLIARO A., (voce) *Legge penale nello spazio*, in *Enc. Dir*., 1973, 1055 ss.

PAGLIARO A., *Principi di diritto penale - Parte generale*, Milano, 1998

PALAZZO F., *Contrasto al terrorismo, diritto penale del nemico e principi fondamentali*, in *Quest. Giust.*, 2006, 674 ss.

PALAZZI M., *I rapporti tra il delitto di autoriciclaggio e quello di trasferimento fraudolento di valori*, in MEZZETTI E.-PIVA D., *Punire l'autoriciclaggio: come, quando e perché*, Torino, 2016, 55 ss.

PALFREYMAN B. M., *Lessons from the British and American Approaches to Compelled Decryption*, in *Brooklyn Law Review*, 2009, 75, 1, 346 ss.

PALIERO C.E., *La causalita dell'omissione: formule concettuali e paradigmi prasseologici*, in *Rivista Italiana di medicina legale*, 1992, 4, 828 ss.

PALUMBO G., *Il trattamento tributario dei bitcoin*, in *Diritto e Pratica Tributaria*, 2016, 1, 2079 ss.

PANATTONI B., *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di notice and take down*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2018, 5, 249 ss.

PANTANELLA A., *Il bene giuridico nel reato di esercizio abusivo di intermediazione finanziaria*, in *Cass. Pen*., 2017, 306 ss.

PARISOTTO R., *Il quadro RW tra valute virtuali e normativa antiriciclaggio*, in *Corriere tributario*, 2018, 15, 1156 ss.

PASSARETTA M., *Bitcoin: il leading case italiano*, in *Banca Borsa Titoli di Credito*, 2017, 4, 471 ss.

PERINI A., voce *Reati tributari*, in *Dig. Pen. Agg*., Torino, 2016, 573 ss.

PEZZELLA V., *Google Italia, diffamazione e riservatezza: il difficile compito del* provider *(e del giudice)*, in *Giur. mer*., 2010, 2232 ss.

PIASENTE M., *Esenzione IVA per i "bitcoin": la strada indicata dalla Corte UE interpretando la nozione "divise"*, in *Corriere Tributario*, 2016, 2, 141 ss.

PICCINNI L.M., DI FRANCO G., *Genesi normativa e peculiarità del money laundering: il delitto di riciclaggio quale reato presupposto per la configurazione dell'art. 25-octies, d.lgs. 231/2001. Da reato dei white collars, a diffuso illecito di criminalità economica*, in *Responsabilità amministrativa delle società e degli enti*, 2015, 1, 32 ss.

PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme,* in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 39 ss.

PICOTTI L., *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee,* in *Riv. trim. dir. pen. econom*., 2011, 4, 827 ss.

PICOTTI L., *Fondamento e limiti della responsabilità penale dei* service-providers *in* internet, in *Dir. pen. proc*., 1999, 1, 379 ss.

PICOTTI L., *Internet e responsabilità penali,* in PASCUZZI G., *Diritto e informatica,* Milano, 2002, 117 ss.

PICOTTI L., *La legge contro lo sfruttamento sessuale dei minori e la pedopornografia in internet*, in *Studium iuris*, 2007, 1207 ss.

PICOTTI L., *La "Raccomandazione" del XV Congresso Internazionale di diritto penale in tema di criminalità informatica,* in *Riv. trim. dir. pen. econ.,* 1995, 4, 1279 ss.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa – Profili sostanziali*, in *Dir. pen. proc.*, 2008, 6, 700 ss.

PICOTTI L., *La rilevanza penale degli atti di «sabotaggio» ad impianti di elaborazione dati,* in *Dir. Inf.*, 1986, 3 969 ss.

PICOTTI L., *La responsabilità penale dei service-providers in internet,* in *Dir. pen. proc*., 1999, 2, 501 ss.

PICOTTI L., *Le nuove definizioni penali di pubblico ufficiale e di incaricato di pubblico servizio nel sistema dei delitti contro la pubblica amministrazione*, in *Riv. trim. dir. pen. econom*, 1992, 264 ss.

PICOTTI L., *L. 23 dicembre 1993, n. 547. Commento all'art. 8 l. 23 dicembre 1993, n. 547*, in *Legislazione penale,* 1996, 1-2, 129 ss.

PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ.,* 2018, 3-4, 596 ss.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004

PISELLI R., *Autonomia negoziale, potere e blockchain. La rivoluzione del contratto,* in NUZZO A. (a cura di), *Blockchain e autonomia privata. Fondamenti giuridici*, Roma, 2019, 25 ss.

PITTIRUTI M., *Digital evidence e procedimento penale*, Torino, 2017

PIVETTI M., *Economia politica*, Bari, 2002

PLASSARAS, N.A., *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, in *Chicago Journal of International Law*, 2013, 14, 377 ss.

PECORELLA C., *Diritto penale dell'informatica,* Padova, 2006

PECORELLA C., voce *Reati informatici*, in *Enciclopedia del Diritto*, ann. X, Milano, 2017, 707 ss.

POMANTE G., *Internet e criminalità*, Torino, 1999

POPP A., *§202c StGB und der neue Typus des europäischen «Software-Delikts»*, in *Goltdammer's Archiv für Strafrecht*, 2008, 375 ss.

PUTINATI S., *Dichiarazione fraudolenta mediante altri artifici*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Diritto penale dell'economia*, vol. I, Vicenza, 2017, 723 ss.

Q- R

RASKIN M., *The Law and Legality of Smart Contracts*, in *Georgetown Law & Tech Review*, 2017, 1, 311 SS.

RESTA F., *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, in *Giur. merito*, 2008, 2147 ss.

RESTA F., *La responsabilità penale del provider: tra laissez faire ed obblighi di controllo*, in *Giur. mer.*, 2004, 9, 1733

RESTA G., *L'identità digitale e l'identità personale*, in *Dir. Inf.*, 2007, 3, 511 ss.

ROCCO A., *L'oggetto del reato e della tutela giuridica penale,* Torino, 1913

RODORORF R., *La Consob come autorità indipendente nella tutela del risparmio*, in *Foro Italiano*, 2000, 147 ss.

RODOTÀ S., *Una Costituzione per Internet*, in *Politica del diritto*, 2010, 3, 339 ss.

RODRIGUEZ AYUSO J. F., *Verso il raggiungimento di un mercato unico interno in materia di transazioni elettroniche. Il nuovo regolamento europeo 910/2014*, in *Federalismi.it*, 2017, 24, 25 ss.

ROMANO M., *I delitti contro la pubblica amministrazione. I delitti dei privati. Le qualifiche soggettive pubblicistiche*, in ID., *Commentario sistematico al codice penale*, Milano, 2013, 16 ss.

ROMANO M., GRASSO G., *Commentario sistematico al codice penale*, Sub *art. 87*, Milano 2012, 30

ROMANO S., *L'ordinamento giuridico*, Firenze, 1917

ROSEMBUJ T., *Bitcoin*, Barcelona, 2016

ROSENDAAL A., *Digital personae and profiles as representations of individuals*, in BEZZI M., DUQUENOY P., FISCHER-HÜBNER S. (a cura di), *Privacy and identity management for life*, Tilburg, 2010, 226 ss.

ROSSI A., *I soggetti persone giuridiche: su quali enti vigila il D.Lgs. 231*?, in *Le Società*, 2011, 1, 24 ss.

ROSSI A., *Prevenzione del riciclaggio e finanziamento del terrorismo: finalità e novità normative*, in *Dir. pen. proc.*, 2018, 1, 25 ss.

ROXIN C., *Strafrecht, Allgemeiner Teil*, Vol. II, *Besondere Erscheinungsformen der Straftat*, Monaco, 2003

RUGA RIVA C., *L'abusivismo finanziario: questioni giurisprudenziali e profili di illegittimità costituzionale*, in *Riv. trim. dir. pen. econ.*, 2001, 3, 531 ss.

S

SAGLIOCCA A., *Open Source Intelligence e Deep Web: scenari moderni delle investigazioni digitali*, in *Ciberspazio e diritto*, 2017, 1, 171 ss.

SALCUNI G., *Le falsità informatiche*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Milano, 2019, 273 ss.

SALERNO A., *Il nuovo falso in prospetto*, in CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Diritto penale dell'economia*, Milano, 2016, 453 ss.

SALVADORI I., *Criminalità informatica e tecniche di anticipazione della tutela penale. L' incriminazione dei "dual-use software"*, in *Riv.it. dir. proc. pen*., 2017, 2, 750 ss.

SALVADORI I., *Il microsistema normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Rivista italiana di diritto e procedura penale*, 2012, 1, 204 ss.

SANFILIPPO P., *L'incerta riforma dei reati di dichiarazione fraudolenta: la riformulazione degli artt. 2 e 3 d.lgs. 74/2000 ad opera del d.lgs. 158/2015 e gli evanescenti profili di differenziazione tra le fattispecie*, in *Legislazione penale*, 2016, 4, 2 ss.

SANTINI S., *L'Unione Europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della direttiva 2017/541*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2017, 7-8, 13 ss.

SARVANKAR S., *Key Disclosure Laws and the Right Against Self-Incrimination in India*, 3 novembre 2017, in https://ssrn.com

SARZANA DI S. IPPOLITO C., *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. proc*, 2008, 12, 1562 ss.

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

SAVONA E.U., *Economia e criminalità*, in *Enciclopedia delle scienze sociali*., vol. IX, Roma, 2001, 97 ss.

SCACCHI F., ZAGHINI G., *MiFID II. I servizi di comunicazione dati: APA, ARM e CTP, in Rivista di diritto bancario*, 18 settembre 2015, 1 ss.

SCARCELLA A., *L'inquinamento elettromagnetico tra getto pericoloso di cose e principio di tassatività in malam partem in materia penale: un difficile compromesso per affermare la rilevanza penale del fatto,* in *Cass. Pen.*, 2009, 3, 944 ss.

SCELSI R. (a cura di), *Cyberpunk. Antologia di testi politici*, Milano, 1990

SCIUBA M. L., *Il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico*, in *Cass. Pen*., 2015, 10, 3507 ss.

SCOLETTA M, *Il nuovo regime penale delle falsità informatiche*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, 28 ss.

SCOLETTA M., *La responsabilità da reato delle società: principi generali e criteri imputativi nel d.lgs. n.231/2001, in* CANZIO G., CERQUA L.D., LUPÀRIA L. (a cura di), *Diritto penale delle società, I, I profili sostanziali*, Padova, 2014, 877 ss.

SEMINARA S., *Delitto tentato e reato impossibile: in confini dell'azione punibile*, in *Spazio filosofico*, 2016, 16, 1 ss.

SEMINARA S., *I soggetti attivi del reato di riciclaggio tra diritto vigente e prospettive di riforma*, in *Dir. pen. proc.*, 2005, 236 ss.

SEMINARA S., *La pirateria su internet e il diritto penale*, in *Riv. trim. dir. pen. ecom.*, 1997, 1, 71 ss.

SEMINARA S., *La responsabilità penale degli operatori su internet*, in *Dir. Inf.*, 1998, 3, 745 ss.

SEMINARA S., *Nuovi illeciti penali e amministrativi nella legge sulla tutela del risparmio*, in *Dir. pen. proc*., 2006, 549 ss.

SERENI A., *Causalità e responsabilità penale*, Torino, 2008

SERGIENKO G., *Self Incrimination and Cryptographic Keys*, in *Richmond Journal of Law & Technology*, 1996, 2

SEVERINO P., *I delitti dei pubblici ufficiali contro la pubblica amministrazione, Le qualifiche soggettive*, Milano, 1983

SEVERINO P., *Pubblico ufficiale e incaricato di un pubblico servizio* voce, in *Dig. disc. pen.*, X, 508 ss.

SEVERINO P., *Sicurezza informatica e prevenzione del cybercrime*, in *LuissOpen*, 8 settembre 2017, 11, 1 ss.

SGUBBI F., *Il falso in prospetto*, in GALGANO F., ROVERSI MONACO F., *Le nuove regole del mercato finanziario*, Padova, 2009, 649 ss.;

SGUBBI F., *Il falso in prospetto,* in SGUBBI F., FONDAROLI D., TRIPODI A.F., *Diritto penale del mercato finanziario,* Padova, 2013, 277 ss.

SGUBBI F., *Il nuovo delitto di "autoriciclaggio": una fonte inesauribile di "effetti perversi" dell'azione legislativa,* in *Diritto penale contemporaneo*, 10 dicembre 2014

SGUBBI F., *Il risparmio come oggetto di tutela penale*, in *Giurisprudenza commerciale*, 2005, 1, 345 ss.

SGUBBI F., *Parere pro-veritate*, in *Dir. inf.*, 2009, 2, 746 ss.

SGUBBI F., *Responsabilità penale per omesso impedimento dell'evento*, Padova, 1975

SGUBBI F., voce *Patrimonio (reati contro il)*, in *Enc. Dir*., XXXII, 1982

SIEBER U., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer*, in *Riv. trim. dir. pen. ecom.*, 1997, 756 ss.

SICIGNANO G. J., *Bitcoin e riciclaggio*, Torino, 2019

SIGNORELLI A., *Il valore giuridico del documento informatico*, in *Il processo telematico*, 15 marzo 2019

SIMONCINI E., *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, in *Riv. Trim. Dir. Pen. Econ*., 2015, 4, 907 ss.

SINGH R., DWIVEDI A.D., SRIVASTAVA G., *Bitcoin Mining: A Game Theoretic Analysis*, in https://semanticscholar.org

SKLAROFF J.M., *Smart Contracts and the Cost of Inflexibility*, in *University of Pennsylvania Law Review*, 166, 2017, 262 ss.

SOANA G., *I reati tributari*, Milano, 2018

SOLDAVINI P., *Il governo Usa non ci ha creduto: svenduti all'asta i bitcoin sequestrati*, in *IlSole24Ore*, 29 maggio 2017

SORBELLO P., *L'abusivismo finanziario tra atto giuridicamente lecito e fatto penalmente rilevante*, in *Giur. Mer.*, 2009, 2499 ss.

SORO A., *Tra privacy e open data intesa possibile*, in *Il Sole24Ore*, 13 ottobre 2014

SPAGNUOLO M – MAGGI F. – ZANERO S., *BitIodine: Extracting Intelligence from the Bitcoin Network*, in AA. VV., *Financial Cryptography and Data Security*, Heidelberg, 2014, 457 ss.

SPATAZZA G., *La società di fatto*, Milano, 1980

SPAZIANTE F., *Le operazioni concernenti i "bitcoin": la declinazione pratica dei principi espressi nella sentenza Hedqvist*, in *Fiscalità e Commercio Internazionale*, 2016, 8, 29

STANZIONE G., *Autoincriminazione e diritto al silenzio*, Padova, 2017

STELLA F., *Leggi scientifiche e spiegazione causale nel diritto penale*, Milano, 1975

STELLA F., *La nozione penalmente rilevante di causa*, in *Riv. It. dir. proc. pen*, 1988, 1217 ss.

STURZO L., *Bitcoin e riciclaggio 2.0*, *Diritto penale contemporaneo*, 2018, 5, 19 ss.

SUMMERS S. – SCHWARZENEGGER C. – EGE G. – YOUNG F., *The Emergence of EU Criminal Law. Cyber-crime and the regulation of the information society*, Oxford, 2014

SURDEN H., *Computable Contracts*, in *UC Davies Law Review*, 2012, 46, 629 ss.

SWANSON T., *Great Chain of Numbers: A guide to Smart Contracts, Smart Property and Asset Management*, Oxford, 2014

T

TASCA P., WIDMANN S., *The challenges faced by blockchain technologies*, in *Journal of Digital Banking*, 2017, 2, 132 ss.

TASCA P., TESSONE C., *Taxonomy of Blockchain Technologies. Principles of Identification and Classification*, 31 marzo 2018, in https://papers.ssrn.com

TEUBNER G., *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten*, in *Ancilla Iuris*, 2018, vol. 35, 38 ss.

TEUBNER G., *Ibridi e attanti, Attori collettivi ed enti non umani nella società e nel diritto*, Milano, 2015

TIWARI N., *The Commodification of Cryptocurrency*, in *Michigan Law Review*, vol. 117, 3, 612 ss.

TODINI C., voce *Imposta sul valore aggiunto*, in *Enciclopedia Treccani – Diritto online*, 2016, in https://treccani.it

TRINCHERA T., *La sentenza delle Sezioni Unite in tema di confisca di beni societari e reati fiscali*, in *Diritto penale contemporaneo*, 12 marzo 2014

TRIPODI A.F., *La Cassazione alla prova dello spamming, tra presunzione e torsioni*, in *Diritto penale contemporaneo*, 2 luglio 2013

TROPINA T., *Public-Private Collaboration: Cybercrime, Cybersecurity and National Security*, in TROPINA T.– CALLANAN C., *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*, Berlino, 2015, 2 ss.

U - V

VACIAGO G., *Digital evidence, I mezzi di ricerca della prova nel processo penale e le garanzie dell'indagato*, Torino, 2012

VALSECCHI V., *La classificazione delle Blockchain: pubbliche, autorizzate e private,* in https://spindox.it

VARDI N., *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. Inf.*, 2015, 1, 450 ss.

VENDITTI M., *Actio libera in causa*, in *Enciclopedia del diritto*, 1958, I, 53 ss.

VENEZIANI P., sub *Art. 3*, in CARACCIOLI I., GIARDA A., LANZI A. (a cura di), *Diritto e procedura penale tributaria. Commentario al D. Lgs. 10 marzo 2000 n. 74*, Padova, 2000, 147 ss.

VENTURINI S., *Sequestro probatorio e fornitori di servizi telematici*, in LUPÀRIA L., *Internet provider e giustizia penale*, Milano, 2012, 107 ss.

VERGINE F., *Confisca e sequestro per equivalente*, Milano, 2009

VITRÒ V., *Le società di fatto: profili sostanziali ed effetti del fallimento*, Milano, 2009

VIZZARDI M., *La Cassazione sul caso Dolce e Gabbana: elusione fiscale e truffa aggravata a danni dello Stato,* in *Diritto penale contemporaneo,* 22 giugno 2012

W - X

WAKNIS P., *Competitive Supply of Money in a New Monetarist Model,* MPRA Paper No. 75401, 11 settembre 2017, https://mpra.ub.uni-muenchen.de

Y- Z

YERMACK D., *Is Bitcoin a real currency? An economic appraisal,* NBER Working Paper No. 19747, National Bureau of Economic Research, Cambridge (MA), 2013

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

ZANCHETTI M., *Il riciclaggio di denaro proveniente da reato,* Milano, 1997

ZANCHETTI M., *Art. 648 bis c. p.*, in CRESPI A.– FORTI G.– ZUCCALÀ G., *Commentario breve al codice penale,* Padova, 2008, 1939 ss.

ZANCHETTI M., *Sub art. 648- ter c.p.*, in CRESPI A., STELLA F., ZUCCALÀ G. (a cura di), *Commentario breve al codice penale,* Padova, 2008, 2297 ss.

ZANNOTTI R, *La truffa*, Milano, 1993

ZANNOTTI R., *La tutela dell'accesso al mercato nella prospettiva della lotta contro il riciclaggio: il caso dell'abusivismo*, in *Indice penale*, 2003, 929 ss.

ZANNOTTI R., *La tutela penale del mercato finanziario*, Torino, 1997

ZANNOTTI R., *Il nuovo diritto penale dell'economia*, Milano, 2017

ZENO ZENCOVICH V., *I rapporti fra responsabilità civile e responsabilità penale nelle comunicazioni su* internet *(riflessioni preliminari)*, in *Dir. Inf.*, 1999, 6, 1049 ss.

ZIRULIA S., *Le Sezioni Unite sul tempus commissi delicti nei reati c.d. ad evento differito*, in *Diritto penale contemporaneo*, 4 ottobre 2018

ABBREVIAZIONI RICORRENTI

Arch. Pen.
Archivio Penale

Cass. Pen.
Cassazione Penale

Giur. mer.
Giurisprudenza di merito

Dir. Inf.
Diritto dell'informazione e dell'informatica

Dir. Internet

Diritto dell'Internet

Dir. Pen. cont.
Diritto penale contemporaneo

Dir. pen. proc.
Diritto penale e processo

Leg. Pen.
Legislazione penale

Riv. it. dir. proc. Pen.
Rivista italiana di diritto e procedura penale

Riv. trim. dir. pen. econ.
Rivista trimestrale di diritto penale dell'economia