UNIVERSITÀ DEGLI STUDI DELL'INSUBRIA DIPARTIMENTO DI DIRITTO, ECONOMIA E CULTURE

DOTTORATO DI RICERCA IN DIRITTO E SCIENZE UMANE

XXXVI CICLO

CRIPTOVALUTE E DIRITTO PENALE: PROGRESSO TECNOLOGICO, LIMITI NORMATIVI, LINEE DI RIFORMA.

Tutor: Chiarissima Prof.ssa Chiara Perini

Tesi di Dottorato di
Carlotta Calemme
Matricola n. 725004

A Stefano,
per la dedizione,
la pazienza e l'amore
con cui mi sostiene
nella realizzazione dei miei sogni.

Alla mia Famiglia,
meravigliosa e imperfetta
così com'è.

INDICE

INTRODUZIONE

Nel contesto socioculturale attuale – sempre più pervaso dall'innovazione informatica e tecnologica – un ruolo predominante è stato assunto negli ultimi anni dalla *blockchain* applicata alle criptovalute.

Detta tecnologia, seppur nata come strumento positivo, funzionale alla pubblicità e alla trasparenza delle transazioni, viene sfruttata dai *cybercriminal,* criminali economici del XXI secolo, con effetti disfunzionali su beni giuridici primari e per l'economia.

Ed invero, detti soggetti, forti dei vuoti normativi in materia, da un lato, sfruttando le caratteristiche proprie della *blockchain* – quali la decentralizzazione, lo pseudoanonimato e l'irreversibilità delle transazioni– e, dall'altro lato, servendosi anche di specifici *software* di *mixing* e *tumbling,* hanno dato vita ad un'ampia casistica di condotte di truffa, riciclaggio, finanziamento del terrorismo, manipolazione del mercato ed *insider trading* basati sull'impiego di criptovalute.

La ricerca muove dall'assunto che vi sia un rapporto inscindibile tra *economia*, *criminalità*, e *diritto penale* fortemente influenzato dal continuo evolversi della tecnologia e dell'informatica. Premessa, questa, che impone – evidentemente – un approccio interdisciplinare volto a comprendere in maniera approfondita il fenomeno indagato da un punto di vista criminologico e sociologico, quindi economico e informatico, ancor prima che penalistico.

In tal senso, lo studio condotto intende indagare il fenomeno della "criminalità economica criptovalutaria" guardando alle caratteristiche del soggetto agente, alle sue modalità di condotta e agli strumenti utilizzati per delinquere, nella consapevolezza che egli – lungi dall'agire a causa di spinte emotive irrazionali – persegue precisi scopi economici, che rappresentano le coordinate di tutte le scelte compiute.

A fronte di meglio comprendere la portata criminale del fenomeno in parola, sarà necessario analizzare la tecnologia *blockchain*, come studiata dalle *scienze informatiche*. Bisognerà, in tal senso, verificare se la normativa penalistica vigente sia già rispondente alle esigenze imposte dal principio di tipicità ovvero in che termini possa e debba essere integrata.

Stante la particolarità della materia, la trattazione verrà condotta prendendo in considerazione i beni giuridici tutelati dall'ordinamento. Verrà quindi analizzata la casistica manifestatasi nell'ultimo decennio al fine di vagliare la sussumibilità delle condotte descritte nelle fattispecie incriminatrici già presenti nell'ordinamento. La riflessione avrà, dunque, ad oggetto la compiutezza del passaggio dal *piano sostanziale* al *piano formale*, sì da indagare se il *crimine* considerato sia già previsto come *reato* ovvero, tanto nel rispetto del principio di legalità quanto di offensività, sia necessario un intervento del legislatore volto a garantire che condotte offensive di beni giuridici già tutelati dall'ordinamento non rimangano impunite.

L'analisi, infine, si sposterà sulle ultime frontiere dei crimini economici che possono essere commessi con l'utilizzo di criptovalute. In tal senso, si procederà ad individuare quei reati che, già previsti dall'ordinamento nella loro forma tradizionale, potrebbero venire ad esistenza anche con l'utilizzo di criptovalute, ad oggi ancora rientranti nella c.d. *cifra nera.*

CAPITOLO I

ANALISI ECONOMICA DEL DIRITTO PENALE E *CYBERCRIME*

1. *Premessa.*

Obiettivi principali del presente studio sono l'individuazione e l'analisi dei reati economici perfezionati e perfezionabili tramite l'utilizzo delle criptovalute basate su tecnologia *blockchain*, al fine di proporre, in un'ottica principalmente general-preventiva, soluzioni normative idonee ad arginare il fenomeno criminale in parola.

Vedremo, infatti, come i *cybercriminal*, forti delle proprie competenze informatiche, riescano ad eludere le caratteristiche della tecnologia *blockchain*, tenendo, così, condotte idonee a ledere beni giuridici di natura economica, con importanti ricadute sul ciclo economico nazionale, europeo ed internazionale.

La ricerca muove dall'assunto che vi sia un rapporto inscindibile tra *economia*, *criminalità* e *diritto penale* fortemente influenzato dal continuo evolversi della tecnologia e dell'informatica. Premessa, questa, che impone – evidentemente – un approccio interdisciplinare volto a comprendere il fenomeno indagato da un punto di vista criminologico e sociologico, quindi economico ed informatico, ancor prima che penalistico.

Appare, invero, necessario riflettere sulle caratteristiche del soggetto agente del crimine economico informatico, le condotte poste in essere, gli strumenti utilizzati per delinquere, nella consapevolezza che tale modello di autore – lungi dal rispondere a semplici spinte emotive irrazionali – persegue precisi scopi economici, che orientano le scelte compiute.

2. *Crimine e reato economico.*

Il fenomeno in parola impone, innanzitutto, di indagare la criminalità economica da un punto di vista sia oggettivo sia soggettivo. È, in tal senso, necessario delimitare l'area di ricerca comprendendo cosa sia un *reato economico*, *da chi sia commesso* e *a quale scopo.* Ed invero, muovendo da una definizione prettamente criminologica (e non giuridica) possiamo affermare che sono qualificabili alla stregua di "crimini economici" i reati caratterizzati da uno stretto rapporto con un'attività professionale o imprenditoriale in ragione delle qualità del soggetto agente, della condotta tenuta, delle tecniche utilizzate per commettere il reato e degli scopi perseguiti[1].

Al riguardo, è bene sin d'ora osservare come, da un punto di vista *giuridico-criminologico*, i concetti di *crimine* e di *reato,* ancorché strettamente connessi, debbano essere tenuti distinti. Vediamo, infatti, come sin dall'inizio del XX secolo importanti sociologi e giuristi si siano interrogati in ordine all'effettivo nucleo degli studi condotti, anche al fine di comprendere quando i due concetti in parola vengano, sostanzialmente, a sovrapporsi, fondendosi in un unico significato. Trattasi, di questione tutt'altro che nominalistica, soprattutto in quegli ordinamenti – come quello italiano – in cui è possibile ravvisare in materia un dualismo linguistico-terminologico, assente in altri idiomi[2].

Per comprendere cosa sia il *reato economico*, è necessario declinare il fenomeno criminale, *lato sensu* inteso, su due diversi piani: il *piano formale* e il *piano sostanziale*[3].

Mentre il *piano formale* guarda alla parte dell'ordinamento giuridico costituito da norme incriminatrici e, quindi, al *reato*, il piano *sostanziale* indaga il *crimine,* inteso come il fenomeno criminale manifestatosi *ex ante* e comunque sottostante alla scelta di incriminazione effettuata dal legislatore. Possiamo quindi dire che mentre il concetto di *reato* contiene quello di *crimine,* quest'ultimo ne rappresenta il sostrato.

La distinzione tra i due piani appare particolarmente rilevante nella materia trattata in ragione delle peculiarità della scienza penale economica, che richiedono sempre più spesso una compenetrazione tra discipline giuridiche e criminologiche. Quel che è certo, infatti, è che storicamente, la *criminalità economica* ha rappresentato, e rappresenta tuttora, il volano del settore criminale: tra i fenomeni criminali che lo Stato intende combattere, quello economico è da sempre caratterizzato da tecniche criminali in continua evoluzione (sul piano sostanziale), difficilmente prevedibili dal potere legislativo, impegnato a una continua rincorsa a fattispecie incriminatrici e, quindi, sanzioni capaci di prevenire – ancorché con fisiologico ritardo – la

---

[1] E.U. SAVONA, Voce "*Economia e criminalità*" in *Enciclopedia delle Scienze Sociali, Istituto della Enciclopedia Italiana Treccani,* Roma*,* 2001*,* pp. 1-10.

[22] Ad esempio, la lingua inglese e la lingua tedesca utilizzano, rispettivamente, i termini *crime* e *Verbrechen*, tanto per indicare il concetto criminologico di *crimine* quanto il fatto antigiuridico riconducibile al *reato*. La lingua tedesca, a ben vedere, distingue il *Verbrechen* dal *Vergehen*, per indicare fatti antigiuridici per i quali è comminata una pena detentiva non inferiore ad un anno e fatti antigiuridici per i quali è prevista una pena detentiva inferiore o una pena pecuniaria. Sul punto, si rinvia a G. FORTI, *L'immane concretezza. Metamorfosi del crimine e controllo penale*, Raffaele Cortina Editore, 2001, p. 300.

[3] G. FORTI, *op.cit.*, pp. 297 ss.

commissione di comportamenti criminosi con siffatte caratteristiche (sul piano formale).

Ragionare per piani, quindi, permetterà di verificare, da un lato, che una fattispecie incriminatrice già presente nell'ordinamento sia effettivamente coerente con il fenomeno che vuole combattere e, quindi, idonea a tutelare in maniera *effettiva* il bene giuridico di riferimento; dall'altro lato, se un dato fenomeno, ancora non tipizzato, sia meritevole e bisognoso di tutela e, quindi, se il sistema presenti o meno lacune[4].

In siffatto contesto, la comprensione e lo studio delle circostanze di luogo e di tempo in cui vengono a consumarsi determinate condotte dovrebbero permettere un più efficiente passaggio dal *piano sostanziale* al *piano formale*. È di tutta evidenza, infatti, come la conoscenza dei meccanismi criminogeni che caratterizzano un dato fenomeno criminale permetta, quantomeno in astratto, migliori politiche preventive del reato.

Il secondo interrogativo riguarda tanto il *criminale economico* quanto i *motivi* che lo spingono ad agire *contra ius*. Trattasi di quesiti fondamentali in un'ottica di general-prevenzione: comprendere le motivazioni e gli scopi che sottostanno all'agire criminale di detti soggetti è necessario per immaginare e, quindi, prevedere una risposta sanzionatoria più adeguata capace di rispondere, in ottica *special-preventiva*, alle esigenze rieducative della pena.

La risposta a detto quesito può essere elaborata sulla base di due differenti approcci criminologici: *la teoria delle associazioni differenziali* e *l'analisi economia del diritto.*

3. *Il criminale economico.*

Preliminarmente, è bene osservare come sin dai primi anni del XX secolo, illustri studiosi, tra criminologi ed economisti, hanno iniziato ad interrogarsi sul binomio *crimine-economia*, individuando un forte nesso tra crimine, criminale, condizioni economiche e motivi a delinquere. Ed invero, il reato, sino ad allora considerato quale prodotto del libero agire[5] è stato

---

[4] Cfr. G. FORTI, *op.cit.,* p. 297 ss.

[5] La Scuola Liberale Classica, sviluppatasi durante gli anni dell'Illuminismo, è stata fondata sui principi liberali, che guardano al diritto penale quale *extrema ratio*, fondato sui principi di certezza del diritto, legalità, offensività, proporzione e colpevolezza. La Scuola Liberale Classica ha sempre guardato all'Autore del reato come a un uomo razionale, dotato di libero arbitrio, pertanto capace di scegliere se e come agire. Chi delinque, quindi, non è un soggetto con caratteristiche biologiche o psicologiche diverse. La scuola classica, dunque, ritiene che gli studi criminologici non debbano guardare al delinquente in quanto tale, alle sue condizioni individuali e alle cause del crimine. È possibile, in particolare, evincere tre principi fondamentali: 1) la condotta di reato è frutto di una libera e volontaria scelta dell'uomo, dettata dal suo libero arbitrio; 2) l'agente è imputabile, in quanto è

progressivamente ricondotto dalla Scuola Positiva all'ambiente sociale cui l'individuo apparteneva. In detto contesto, si sono sviluppati due diversi filoni di ricerca: il *determinismo sociale* e il *determinismo biologico*[6].

Mentre i fautori del *determinismo sociale* ritenevano che l'agire criminoso non fosse mosso unicamente dalla volontà del singolo quanto, piuttosto, da fattori legati al suo contesto sociale, il *determinismo biologico* interpretava il reato come la conseguenza di patologie psichiche da cui erano affetti gli autori. I positivisti, in definitiva, consideravano il crimine quale fenomeno dovuto a cause specifiche riconducibili ad alterazioni biologiche, psichiche e sociali, che rendevano i soggetti (poi autori di reato) essenzialmente "diversi" dagli altri consociati.

Con l'avvento del pensiero marxista, poi, il *focus* è stato spostato sulle *diseguaglianze sociali* causate dal rapporto tra classi.

In particolare, William Adrian Bonger, nel 1916, nell'analizzare dati statistici relativi ai furti commessi in tredici Paesi, in diversi periodi del XX secolo, scriveva testualmente: "*There are some needs which a man must satisfsy, without which his existence is impossible. These are fundamental needs, independent of environment. If a man has not sufficient food, if he has not (...) clothing to protect him against cold, if opportunity for rest is lacking, etc., his life is danger. In our present society there are always a number of person who are in want of the strict necessaries of life, and who are therefore obliged to steal if they do not wish to succumb to poverty*"[7]. Bonger, pur riconoscendo l'esistenza di differenze innate e fisiologiche tra individui, ha rilevato come i fattori scatenanti il comportamento criminoso dovessero essere ricercati nell'ambiente sociale e nello sviluppo economico e, più precisamente, nella lotta tra classi, che favoriva il passaggio da una *potenziale aggressività* all'*effettiva commissione di un reato.* Ha sostenuto, al riguardo, che a causa del capitalismo l'uomo fosse divenuto particolarmente egoista e, quindi, maggiormente soggetto alle spinte criminali che, al contrario, non vi sarebbero state all'interno di un sistema che avesse favorito comportamenti altruistici. Inevitabilmente, chi apparteneva alle classi più basse era spinto a delinquere;

---

concretamente capace di intendere e di volere e comprende pienamente il disvalore sociale delle sue condotte, nonostante il quale decide, liberamente, di agire; 3) la pena, pertanto, non può che essere la necessaria retribuzione del reato compiuto e la comminazione dovrà essere afflittiva, personale, proporzionata, determinata e inderogabile. I più noti esponenti sono Cesare Beccaria, Montesquieu, Filangieri e Voltaire. In materia, si rinvia a F. MANTOVANI, *Diritto penale. Parte Generale,* X ed*.,* Cedam, Milano, 2019, p. 551; G. FORTI, *L'immane concretezza. Metamorfosi del crimine e diritto penale*, Milano, 2000, pp. 198 ss.

[6] Cfr. G. FORTI, *op. cit*., pp. 210 ss.; F. MANTOVANI, *op. cit*., p. 553 ss.

[7] W.A. BONGER, *Criminality and economic conditions*, Little Brown, Michigan, 1916 p. 564.

al contrario, soggetti borghesi delinquevano occasionalmente. Solo marginalmente, poi, Bonger ha ammesso l'esistenza di criminali professionali, quali soggetti nati, cresciuti ed educati al crimine, a prescindere dalla variabile del sistema economico di riferimento.

Siffatta impostazione portava, così, a ritenere che il rimedio alla delinquenza potesse essere ricercato nel miglioramento delle condizioni sociali e nella garanzia di un maggiore benessere economico.

3.1 *La teoria delle associazioni differenziali.*

Gli esiti a cui sono giunti la Scuola Positivista, prima, e i criminologi marxisti, poi, hanno trovato un progressivo dissenso fondato sull'opposta tesi che il comportamento criminale non possa essere spiegato né dalle patologie sociali né, tantomeno, dalle patologie individuali dovendosi, piuttosto, ritenere che "*persone di elevata condizione sociale pongono in essere comportamenti criminali (...) che differiscono da quelli delle classi socioeconomiche inferiori soprattutto nelle procedure amministrative impiegate nei confronti dei rei; e che la differenza nelle procedure applicate non assume rilievo dal punto di vista della cause del delitto*"[8].

Il primo ad ammettere l'esistenza di modelli criminali diversi da quelli sino ad allora proposti è stato Edwin H. Sutherland, criminologo americano, che nella prima metà degli anni '50 del XX secolo – dopo avere vissuto la crisi economica del 1929, causata dal crollo dell'economia americana, e avere osservato i conseguenti effetti depressivi sulle economie dei Paesi europei ad essa collegati – ha denunciato la criminalità dei *White Collar* in piena contrapposizione con la criminalità dei c.d. *worker*. In tal senso, la criminalità dei colletti bianchi è stata dall'autore provocatoriamente proposta come contraltare ai delitti commessi da coloro che indossavano un vestiario meno ricercato che veniva attribuito ai criminali.

L'obiettivo di Sutherland era dimostrare come fenomeni sostanzialmente criminali potessero essere – e, anzi, sono – commessi da soggetti che appartengono ai ceti più elevati della società che, proprio in ragione delle loro caratteristiche sociali, tengono condotte particolarmente offensive degli interessi economici.

Sono state, così, per la prima volta, confutate le teorie criminologiche basate su fattori psicologici e sociali che avevano sino ad allora individuato nella povertà uno dei presupposti della criminalità. In particolare, Sutherland

[8] E.H. SUTHERLAND, G. FORTI (a cura di), *Il crimine dei colletti bianchi. La versione integrale*, Milano, 1987, p. 6-8, traduzione integrale di E.H. SUTHERLAND, *White Collar Crime*, The Dryden Press, New York, 1949.

ha ritenuto che si dovesse negare la validità delle teorie sino ad allora elaborate posto, in primo luogo, che gli studi aventi ad oggetto il rapporto tra *cicli economici* e *tasso di criminalità* – prima non considerati – avevano permesso di accertare l'esistenza di comportamenti criminali indipendenti dalla povertà e da altri fattori ad essa correlati; in secondo luogo, che le analisi statistiche su cui erano state elaborate le precedenti teorie dovevano considerarsi viziate in quanto basate su dati parziali, che non consideravano l'intera casistica delle azioni criminali.

Partendo da dette considerazioni, Sutherland, conscio della rivoluzione criminologica proposta, ha suggerito di adottare una *teoria generale del comportamento criminale*, che si fondi sulla premessa che anche soggetti appartenenti ai più alti ranghi della società delinquono, offendendo particolari categorie di beni giuridici strettamente connesse e coinvolte nelle loro attività occupazionali. Attività che fungono, al contempo, da *occasione*, *motivo* e *causa* delle condotte criminose tenute.

Al riguardo, è apparso sin da subito e in tutta evidenza come i crimini commessi dai colletti bianchi abbiano finalità economiche, con costi particolarmente notevoli a carico della comunità tutta[9].

Se, infatti, i *reati comuni* – quali devono considerarsi, in un'ottica prettamente criminologica e non giuridica, quelli generalmente commessi dai *Worker* ovvero dai colletti bianchi al di fuori delle proprie occupazioni – hanno un basso impatto sulle istituzioni e sull'organizzazione sociale, al contrario, i reati commessi dai soggetti più *rispettabili* della società avranno un "costo finanziario (…) probabilmente molte volte maggiore del costo di quei reati che si ritengono costituire la «questione criminale»[10]", posto che "per quanto ingente sia il danno economico prodotto dai reati dei colletti bianchi, ancora più grave è il danno che essi arrecano ai rapporti sociali: sono abusi dell'altrui fiducia e quindi creano sfiducia, deprimendo la morale pubblica e creando disorganizzazione sociale su larga scala"[11].

Dal punto di vista della genesi del crimine la teoria di Sutherland si fonda, essenzialmente, sul concetto di *associazione differenziale.*

Si è detto che con l'opera *White Collar Crime* è stato compreso, per la prima volta, che gli studi criminologici sull'autore del reato, sino ad allora considerato per le sue caratteristiche biologiche, psicologiche e sociologiche, dovessero muovere dalla capacità del soggetto agente di *apprendere* determinati comportamenti criminali, indipendentemente dalla classe sociale di appartenenza.

[9] *Ivi*, pp. 8-11.
[10] *Ivi,* p. 11.
[11] *Ivi*, pp. 11-12.

Partendo da questo presupposto e dallo studio di documenti biografici e/o autobiografici di uomini di affari a lui noti[12] Sutherland ha, così, formulato la *teoria delle associazioni differenziali*. In simile prospettiva, un soggetto inserito in un determinato gruppo di persone, tra loro strettamente legate, tenderà a condividerne la scala valoriale. In tal senso, se il gruppo si isola dal resto della società di riferimento, divenendo un'*associazione differenziale,* il rischio è che le persone ad essa appartenenti coltivino valori differenti e paralleli rispetto al contesto sociale generale in cui il gruppo si è sviluppato. Pertanto, la forza dell'*associazione differenziale* deve essere ricercata nella sua *capacità di convincimento* dei consociati circa la liceità e positività di un determinato comportamento, in una situazione di isolamento rispetto ad altri individui appartenenti alla società, che guardano a quella stessa condotta in termini sfavorevoli. Tale convinzione spingerà il singolo associato a tenere condotte criminali condivise e liceizzate dal gruppo di riferimento, a cui il singolo decide di aderire, a prescindere dal suo *status* di nascita o dalle sue caratteristiche biologiche e/o psicologiche[13].

L'apprendimento del comportamento criminoso è, quindi, frutto di un preciso *processo differenziale* che porta il soggetto agente ad apprendere, attraverso il contatto interpersonale, sia il comportamento criminale sia le tecniche di realizzazione di un dato crimine, i motivi, gli impulsi, le razionalizzazioni dello stesso e gli atteggiamenti da adottare nella sua commissione[14].

In detto contesto, l'appartenenza al gruppo conferisce al singolo, da un lato, un importante senso di protezione dalla possibilità di essere scoperti; dall'altro lato, fa sì che egli non abbia la percezione dell'illiceità del comportamento tenuto, in quanto frutto della condivisione di una precisa scala

---

[12] Si tenga presente che nel 1948, quando l'Autore, dopo aver dedicato circa un ventennio allo studio delle «*violazioni della legge commesse da persone di elevata condizione socio-economica*», presenta alla casa editrice Dryden Press a New York il manoscritto della sua opera, questo conteneva anche una serie di esempi a supporto della sua tesi comprendenti anche nomi e cognomi di personaggi di spicco dell'epoca o riferimenti che rendevano questi perfettamente riconoscibili; quindi l'editore, per evitare il rischio di esporsi a procedimenti giudiziari per diffamazione e calunnia, pubblica l'opera di Sutherland ma priva dei riferimenti diretti e non senza poche difficoltà da parte dello stesso autore, pressato da più fronti: Sutherland all'epoca era anche direttore del Dipartimento di Sociologia presso l'Università dell'Indiana, in parte finanziata da soggetti e società contro cui Sutherland aveva puntato il dito nel suo manoscritto. L'opera viene pubblicata nella sua interezza e completezza, precedentemente minata dalla mancata pubblicazione del capitolo III del manoscritto originario (*Tre campioni di società*), solo nel 1983, dopo trentatré anni dalla morte di Sutherland e ben trent'anni dopo il decorso della prescrizione dei reati commessi dai colletti bianchi.

[13] *Ivi,* pp. 311 ss.

[14] E.H. SUTHERLAND, *Principles of Criminology*, Philadelphia, 1947, p. 5 ss

valoriale che, da un punto di vista criminologico, *neutralizza* la percezione dell'autore circa la gravità dell'atto commesso e delle conseguenze da esso derivanti, al punto che egli neanche si percepisce quale *criminale*, quanto piuttosto come "mero" *trasgressore della legge*[15].

3.2 *Il privilegio degli affari.*

Un primo fenomeno da attenzionare è il *privilegio degli* affari[16].

La mancata percezione da parte della società della natura criminosa dei comportamenti tenuti dai Colletti Bianchi è favorita dall'influenza politica e dalle capacità economiche di cui dispongono, che permettono loro di evitare che le condotte tenute vengano scoperte e, quindi, punite.

Sin dal principio della sua ricerca Sutherland ha, infatti, rilevato come "Le persone appartenenti a ceti socioeconomici superiori godono di un maggiore potere politico ed economico e sfuggono alla condanna e all'arresto più facilmente degli individui che non dispongono di tale potere. I ricchi possono avvalersi di abili avvocati e comunque influenzare a proprio favore l'amministrazione della giustizia più efficacemente degli appartenenti a classi socioeconomiche inferiori. Gli stessi criminali di professione, grazie al potere politico ed economico di cui dispongono, si sottraggono alla condanna e all'arresto più facilmente dei criminali dilettanti od occasionali, che di tale potere sono pressoché privi"[17]. Concetto, questo, reso nell'espressione "*privilegio degli affari*", che si manifesterebbe tramite due distinti fenomeni tra loro complementari: la *depenalizzazione prasseologica* e *l'influenza dei "colletti bianchi" nella formazione della norma penale*[18].

La *depenalizzazione* è un concetto giuridico consistente nella trasformazione di un illecito penale in un illecito civile o amministrativo: una determina condotta, prima ritenuta penalmente rilevante, al cui accertamento seguiva una *pena*, a fronte di una decisione di politica criminale formalizzata in una legge diviene rilevante dal punto di vista civile o amministrativo, di talché alla sua commissione conseguirà una sanzione civile o amministrativa. È evidente, quindi, che la locuzione *depenalizzazione prasseologica* costituisca un ossimoro, non alludendo a una sequenza di leggi, ma rappresentando, piuttosto, la conseguenza di un comportamento attuato nella prassi.

---

[15]Cfr. P. MARTUCCI, *La criminalità economica. Una guida per capire*, Bari, 2006, pp. 51-52.

[16] Cfr. P. MARTUCCI, *op. cit.*, pp. 15 ss.

[17] E. H. SUTHERLAND, G. FORTI (a cura di), *op. cit.*, p. 7.

[18] G. FORTI, *op.cit.*, pp. 313- 314; E. H. SUTHERLAND, G. FORTI (a cura di), *op. cit.*, pp. 67 ss.

In particolare, Sutherland ha rilevato come nei confronti dei *colletti bianchi* vi sia una sostanziale e prasseologica, appunto, applicazione differenziata della legge, che trova le sue cause in tre diversi fattori: (1) lo *status dell'uomo d'affari*; (2) la *tendenza all'abbandono della sanzione penale*; (3) la *disorganicità della reazione della collettività nei confronti dei crimini commessi dai colletti bianchi*[19].

(1) Quanto allo *status dei colletti bianchi*, è noto che la formazione della legge in generale e in particolare in materia penalistica, dovrebbe – almeno astrattamente – conformarsi alle caratteristiche del soggetto agente come preliminarmente studiate, valutate ed individuate, oltre che dal legislatore, anche dagli operatori giudiziari. Ciò detto, la possibile commissione di reati da parte degli appartenenti al *gruppo* dei colletti bianchi si pone in stretto contrasto con il sentimento, "misto di timore e ammirazione*"*[20], che le Autorità giudiziarie e amministrative nutrono nei confronti di questi soggetti.

In primo luogo, Sutherland ha evidenziato come se da un lato in un sistema – qual è quello americano – caratterizzato dall'elezione degli organi giurisdizionali – "i responsabili della giustizia penale temono di inimicarsi gli uomini di affari perché, tra le molte conseguenze, ciò potrebbe comportare una riduzione dei finanziamenti elettorali necessari a sostenere la loro successiva candidatura"[21]; dall'altro lato, "il legislatore confida nel fatto che, con una lievissima pressione, questi rispettabili gentiluomini si conformeranno alle legge"[22].

In secondo luogo, l'appartenenza degli uomini d'affari allo stesso *gruppo* – *rectius* "l'omogeneità culturale" – dei rappresentanti dei poteri legislativo, esecutivo e giudiziario, non permette di pensare al colletto bianco come ad un criminale.

Siffatto fenomeno è stato efficacemente descritto da Sutherland con la metafora di Daniel Drew, finanziere americano, che guardava alla legge come a una ragnatela: *"*va bene per le mosche e gli insetti più piccoli, per così dire, ma si lascia perforare dai grossi calabroni. Quando le astruserie della legge mi intralciavano, sono sempre riuscito a sbarazzarmene con la massima facilità" [23].

(2) Quanto al fattore relativo all'*abbandono della sanzione penale nei confronti degli uomini d'affari*, la *depenalizzazione prasseologica*, comporterebbe a) pene molto blande, se non addirittura inesistenti; b) la

---

[19] *Ivi,* pp. 67-74.
[20] E. H. SUTHERLAND, *op.cit.*, p. 67.
[21] *Ibidem.*
[22] *Ibidem.*
[23] *Ivi*, p. 68.

sostituzione della pena con l'istituto della *probation* e la previsione di *misure assistenziali*; c) maggiore attenzione al *percorso di recupero del reo* tramite percorsi rieducativi e di assistenza sociale. Mutamenti, questi, dovuti, a una maggiore collaborazione tra ceti sociali, ma anche a una sostanziale perdita di autorevolezza dello Stato, con conseguente "inettitudine dei sistemi penali a produrre una sostanziale riduzione dei tassi di criminalità"[24], nonché alla progressiva sparizione della *punizione* nell'assetto culturale di riferimento[25].

(3) Con il terzo e ultimo fattore considerato l'Autore parrebbe avere riflettuto sulla *percezione e la conseguente reazione della società ai crimini commessi dai gentiluomini d'affari*. In tal senso, ha ritenuto necessario considerare l'importanza dello stretto rapporto tra *diritto* e *morale* in relazione all'ambito analizzato. Invero, i comportamenti criminali dei colletti bianchi costituiscono fenomeni molto complessi, non solo nella loro struttura, ma anche nella percezione che di tali crimini ha la società. D'altra parte, la natura dei beni giuridici coinvolti nelle condotte tenute dai colletti bianchi – diversamente da quanto avviene per i reati commessi dai *Worker* – rende difficilmente percepibile l'offesa da parte della società.

A ben vedere poi, tra la commissione di un reato economico e la percezione dello stesso da parte dei consociati, si frappone – oltre alla capacità dei colletti bianchi di delinquere senza essere scoperti, approfittando dei vuoti normativi offerti dal sistema – la profonda difficoltà dei soggetti comuni di percepire l'offesa subita anche in ragione delle tempistiche dell'accertamento, particolarmente complesso, del fatto.

Si è detto, poi, che è la stessa società a negare la possibilità che un colletto bianco possa delinquere: l'uomo di affari viene considerato come uomo di elevato *status* sociale, rispettoso della legge per definizione.

In siffatto contesto, l'apparenza prevale sulla realtà: non rileva se effettivamente i colletti bianchi violino la legge, ciò che importa è che questi riescano ad «*attenersi alla legge manifestamente e di sottrarvisi nascostamente*»[26].

Siffatto obiettivo, principalmente volto a tutelare la propria rispettabilità, sì che non venga neanche insinuato il dubbio circa la possibile commissione di reati da parte di tali soggetti, viene perseguito con l'impiego di professionisti esperti capaci non solo di eludere le normative vigenti, ma anche di individuare tecniche legislative idonee ad offrire l'impunità delle condotte perpetrate. Così facendo gli uomini d'affari potranno incidere nella *formazione delle norme incriminatrici*, tramite pressioni politiche (*lobbying*), volte a

---

[24] *Ivi,* p. 69.
[25] *Ivi,* pp. 69, 70.
[26] *Ivi,* p. 295.

liceizzare determinati comportamenti ovvero a introdurre norme di *legislazione penale simbolica* con la formulazione di fattispecie incriminatrici inidonee a perseguire concretamente gli interessi proclamati.

Si comprende, pertanto, come tanto più l'associazione differenziale dominante riuscirà a imporre, in via normativa, la propria scala valoriale, tanto più saranno liceizzati i comportamenti astrattamente criminosi dagli stessi tenuti[27]. In tal senso, l'ordinamento giuridico di riferimento conoscerà ipotesi di *immunità sostanziali* causate dall'inceppamento del meccanismo *norma-condotta illecita - sanzione*. Potrà, invero, accadere che la fattispecie penale, proprio in ragione della sua formulazione, non sia in grado di rispondere al bisogno di pena susseguente alla lesione di un bene giuridico tutelato dall'ordinamento, incapace di associare a un determinato comportamento *potenzialmente* illecito a una sanzione, verificandosi, in sostanza, un'ipotesi di ineffettività del sistema penale: il bene giuridico tutelato è offeso, ma la condotta tenuta dal soggetto agente non è punibile.

Al proposito, Sutherland ha evidenziato come dette immunità siano distribuite, in maniera assolutamente differenziale, a favore dei soggetti appartenenti ai ceti più alti della società, a discapito dei ceti inferiori, vittime del pugno di ferro tra il legislatore e l'attività giudiziaria. È questa la conseguenza di un sistema a differenziazione progressiva, che permette ai *colletti bianchi* di sfruttare a loro favore i bivi del sistema penalistico e di rifuggire, così, dalla condotta. Al contrario, i ceti inferiori subiranno tali biforcazioni, andando incontro a un verdetto di colpevolezza spesso caratterizzato dall'inflizione di pene particolarmente severe.

Come noto, il "processo di selezione criminale" in commento è stato visivamente descritto con l'immagine del c.d. *imbuto forato a tre strati*[28]*,* ove la criminalità è rappresentata dal liquido che, solo in parte, si riversa in esso. Il

---

[27] L'elaborazione della *teoria delle associazioni differenziali* trova, a ben vedere, il suo fondamento nel concetto di *disorganizzazione sociale*, elaborato dall' dell'Università di Chicago in cui studiò Sutherland. Tuttavia, Sutherland preferì sposare il concetto di *associazione differenziale* – inteso come il processo che porta un individuo a delinquere – differenziandolo dalla *disorganizzazione sociale* che, invece, può manifestarsi o nelle forme dell'anomia (assenza di regole capaci di orientare il comportamento generale o dell'antinomia tra regole, caratterizzata dalla compresenza, all'interno della società, di due gruppi distinti, con classi valoriali diverse, rispettivamente favorevoli o sfavorevoli alla commissione di reati. Al riguardo, lo stesso Sutherland ha evidenziato come la teoria delle associazioni differenziali e la disorganizzazione sociale, pur differendo tra loro, siano concetti "reciprocamente compatibili e complementari", potendosi applicare sia ai reati commessi dai *workers* sia da quelli commessi dai *white collars*. Cfr. E.H. SUTHERLAND, *op. cit.*, p. 322; G. FORTI, *op. cit.*, pp. 510 ss.

[28] C. E. PALIERO, *Minima non curat praetor. Ipertrofia del diritto penale e decriminalizzazione dei reati bagatellari*, Cedam, 1985, p.236; G. FORTI, *L'immane concretezza*, *op.cit.*, p. 63

liquido che non cade nell'imbuto costituisce la cosiddetta *cifra nera* o *cifra oscura*[29]. L'imbuto è diviso, appunto, in tre strati, ciascuno di essi corrispondente a una delle tre fasi del procedimento penale (indagini preliminari, udienza preliminare, dibattimento). Ogni strato è caratterizzato da fori che permettono ad alcuni reati di uscire dall'alveo della punizione grazie alle biforcazioni del sistema giudiziario: si pensi, a titolo di esempio, a diversi reati procedibili a querela per i quali potrebbe non procedersi mai; piuttosto che ai reati che, pur essendo procedibili d'ufficio, vedono il procedimento penale chiuso con un'archiviazione[30].

3.3 *L'analisi economica del comportamento criminale.*

La seconda chiave di lettura del crimine e del criminale economico è rappresentata dall' analisi economica del comportamento criminale. Trattasi di un segmento di una disciplina più ampia, l'*Economic Analysis of Law* (EAL), che coinvolge tutte le branche dell'ordinamento giuridico e che, da un punto di vista metodologico, si caratterizza per il compimento di un'analisi degli istituti in termini strettamente economici. L'EAL, più precisamente, presuppone che gli strumenti giuridici, vale a dire *le norme,* siano costruiti secondo un'analisi di efficienza rispetto all'obiettivo perseguito.

Orbene, come noto, nella materia penalistica, l'efficienza dell'istituto giuridico opera, innanzitutto, in chiave general -preventiva. Ed invero, la norma, di regola, si rivolge ai consociati al fine, in primo luogo, di prevenirne la violazione.

---

[29] Il riferimento è alla *criminalità nascosta,* intesa come l'insieme di quei reati che sono stati effettivamente commessi, ma non registrati (T. BANDINI ET AL, *Criminologia. Il contributo della ricerca alla conoscenza del crimine e alla reazione sociale*, Vol. I, Giuffrè, Milano, 2003). In particolare, con il termine *cifra nera* si fa riferimento agli illeciti effettivamente commessi, ma non scoperti. Da distinguere dal concetto di *cifra grigia* in cui rientrano, invece, le violazioni commesse e scoperte dalle Autorità giudiziarie, ma non attribuibili ad alcun autore, che rimane ignoto e, quindi, impunito. Nel primo caso, pertanto, il procedimento penale non avrà neanche inizio, mentre nel secondo si concluderà all'esito delle indagini con un'archiviazione, stante l'impossibilità di pervenire alla condanna del soggetto agente. In materia, cfr. E. PALIERO, *Minima non curat praetor*, *op. cit.*, pp. 214 ss.

[30] Al riguardo, è interessate notare come, se in alcuni Paesi l'approccio sanzionatorio nei confronti dei colletti bianchi è mutato, irrigidendosi, in Italia il fenomeno della *depenalizzazione prasseologica*, nella sua duplice manifestazione come sopra richiamata, non accenna a diminuire. Per una riflessione in materia, si rinvia a G. MANNOZZI, *Il crimine dei colletti bianchi: profili definitori e strategie di contrasto attraverso i metodi della giustizia riparativa* in AA.VV., *Europe in crisis: crime, criminal justice, and the way forward. Essays in honour of Nestor Courakis*, C.D. SPINELLIS, N. THEODORAKIS, E. BILLIS, G. PAPADIMITRAKOPOULOS, 2017, pp. 1365-1394, in www.crime-in-crisis.com., reperibile al seguente link.

In tal senso, appare fondamentale, come anticipato, una previa conoscenza degli *input* intenzionali dell'agire umano e, quindi, sul fronte penalistico, delle caratteristiche del *crimine* e del *criminale,* anche con riguardo ai *motivi* che lo inducono a tenere una determina condotta.

Si comprende, pertanto, come il nucleo della *teoria economica del crimine* debba essere individuato nella *deterrenza*, intesa come l'abilità dell'intero apparato penale a *contrastare* (in ottica general preventiva) e *punire* (in ottica special preventiva) la commissione del crimine, in modo da escludere violazioni future e limitare i danni nei confronti della società, intesi anche come i costi che questa deve sostenere per *prevenire* il crimine e per *rispondere* alla sua commissione.

Sebbene il caposcuola dell'Analisi economica del diritto sia spesso individuato in Gary Becker – il cui pensiero sarà analizzato nel prosieguo – in realtà è possibile rinvenire tracce di tale prospettiva già negli scritti di Montesquieu, e Bentham, primi ad ammettere la possibilità di un approccio economico alla materia giuridica[31].

In particolare, già nel 1748 Montesquieu nella sua opera *De l'esprit des lois* ha posto in luce come, negli Stati moderati, un particolare deterrente alla commissione di reati dovesse essere individuato, in primo luogo, nella reputazione del soggetto agente nella società di riferimento, al punto da riflettere sulla possibilità che la tutela della stessa potesse costituire, di per sé, un deterrente alla commissione di reato. In secondo luogo, proprio in un'ottica di analisi economica del diritto, egli ha rilevato l'importanza dell'effettività della legge, sottolineando che così *"*come le leggi inutili indeboliscono le leggi necessarie, quelle che si possono eludere indeboliscono la legislazione. Una legge deve avere il suo effetto, e non bisogna permettere di derogarvi con una convenzione particolare"[32].

In continuità con il pensiero di Montesquieu si pone, un ventennio più tardi, nel 1764 il pensiero di Cesare Beccaria, Autore di *Dei delitti e delle pene*. Egli, invero, nel condividere le conclusioni a cui era giunto Montesquieu rispetto ai rapporti tra deterrenza, deterrenza marginale ed efficacia della legge penale, ha fornito, per la prima volta, a una definizione strettamente economica

---

[31] C. E. PALIERO, *L'economia della pena (un work in progress)*, in *Rivista italiana di diritto e procedura penale*, Fascicolo 4, 2005, pp. 1343, 1344. In materia si rinvia, altresì a E. MONTANI, Economic Crimes*. Diritto penale ed economia: prove di dialogo*, in *Rivista Trimestrale di Diritto Penale dell'Economia*, 2005, pp. 909 ss. nonché E. MONTANI*, La Babele dell'EAL e il diritto penale*, in *Rivista Trimestrale di Diritto Penale dell'Economia*, 2007*,* pp. 45 ss.

[32] C. MONTESQUIEU, *De l'Esprit des lois*, trad. it., *Lo spirito delle leggi*, edizione a cura di R. Derathé e B. Boffito Serra, 2004, Parte VI, Libro XXIX, Capitolo XVI, *Cose da osservare nella composizione delle leggi*, p. 943.

della *pena*, considerata quale costo per il condannato. In tal senso, a Beccaria si deve lo spostamento dell'attenzione dall'aspetto *qualitativo* della pena a quello *quantitativo*, dovendosi individuare il fulcro della sanzione non tanto nell'intenzione di retribuzione, quanto nella sua estensione.

Con tali Autori ha assunto, pertanto, rilevanza il ruolo svolto dal *pensiero razionale* nella commissione di un crimine in particolare economico: Cesare Beccaria per primo, rilevando come *"gli uomini non rischiano che a proporzione del vantaggio che l'esito felice dell'impresa produrrebbe"*[33], compresе come la commissione di un reato economico sia subordinata all'accettazione, da parte del soggetto agente, di un rischio direttamente proporzionale al vantaggio che gli potrebbe derivare dalla condotta tenuta.

Tali concetti sono stati, poi, sviluppati da Jeremy Bentham nella sua opera *Introduzione ai principi della morale e della legislazione*, pubblicata, per la prima volta, nel 1798. Egli, considerato il padre dell'utilitarismo[34], rispetto alla legislazione penale, ha rilevato come un sistema penale possa dirsi efficiente solo quando il legislatore agisca in ottica utilitaristica, dovendosi qualificare alla stregua di *reati* "solo quegli atti che il bene del pubblico richiede siano tali. (…) Il bene del pubblico non può richiedere che venga dichiarato reato un atto che non tenda, in un modo o nell'altro, ad andare a detrimento del pubblico. Nel caso di un tale atto, ogni pena risulta *infondata*"[35].

Successivamente, sulla scia dei principi sino ad allora elaborati il sociologo Gary S. Becker, con la sua opera *L'approccio economico al comportamento umano*, ha per la prima volta osservato come il reato possa rappresentare, oltre che un'offesa nei confronti di beni giuridici della *vittima*, anche un vero e proprio *costo sociale*[36].

Al riguardo, Becker ha evidenziato come il realizzarsi di eventi criminali dipenda, fondamentalmente, dalla qualità dell'investimento che la collettività, rappresentata dai politici, sceglie di fare rispetto alla sicurezza e al mercato del lavoro: è necessario ritenere che l'intero progetto della società, volto alla lotta all'illegalità, abbia (o dovrebbe avere) come unico scopo la dissuasione dei consociati dal delinquere. Per questo motivo, comprendere

---

[33] C. BECCARIA, *Dei Delitti e delle Pene,* a cura di R.FABIETTI, Mursia, Milano, 1973, p.91.

[34] Il pensiero utilitaristico si basa sull'assunto per cui l'uomo, per propria natura, sia portato a pensare, innanzitutto, al proprio interesse. Questa teoria avvicina l'*utilità* alla *morale* sostenendo che la moralità consiste nel comprendere che l'interesse del singolo coincide con l'interesse della collettività. *Cfr.* D. CANTIMORI, voce *"Utilitarismo"*, in *Enciclopedia Italiana*, Istituto della Enciclopedia Italiana Treccani, 1937, in www.treccani.it, reperibile al seguente link.

[35] J. BENTHAM, E. LECALDANO (a cura di), *Introduzione ai princìpi della morale e della legislazione*, Utet, Torino, 1998, p. 307.

[36] G.S. BECKER, *L'approccio economico al comportamento umano,* Bologna, 1998, pp. 141 ss.; C. E. PALIERO, *L'economia della pena, op.cit.*

quale sia il prezzo che un criminale è disposto a pagare permetterà al legislatore di prevedere una politica del diritto di per sé non solo repressiva, ma anche economicamente più vantaggiosa: l'educazione del consociato, l'assoluta convinzione in capo a quest'ultimo di ciò che è giusto e ciò che è sbagliato, di ciò che è illegale e di quel che non lo è, costituisce il miglior strumento di prevenzione esistente.

Becker ha sostenuto che ogni individuo che compia tale ragionamento, riflette su tre diversi livelli di utilità derivanti dall'azione conseguita[37]:

(a) Utilità derivante dalla scelta di non commettere il crimine;
(b) Utilità derivante dalla commissione del crimine e dalla possibilità di non essere scoperto e quindi punito;
(c) Utilità derivante dalla commissione del crimine e dalla possibilità di essere scoperto e quindi punito.

In particolare, Becker ha elaborato la "funzione di mercato dei reati" evidenziando come la scelta da parte di un soggetto circa l'opportunità di commettere o meno un reato e, quindi, il numero di reati commessi all'interno di una società, sia strettamente connessa (a) alla probabilità di essere condannato; (b) alla gravità della pena a cui sarà sottoposto se condannato; (c) ad altri fattori extra-sistemici, a cui dovrà aggiungersi (d) la propensione al rischio, che varia al variare delle qualità del soggetto agente[38].

In quest'ottica, pertanto, è possibile ritenere che la commissione di un reato da parte di un soggetto è subordinata a una previa valutazione volta a verificare che, a parità di risorse impiegate, l'utilità conseguita con la violazione della legge sia superiore a quella che si potrebbe ottenere rispettandola. Il criminale economico compie una analisi costi-benefici, fortemente influenzata dalla aspettativa di punizione, dalla severità della sanzione prevista nonché dalla probabilità che il reato possa essere scoperto e, quindi, punito[39].

È, di tutta evidenza, pertanto, come il *criminale economico* compia scelte criminali fortemente *razionali*.

Tale aspetto, a bene vedere, emerge già dalla lettura di "White Collar Crime".

---

[37] G. CHIERICHIELLO, *Il "criminale razionale", ovvero la teoria microeconomica del crimine. Un saggio introduttivo*, in *Archivio penale,* 2018, 2, pp. 5 ss., in www.archiviopenale.it.
[38]G.S. BECKER, *op. cit.*; P. MARTUCCI, *op. cit.,* pp. 52-53.
[39] *Ibidem.*

Invero, Sutherland, per primo, ha evidenziato come i reati commessi dagli uomini di affari siano quelli in cui il rischio di scoperta è davvero minimo. In primo luogo, in ragione e delle difficoltà che potrebbero incontrare le Autorità nell'individuare e, quindi, nel punire la commissione di un determinato reato, ma anche della sostanziale impassibilità del titolare del bene giuridico offeso, che faticherà anche a rendersi conto dell'offesa subita.

In secondo luogo, i criminali economici, nell'intento di scansare la punizione, commettono reati molto ardui da accertare, vuoi per la complessità dell'azione criminale intrapresa, vuoi per il vuoto normativo in materia, dovuto, spesso volte, anche all'innovatività delle tecniche utilizzate da tali soggetti per delinquere. Elementi, questi, favoriti anche dalla pratica del *fixing*, inteso come la "sistemazione dei procedimenti" nella convinzione "di poter mettere a posto qualsiasi caso, visto che è sempre possibile trovare l'anello debole nella catena di persone da cui dipende la pronuncia di una condanna"[40].

3.3.1 *La razionalità dei criminali economici.*

L'analisi economica del diritto penale ha, poi, permesso di spiegare l'esistenza di *razionalità criminali* tra loro molto diverse.

Invero, Carlo Enrico Paliero, tra i pionieri dell'analisi economica del diritto penale in Italia, ha rilevato come il criminale economico –sebbene sia un soggetto "profondamente razionale e, quindi, orientato da un'attenta analisi costi-benefici sulla base del *know- how* per lui disponibile (…) scarsamente condizionato dagli elementi caratteristici della psiche nella sua *unicità, labilità* e *permeabilità* a stimoli esterni, anche contingenti (come è invece, paradigmaticamente, l'autore del delitto passionale o d'impeto)"[41] al punto da non lasciarsi influenzare se non minimamente, dall'ambiente, in cui agisce – può agire secondo i modelli di comportamenti condivisi dall'associazione differenziale di riferimento.

Punto di partenza, in materia, è rappresentato dall'opera *Economia e Società*, del sociologo tedesco Max Weber – tra i fondatori della sociologia moderna e della scienza politica – pubblicata postuma nel 1922.

È bene evidenziare come, sin dalle prime pagine dell'opera weberiana, emerga come con il termine *agire sociale* non si faccia riferimento ad ogni

[40] E.H. SUTHERLAND, G. FORTI (a cura di), *op. cit.*, pp.300-302.

[41] C.E. PALIERO, *Principio di colpevolezza e reati economici*, in R. BORSARI, L. SAMMICHELI, C. SARRA (a cura di) Homo oeconomicus*: neuroscienze, razionalità decisionale ed elemento soggettivo nei reati economici,* Padova, Padova University Press, p. 22, 2015; D. FONDAROLI, Homo oeconomicus. *La responsabilità in attività d'impresa tra condizionamenti comportamentali e "spinta gentile"*, in C. PIERGALLINI, G. MANNOZZI, C. SOTIS, C. PERINI, M. SCOLETTA, F. CONSULICH (a cura di), *Studi in Onore di Carlo Enrico Paliero,* Milano, 2022, p. 1527.

modalità di azione in quanto “L’agire sociale non si identifica né con un agire uniforme di più individui, né con un agire qualsiasi influenzato dall’atteggiamento di altri”[42].

In detta opera sono stati elaborati quattro diversi paradigmi dell’agire sociale[43]:

(a) Il *paradigma tradizionale*;
(b) Il *paradigma affettivo*;
(c) Il *paradigma assiologico*;
(d) *Il paradigma teleologico*.

Quanto al *paradigma tradizionale*, Weber ha sottolineato come l’agire sociale di un soggetto possa essere influenzato, o addirittura determinato, dalla razionalità, sulla base delle sue sensazioni: in tal caso, il comportamento del soggetto agente all’interno delle società è ispirato alle consuetudini da quest’ultimo conosciute e assimilate. L’individuo, infatti, preferisce non adottare comportamenti innovativi al fine di non dover subire conseguenze inaspettate. La sua razionalità, però, assume caratteri irrazionali: la reazione di un soggetto ad un determinato stimolo è automatico, non ragionato.

Al contrario, il *paradigma affettivo* è assolutamente privo di razionalità e di razionalizzazione: ciò potrebbe comportare, a fronte di uno stimolo esterno, una reazione emotiva assolutamente incontrollabile da parte del soggetto agente.

Il *paradigma assiologico*, invece, vede il soggetto agente comportarsi nel rispetto di principi rispondenti a valori superiori, quindi a canoni religiosi, etici, estetici, del tutto indipendenti da qualsiasi logica.

Vi è, infine, il *paradigma teleologico*, pienamente orientato dall’agente a un fine e, quindi, al soddisfacimento dei propri scopi. Il *paradigma teleologico* non è sovrapponibile a nessuno né a quello affettivo né a quello tradizionale, che non è orientato non allo scopo, bensì al *valore.*

Sicché, mentre il *paradigma tradizionale* analizzato è sempre caratterizzato da una “razionalità irrazionale” quanto più eleva a massimo valore il valore stesso per cui decide di agire; al contrario, il *paradigma teleologico* è razionalità assoluta: la sua scelta non sarà reazione automatica abitudinaria allo stimolo esterno, bensì scelta ragionata, studio dei mezzi necessari al ragionamento degli scopi e delle conseguenze derivanti da questi ultimi.

---

42 M. WEBER, *Economia e Società*, Edizione di Comunità, 1968, p.20.
43 *Ivi*, pp. 21, 22, 23.

Tale distinzione può applicarsi anche al criminale economico. Invero, Carlo Enrico Paliero, proprio partendo dalla teoria weberiana, ha individuato tre diverse tipologie di comportamento criminale: (1) il *comportamento assolutamente anelastico*, (2) il *comportamento relativamente anelastico* e (3) il *comportamento elastico*[44].

(1) Nel primo modello di comportamento considerato, quello *assolutamente anelastico*,

rientra l'agire di tutti quei soggetti disposti a commettere un'azione criminosa indipendentemente da una valutazione costi-benefici. In particolare, dobbiamo distinguere:

(a) i c.d. *criminali affettivi*, quali i soggetti che, nel commettere reato, si lasciano determinare nelle proprie decisioni da una ampia componente affettiva. È questo il classico esempio del delinquente passionale che, colto da un momento di rabbia, sceglie di agire indipendentemente dal rischio di essere scoperto e della gravità della sanzione;

(b) i *criminali tradizionali*, spinti a violare la norma penale da un condizionamento culturale strettamente legato al gruppo cui il soggetto appartiene. Si pensi, in questo senso, alla criminalità organizzata di tipo arcaico, ad esempio alla mafia.

(2) Nell'alveo del *comportamento relativamente anelastico* rientrano, invece, i *criminali assiologici*: questi devono collocarsi nel *paradigma teleologico* definito da Weber. Sono, infatti, assolutamente orientati al *valore* ancor prima che allo *scopo*: la violazione della norma da parte di questi soggetti è dovuta a una profonda adesione e condivisione di valori ideologici. L'esempio classico è rappresentato dal *kamikaze*: egli non si interessa in alcun modo alla risposta sanzionatoria. A queste condizioni risulta evidente come neanche un aumento della sanzione o un rafforzamento nella risposta sanzionatoria possano far desistere l'*assiologico* dal compiere una determinata azione criminale: il legislatore non potrà fare altro che anticipare l'intervento, quindi prevedere reati di pericolo.

(3) Rileva, infine, il *comportamento elastico*, il cui fondamento weberiano è rappresentato dal *paradigma teleologico.* Qui si colloca il *criminale razionale.* Tra questi rientra sicuramente il *criminale economico*, fortemente motivabile su una base costi- benefici: il soggetto che voglia commettere un reato economico, prima di agire, valuterà, si è detto, le variabili che incidono sul *costo del reato*, *il rischio di scoperta* e la *gravità della sanzione*. Quanto ai primi due fattori, è noto che il fenomeno della c.d. *cifra nera* riesca ad abbattere, agli occhi del criminale razione, il costo del reato:

---

[44] C.E. PALIERO "*L'economia della pena", op.cit.*

tanto più sarà basso il rischio di scoperta, tanto minore sarà il costo del reato e maggiore il vantaggio derivante dalla violazione commessa, considerati il bene giuridico violato, da una parte, e l'interesse a cui aspira il criminale. Di talché, se il costo del reato aumenta tanto da sopravanzare il beneficio che questo può raggiungere, determinando la scoperta del reato – cui seguirebbe la perdita reputazionale – il criminale economico desisterà dal violare la norma.

Ed invero, un ruolo fondamentale in materia, si è in parte anticipato, è svolto proprio dalla reputazione di cui l'agente gode nella società di riferimento in ragione dell'elevato *status sociale.* La criminalità economica, in tal senso, risponde a precise dinamiche psicosociali. Tra le peculiarità del fenomeno analizzato, infatti, è necessario considerare, da un lato, la percezione che i colletti bianchi hanno di se stessi e, dall'altro lato, l'importanza dagli stessi riconosciuta all'opinione che la collettività ha di loro. Si è visto, d'altra parte, come sin dagli studi condotti da Sutherland fosse emerso che i criminali economici non si considerano *criminali*, quanto, piuttosto, *trasgressori della legge*. Questi, pur non mancando di riconoscere il disvalore delle condotte tenute, tendono a considerarle delle mere irregolarità formali a fronte di leggi inidoneo allo scopo di tutela[45].

Non vi è dubbio, pertanto, che nella sua analisi costi-benefici egli contempli anche il fattore reputazionale, desistendo dal commettere condotte penalmente rilevanti ogniqualvolta il rischio di scoperta e di perdita della reputazione appaia troppo elevato.

3.4 *Economia e criminalità.*

Questo primo frammento della ricerca conferma, quindi l'importanza, inizialmente solo ipotizzata, della sinergia tra le scienze economiche e le scienze giuridiche per un compiuto studio del fenomeno economico-penalistico rappresentato dalla *criminalità economica*.

Al riguardo, la dottrina[46] ha rilevato la sussistenza di almeno tre diverse relazioni tra *economia* e *criminalità*, evidenziando come la loro compresenza possa assurgere ad indice della natura *economica* del reato e della qualificazione del soggetto agente quale *criminale economico*. Possiamo così sintetizzarle:

(i) la *condotta* posta in essere è *razionale*: l'autore, nella rappresentazione e nella volizione del fatto di reato, è fortemente sensibile alla

[45] E.H. SUTHERLAND, G. FORTI, *op. cit.,* pp. 293- 302.
[46] E.U. SAVONA, *op.cit.,* pp. 1-10.

valutazione *costi-benefici*, in termini sia strettamente economici sia sanzionatori;

(ii) l'*autore del reato* ha un'elevata posizione sociale, che gli permette di agire illegalmente e con abuso della fiducia di terzi nell'ambito di un'attività economica lecita;

(iii) le condotte realizzate dall'autore del reato *ledono il ciclo economico*[47].

3.5 *Dal carrot-stick approach al nudging.*

Le caratteristiche strutturali dei reati economici, tanto oggettive quanto soggettive, inducono ad interrogarsi in ordine all'elemento della colpevolezza, al fine di comprendere in che termini il legislatore possa agire in prospettiva general-preventiva - ancor prima che special preventiva - per ridurre la commissione di un crimine orientato allo scopo.

Ed invero, come osservato da autorevole dottrina, la colpevolezza si fonda su due distinti caposaldi: la *riprovevolezza* dell'azione e la *motivabilità* del soggetto agente[48].

Quanto alla *riprovevolezza*, è noto che un soggetto potrà incorrere nella punizione prevista dal legislatore solo ed esclusivamente quando abbia violato il precetto penale, manifestando un comportamento giuridicamente contrario a quello richiesto dall'ordinamento di riferimento.

La *motivabilità*, invece, guarda alla funzione più strettamente general-preventiva della norma, intesa come la possibilità che il soggetto agisca nel senso richiesto dal legislatore, astenendosi dal compiere o compiendo – rispettivamente nei reati commissivi e nei reati omissivi – l'azione descritta dalla norma incriminatrice.

In tal senso, è stato osservato come affinché vi sia colpevolezza "è necessario che il reo non si sia conformato alla norma nonostante avesse la possibilità di farlo, e che il suo atteggiamento interiore assuma - quindi - una consapevole/determinata posizione di antagonismo rispetto ai valori propugnati dall'ordinamento"[49]. E, d'altra parte, come osservato dalla Corte costituzionale, il principio di colpevolezza "mira a garantire ai consociati libere scelte d'azione, sulla base di una valutazione anticipata ("calcolabilità") delle conseguenze giuridico-penali della condotta; "calcolabilità" che verrebbe meno ove all'agente fossero addossati accadimenti estranei alla sua sfera di consapevole

---

[47] Si rinvia a R. De Luca, C. Macrì-B.Zoli, *Anatomia del Crimine in Italia*, Giuffrè, Milano, 2013, pp. 722 ss.

[48] C.E. Paliero, *Principio di colpevolezza e reati economici, op.cit.,* p.17; R. Bartoli, *Colpevolezza: tra personalismo e prevenzione,* Giappichelli, Torino, 2005.

[49] C.E. Paliero, *Principio di colpevolezza e reati economici, op.cit.,* p.20.

dominio, perché non solo non voluti né concretamente rappresentati, ma neppure
prevedibili ed evitabili”[50].
Ciò detto, proprio le caratteristiche socio-criminologiche dei criminali economici, come sopra descritte, rendono il concetto di *motivabilità* particolarmente rilevante. Ed infatti, la razionalità di tali autori in uno con il proprio *agire fortemente orientato allo scopo* inducono ad interrogarsi sulla necessità e sulla possibilità che la norma penale influenzi *ex se* le scelte dei criminali economici, in termini di astensione dalla commissione del reato.

In questa direzione il legislatore ha nel passato più recente adottato, almeno astrattamente, il c.d. *carrot-stick approach*, cercando di orientare, il comportamento razionale del criminale economico, andando ad incidere, più che sul fattore di appartenenza a una associazione differenziale, sulla sua analisi costi-benefici. In tal senso, a misure fortemente punitive, riservate a chi viola il precetto, si contrappone un’importante componente premiale, riconosciuta a chi si astiene dal porre in essere comportamenti lesivi degli interessi tutelati dall’ordinamento[51].

Tale scelta si colloca in un più ampio contesto che ha visto le strategie di politica pubblica svilupparsi in ragione delle peculiarità dell'*homo oeconomicus*, ritenuto – si è detto – un soggetto fortemente razionale, orientato al profitto in ogni sua azione. In tal senso, partendo dal presupposto citato, la normativa statale, anche in ambito penalistico, si è caratterizzata per la sua intrinseca razionalità. In particolare, è stato evidenziato come la regolamentazione tradizionale potesse essere suddivisa in tre tipologie: (i) messa a disposizione di informazioni e di persuasione razionale; (ii) incentivi negativi e positivi; (iii) regolamentazione legale[52].

Ciò nonostante, studi più recenti di economia comportamentale hanno sostenuto una crisi della razionalità umana come conosciuta sino ad oggi, sostanzialmente causata da errori cognitivi causati da *bias* e sollecitazioni esterne che rendono fallace il giudizio umano, mostrando l'agente in tutta la sua umanità con conseguente erosione del mito dell'*homo oeconomicus*, quale

---

[50] Corte cost., sentenza n. 332 del 24 luglio 2007.

[51] In materia, è particolarmente interessante lo studio condotto da G. ANDRIGHETTO, D. VILLATORO, *Beyond the Carrot and Stick Approach to Enforcement: An Agent-Based Model*, *in European Perspective on Cognitive Science*, New Bulgarian University Press, 2011.

[52] M. BARBERA, *Il nudge e le condizioni per la sua applicazione nello Stato liberale*, in AA.VV. (a cura di), *Dalle regole ai comportamenti. Conversazioini in tema di amministrazione e persuasione,* Mimesis, 2022, pp. 19 ss.

soggetto razionale, orientato al profitto e alla massimizzazione del proprio benessere personale[53].

È, invero, necessario considerare che il processo decisionale di ciascuno, ancorché fortemente razionale, è costellato da pregiudizi cognitivi e irrazionali che influenzano la scelta dell'agente e che, in qualche misura, possono essere predetti dalle scienze sociali.

Siffatti mutamenti riguardanti il processo decisionale sono oggetto di attenta disamina da parte tanto di studi di economia comportamentale quanto di psicologica comportamentale e cognitiva. L'obiettivo consiste nell'individuare precisi strumenti ermeneutici idonei ad apportare, in un'ottica predittiva e fondata sulla consapevolezza della ripetibilità dei comportamenti irrazionali, un'importante modifica nelle tecniche preventive attuate dal legislatore, sì da orientare i comportamenti della collettività. Tale impostazione può interessare, in tutta evidenza, anche la commissione dei reati economici.

D'altra parte, la continua evoluzione della criminalità economica pare confermare, almeno parzialmente, il fallimento del *carrot-stick approach*, incentrato, principalmente, sulla minaccia della pena (tendenzialmente detentiva) e sull'utilizzo di misure ablatorie reali utili, quantomeno in astratto, ad azzerare l'eventuale profitto derivante dalla commissione del reato.

Appare, pertanto, interessante indagare la possibilità di orientare il comportamento umano attuando un processo di sensibilizzazione a valore etici tramite tecniche di *nudging.*

Il *nudge* o *spinta gentile* è stato definito da Sustein come "ogni aspetto nell'architettura delle decisioni che modifica il comportamento delle persone in modo prevedibile senza vietare loro alcuna scelta e senza cambiare in modo significativo i loro incentivi economici. Per valere come *nudge* l'ingerenza deve potere essere evitata facilmente e a basso costo"[54]

Obiettivo principale della *spinta gentile*, pertanto, consiste nel tentativo di migliorare le condizioni della collettività orientandone le decisioni senza, tuttavia, incidere sulla libertà di scelta. In tal senso, Thaler e Sunstein hanno classificato detto approccio quale *paternalismo libertario*, volto a influenzare il comportamento dei destinatari, in senso debole e libertario, sì da non incidere sulle scelte con obblighi e previsioni legali; si contrappone, pertanto, al *paternalismo forte* che, al contrario, è incentrato su coartazioni e imperativi che

[53] Sul ruolo del *bias* nella società con riguardo ai crimini commessi dai colletti bianchi, v. S. P. SHAPIRO, *Collaring the Crime, not the Criminal: Reconsidering the Concept of White-Collar Crime*, in *American Sociological Review,* Vol. 55, n. 3, 1990, p. 346-365, in www.jstor.org, reperibile al seguente link.

[54] R. THALER, C. SUSTEIN, Nudge. *La spinta gentile. La nuova strategia per migliorare le nostre decisioni sul lavoro, salute, felicità*, trad. it., Milano, 2009.

non lasciano libertà di scelta alcuna al soggetto che, al contrario, agirebbe al solo fine di evitare la sanzione"[55]

Ancorché l'applicazione di simile tecnica di regolamentazione, ad oggi oggetto di verifica sperimentale, sia fortemente discussa[56], soprattutto con riferimento alle criticità che deriverebbero in punto di tutela delle libertà individuali e, più precisamente, di libero arbitrio appare interessante riflettere sulla possibilità di considerare l'utilizzo della *spinta gentile* in ambito penalistico, con particolare riferimento ai reati commessi dai colletti bianchi.

La dottrina intervenuta in materia ha evidenziato come la spinta gentile non possa costituire uno strumento alternativo alla norma dovendosi, piuttosto, immaginare quale ipotesi di complementarità al precetto e alla sanzione[57].
Siffatto approccio sembra ben applicabile ai colletti bianchi in ragione delle loro caratteristiche criminologiche e sociologiche, quali soggetti appartenenti a classi sociali fortemente istruite, capaci di comprendere le caratteristiche e i limiti della realtà di riferimento.
È stato, infatti, osservato come con riferimento ai reati economici la natura razionale dell'agire criminale potrebbe indurre a "una sorta di consacrazione del *dolus in re ipsa* e della de-psicologizzazione dell'illecito, con conseguente attribuzione dell'imputazione oggettiva"[58]

D'altra parte, è stato rilevato come lo studio circa l'applicabilità di tecniche di *nudging* potrebbe portare a risultati positivi per allontanare effetti negativi causati da determinati tratti della personalità "che possono lambire i confini della psicopatia, con prevedibile incidenza sui parametri di esclusione totale o parziale della capacità di intendere e di volere". In tal senso, è stata ipotizzata la possibilità di integrare, a fini preventivi, proprio tramite l'attuazione di strumenti di *nudging*, programmi di *compliance,* che possano

---

[55] R. THALER, C. SUSTEIN, *Libertarian paternalism is not an oxymoron*, in *The University of Chicago Review,* vol. 70, n. 4, 2003, pp. 1159-1202.
[56] A. GRAGNANI, Nudging *e libertà costituzionale,* in www.dirittifondamentali.it, 2021; S. CASSESE, *Exploring the legitimacy of Nudging,* in AA.VV. (a cura di), *Choice Architecture in Democracies – Exploring the legitimacy of Nudging*, Nomos, Baden- Baden, 2016, pp. 242 ss.
[57] G. TUZET, Nudge: *la struttura normativa*, in *Gior.it. psicologia,* 2, 2020, p.518; D. FONDAROLI, *Metafore:* l'homo oeconomicus *e la "spinta gentile" nella prospettiva del sistema punitivo*, in *Criminalia. Annuario di scienze penalistiche*, 2022, pp. 243 ss., in www.discrimen.it, reperibile al seguente link.
[58] R. BORSARI – L. SAMMICHELI (a cura di) Homo oeconomicus*: neuroscienze, razionalità decisionale ed elemento soggettivo nei reati economici,* Padova, Padova University Press, 2015, pp. 9 ss.

portare al superamento di strutture basate unicamente sull' affidamento fiduciario a soggetti con compiti decisori”[59].

4. *Il White Collar Crime nel cyberspazio.*

A partire dalla rivoluzione di Sutherland, sono state molteplici le innovazioni che hanno riguardato l’evoluzione del crimine e del criminale economico, fortemente influenzata, tra gli altri fattori, anche dalla continua evoluzione tecnologica e, in particolare, dell’informatica.

Da un punto di vista prettamente criminologico, ancor prima che giuridico, paiono potersi ricomprendere nel novero dei colletti bianchi anche i soggetti che, forti delle proprie competenze informatiche, riescano a commettere reati economici, senza essere scoperti e, quindi, incorrere sanzione.

In tal senso, l’evoluzione del *crimine economico* è proceduta con quella del *criminale economico* senza che, ancora una volta, il legislatore sia riuscito a captare e, quindi, ad anticipare da un punto di vista formale condotte che hanno progressivamente – e sottotraccia – preso piede sul piano sostanziale.

Ancora una volta, quindi, la criminalità economica ha rappresentato il volano del crimine, complice anche la velocità con cui si è evoluto l’utilizzo della rete internet e delle discipline informatiche. Quest’ultimo, nato come strumento militare, si è diffuso a macchia d’olio in ambito lavorativo, scolastico, sino ad essere, oggi, a completa disposizione dei privati, dando così luogo al c.d. *cyberspace*[60].

Parallelamente, da un punto di vista più strettamente tecnologico, si è assistito alla nascita dei *device*, che hanno permesso un più semplice e fruibile accesso al *web* tramite l’utilizzo di *personal computer* e di telefoni cellulari, ben presto divenuti *smartphone*.

Siffatta rivoluzione ha inevitabilmente coinvolto tutti gli ambiti di produzione che si sono adeguati all’innovazione, sicché si sono evolute le aziende, le pubbliche amministrazioni, ma anche le discipline più classiche dell’economia e la finanza[61]. Tutto ha iniziato a viaggiare, in maniera interconnessa, a velocità altissime, non dando mondo al legislatore di poter intervenire tempestivamente nella regolazione del fenomeno, esploso all’improvviso.

---

[59] M. BERTOLINO, Corporate, *criminalità*, compliance *d’impresa e personalità del* white collar offender, in *Archivio penale,* 3, 2019, p.10, in www.archiviopenale.it, D. FONDAROLI, Homo oeconomicus, *op. cit.*, p. 1533.

[60] In materia, L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale, una visione di insieme*, in AA.VV. (a cura di) *Cybercrime,* II Edizione, Utet, Torino, 2023, p. 36.

[61] F. GARGIUOLI, *Cybercrime*, Aracne Editrice, Roma, 2017, p.8.

Il dato normativo, tuttavia, è rimasto a lungo immutato e, ancora oggi, fatica a rispondere alle esigenze manifestatasi. In detto contesto, ben presto alcuni soggetti hanno iniziato a comprendere le potenzialità del neonato strumento tecnologico e le alterazioni che sarebbero potute derivare, da un lato, dallo scorretto, ma legale – perché non vietato, non tipizzato – utilizzo dello stesso; dall'altro lato, dalle difficoltà delle Autorità giudiziarie di far rispettare nel mondo *virtuale* quelle norme nate per la tutela del mondo *reale*.

In tal senso, a fronte di un'unica fattispecie incriminatrice orientata al crimine commesso nel mondo *reale* si è assistito a una duplicazione del *locus commissi delicti*, divenuto anche *virtuale*, con conseguente "liceizzazione" di condotte – almeno astrattamente – criminali.

Si è, così, venuto a creare un *vacuum* di tutela dei beni giuridici offesi in uno spazio sino ad allora rimasto inesplorato: la norma non riesce a rispondere alla condotta criminosa virtualmente tenuta e la condotta, da illecita, diviene "lecita", sicché il principio di legalità, da baluardo nelle mani del cittadino e del giudice, diviene arma nelle mani dei criminali economici, limite per le Autorità giudiziarie.

Tale fenomeno è stato progressivamente qualificato alla stregua di *cybercrime*, in quanto caratterizzato dall'utilizzo criminale della tecnologia informatica *lato sensu* intesa, ricomprendendo tanto i reati che offendono i neonati beni informatici quanto quelli perfezionatisi con l'utilizzo degli stessi.

In particolare, i *reati cibernetici* (*cybercrime*) rappresentano l'evoluzione degli originari *reati informatici* (*computer crime*), la cui commissione era circoscritta a reti telematiche chiuse, in singoli sistemi o in singoli settori. Rientrano nella categoria dei *cybercrime* tutti i reati che possono essere commessi nel *cyberspace.*

Distinguiamo i reati cibernetici "in senso stretto" dai reati cibernetici "in senso ampio".

Quando la formulazione delle fattispecie incriminatrice prevede la rete quale elemento essenziale o circostanziale del reato, ci troveremo innanzi a *cybercrime* "in senso stretto": in tal senso, vi rientrano i reati che, commessi dai *cybercriminal*, ricadono direttamente su beni e strumenti informatici citati nella norma incriminatrice. È bene evidenziare come tale categoria sia sovrapponibile a quella dei "reati informatici in senso stretto", quali condotte necessariamente commesse in rete[62]; al contrario, saranno qualificabili alla stregua di reati cibernetici "in senso ampio" le condotte criminose che sfruttano lo strumento informatico come mezzo per la commissione del reato, che

[62] Non può, tuttavia, affermarsi il contrario: non tutti i reati informatici sono *cybercrime,* potendo, quantomeno astrattamente, l'elemento che richiama le tecnologie informatiche non richiedere espressamente anche la commissione in rete.

avrebbe potuto essere perfezionato anche con modalità tradizionali, senza che, tuttavia, le stesse siano necessariamente sussumibili nella fattispecie incriminatrice tradizionalmente applicata[63].

Ulteriore caratteristica del *cybercrime* deve poi essere rintracciata nel moltiplicarsi dei rapporti tra soggetti nella rete, con un progressivo aumento della messa in pericolo per i beni giuridici tutelati, il cui catalogo non si è particolarmente espanso, assistendosi, piuttosto, a un ampliamento delle *modalità* di offesa di beni giuridici tradizionali.

La risposta del legislatore al fenomeno in parola, oltre che tardiva, non è stata sufficientemente adeguata: partendo dal presupposto che il *cybercrime* fosse dovuto a un riversamento nella rete delle patologie sociali presenti nel mondo reale, il legislatore ha, a lungo, ritenuto che la lotta a tale tipologia di crimine potesse essere compiuta tramite un mero *adeguamento* delle fattispecie incriminatrici vigenti, ampliando la loro applicazione anche alle condotte tenute con modalità cibernetiche. Appare evidente, tuttavia, come, in un ordinamento giuridico imperniato sul principio di legalità, un siffatto allentamento delle maglie si pone in possibile conflitto con i collegati canoni di tassatività, determinatezza e precisione.

Il risultato è una legislazione incompleta, sviluppatasi in modo frammentario, che richiama la necessità di definire una normativa giuridica generale, in cui siano definiti nuovi criteri, precise regole di imputazione della responsabilità penale nonché i presupposti affinché possa essere irrogata una sanzione anche per fatti commessi nel *cyberspace.*

Questo da un punto di vista oggettivo[64].

Da un punto di vista soggettivo notiamo, poi, che i *cybercriminal* riescono a perpetrare le proprie condotte criminose servendosi di particolari conoscenze tecnologiche ed informatiche che permettono loro di delinquere nel mondo *virtuale* senza il rischio di essere scoperti.

Diversi studi hanno analizzato le tradizionali teorie criminologiche per spiegare le attitudini dei criminali informatici, che possono essere pacificamente spiegate con la teoria delle associazioni differenziali di Edwin H. Sutherland.

---

[63] M. FUMO, *La condotta nei reati informatici,* in *Archivio penale*, 3, 2013, pp. 775 ss., in www.archiviopenale.it. In materia, L. PICOTTI, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme*, *op.cit*., p. 79.

[64] Per un approfondimento sull'analisi dei tratti comune dei crimini commessi dai colletti bianchi si rinvia a S.P. GREEN, *Lying, Cheating and Stealing. A moral theory of White-Collar Crime*, Oxford, Oxford University Press, 2006; H. CROALL, *Understanding white collar crime,* Open University Press, Buckingham-Philadelphia, 2001.

Al riguardo, Pierpaolo Martucci ha individuato nei «*fattori psicosociali*»[65] il comune denominatore di tutti i reati economici, dagli arbori ad oggi. Innanzitutto, si è già vista e ripetuta più volte, l'importanza che assumono nell'agire del "colletto bianco" la percezione che lo stesso ha della violazione compiuta, da un lato, e la sensazione percepita dalla collettività, dall'altro. I criminali economici si considerano trasgressori e non criminali: tengono molto a questa distinzione e fanno di tutto affinché anche la collettività non consideri il loro atteggiamento criminale un fattore stigmatizzante. Il criminale economico vuole tutto: profitto illecito, reputazione intatta e potere.

I mezzi utilizzati sono molteplici e gli strumenti e le tecniche di cui si serve nella corsa al profitto sono in continua evoluzione. La caratteristica fondamentale risiede nella capacità di trasformare le proprie competenze in armi efficienti e spesso – almeno inizialmente – imbattibili per ottenere, in maniera completamente razionale, il profitto puntato all'inizio della scommessa. Per il criminale economico, sia che esso agisca nel mondo *reale* che nel mondo *virtuale,* la condizione ottimale in cui muoversi, dal punto di vista giuridico, è il vuoto ormativo, la lacuna, l'antinomia.

Inoltre, se è vero che i "colletti bianchi" sono soggetti che riescono a delinquere grazie alla propria posizione sociale, alle proprie conoscenze personali, alle proprie occupazioni e alle proprie competenze è altrettanto vero che i *cybercriminal,* proprio come i *White Collar,* sono soggetti competenti, capaci, che conoscono approfonditamente il mondo virtuale, le sue falle e i vuoti giuridici normativi che è bene sfruttare per poter trarre un profitto senza il rischio di scoperta. E non pare un caso, infatti, che la maggior parte dei reati che possono essere commessi dai criminali informatici rientrino nell'alveo dei reati economici o comunque di quelle fattispecie incriminatrici immaginate dai legislatori per tutelare il bene giuridico *patrimonio*.

È, pertanto, possibile affermare la piena compatibilità tra la teoria criminologica di Sutherland e la figura del *cybercriminal*: non solo *il privilegio degli affari*, ma anche e soprattutto, si è detto, *le associazioni differenziali*. A questo proposito giova rilevare che vi sarebbe un'unica differenza: se per i "colletti bianchi" di Sutherland la sensazione di protezione dal rischio di scoperta e la conseguente accettazione del pericolo derivante dalla commissione del crimine commesso sono dovuti alla condivisione con altri soggetti di una scala valoriale alterata rispetto a quella del contesto sociale di riferimento, quindi alla certezza che nessuno tradirà mai l'associazione differenziale, il *cybercriminal* si sente protetto dall'anonimato che la rete – alterata anch'essa – gli fornisce.

---

[65] P. MARTUCCI, *op.cit.* p.51.

CAPITOLO II

DALLA DECENTRALIZZAZIONE DELLA MONETA ALLO SFRUTTAMENTO DELLE CRIPTOVALUTE COME STRUMENTO CRIMINALE: ELEMENTI INFORMATICI ED ECONOMICI

1. *Premessa.*

Prima di addentrarci nel vivo dello studio condotto è necessaria una breve ambientazione della ricerca.

Nel contesto socioculturale attuale – sempre più pervaso dall'innovazione informatica e tecnologica – un ruolo predominante è stato assunto negli ultimi anni dalla *blockchain* applicata alle criptovalute. Detta tecnologia, seppur nata come strumento positivo, funzionale alla pubblicità e alla trasparenza delle transazioni, viene sfruttata dai *cybercriminal*, criminali economici del XXI secolo, con effetti disfunzionali su beni giuridici primari e per l'economia.

Ed invero, detti soggetti, forti dei vuoti normativi in materia, da un lato, sfruttando le caratteristiche proprie della *blockchain* – quali la decentralizzazione, lo pseudoanonimato e/o anonimato e l'irreversibilità delle transazioni– e, dall'altro lato, servendosi di specifici *software* di *mixing* e *tumbling*, hanno dato vita ad un'ampia casistica di reati, tra cui – come sarà meglio specificato nel prosieguo – le fattispecie di truffa, riciclaggio, finanziamento del terrorismo, manipolazione del mercato ed *insider trading* basati sull'impiego di criptovalute.

Si è detto come caratteristica principale della ricerca condotta è da individuarsi nella sua intrinseca e necessaria interdisciplinarità, fondamentale per comprendere cause, modalità e conseguenze dell'utilizzo delle criptovalute come strumento criminale.

Da un lato, si tratta di una materia che diverrebbe incomprensibile in assenza di poche, ma fondamentali, nozioni informatiche, capaci di spiegare le criticità del fenomeno trattato.

Dall'altro lato, ancora una volta, si renderà necessario richiamare concetti propri delle scienze economiche fondamentali, innanzitutto, nel procedimento di qualificazione giuridica delle criptovalute.

2. *La decentralizzazione della moneta e la nascita delle criptovalute.*

Sebbene si discuta delle criptovalute quale strumento criminale, queste trovano, in realtà le proprie origini nell'America degli anni '80 del '900, quando il movimento *Cypherpunks* ha immaginato per la prima volta una moneta che potesse essere decentralizzata, quindi non sottoposta al controllo delle autorità – nazionali o sovranazionali – e pseudoanonima, potendo così garantire l'anonimato a chi la utilizzasse e al contempo la possibilità di controllo quando vi fossero operazioni sospette[66].

Obiettivo principale di tale movimento, definito anche *cripto anarchico*, era – ed è tuttora – la tutela della *privacy* quale bene comune. In tal senso, il movimento *cypherpunk*, conscio del cambiamento politico e sociale

---

[66] Per completezza, è bene osservare come studi minoritari riconducano la nascita della criptovaluta, quale moneta decentralizzata, alla Scuola Austriaca. In particolare, secondo la teoria c.d. austriaca, dalle origini dei suoi principali esponenti, Ludwig von Mises e Friedrich Hayek, i cicli economici sono l'inevitabile conseguenza degli interventi monetari sul mercato, per cui un'espansione eccessiva del credito bancario sarebbe causata da tassi di interesse bassi fissati da una banca centrale. Alla lunga questo meccanismo sarebbe alla base della recessione, quindi del fallimento di imprese e della conseguente povertà del popolo. Per questo motivo gli Austriaci pensano che il sistema bancario debba essere abolito e che si debba passare a un denaro decentralizzato il cui valore non può essere manipolato da alcuna autorità. Tale teoria in parte coincide con la concezione dei *Cypherpunk*. *Cfr.* N. LECIS, *La teoria austriaca del ciclo economico*, 2018, in www.financecue.it, reperibile al seguente link.

proposto, da sempre sostiene l'utilizzo della crittografia[67] quale strumento idoneo e necessario per la tutela della *riservatezza.* È proprio dai soggetti aderenti a questo movimento che sono sorte tutte le idee che hanno portato al raggiungimento dell'obiettivo primario dei *cypherpunk*: una valuta digitale decentralizzata, pseudoanonima e quantitativamente limitata.

La prima manifestazione della filosofia *cypherpunk* deve essere ricercata nell'opera di David Chaum, *Blind Signatures for Untreaceable Payments*, in cui, per la prima volta, è stato introdotto il concetto delle c.d. "firme cieche", quali firme digitali apposte su un messaggio prima della apertura e lettura da parte del destinatario[68]. Solo successivamente, nel 1985, sulla scia dell'opera *1984* di George Orwell, David Chaum ha pubblicato un ulteriore lavoro dal titolo *Security without Identification: Transaction Systems to Make Big Brother Obsolete,* considerata la prima reale manifestazione dell'esistenza del movimento criptoanarchico.

È solo negli anni successivi, tuttavia, che Chaum elabora il concetto di *chiave pubblica* e *chiave privata* ed è il 1989 quando le idee dei *cypherpunk* trovano concretizzazione nella DigiCash inc., società fondata dallo stesso Chaum, il cui scopo era proporre un nuovo sistema elettronico di pagamenti. In tale contesto, per la prima volta, la crittografia viene applicata al concetto di moneta, sì da garantire, tramite un sistema di emissione centralizzato, l'anonimato di tutte le transazioni. In detta fase, infatti, alle poche banche aderenti all'iniziativa era riconosciuto un ruolo di certificazione e controllo crittografico della moneta, utile a garantire l'anonimato degli utenti a fronte di transazioni sicure. Detto progetto, tuttavia, fallirà a causa del rifiuto delle banche di accettare una simile innovazione.

È il 1993 quando Eric Huges, matematico dell'Università della California di Berkley, pubblica in rete il *Cypherpunk's Manifesto*[69], documento con cui il movimento criptoanarchico manifesta, appunto, la volontà di diffondere sistemi di crittografia a chiave pubblica, firma elettronica e denaro digitale, quali strumenti idonei a rendere anonimi i propri utenti, tutelandone la *privacy*[70].

---

[67] La crittografia è una branca della matematica utile a proteggere informazioni che non possono essere rese pubbliche. La crittografia rende l'informazione leggibile unicamente al destinatario che sia a conoscenza degli strumenti utili a renderla intellegibile. Cfr. U. BUONORA, S. CAPACCIOLI (a cura di), *Spiegazioni dei fondamentali,* in *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021, pp. 55 ss.
[68] D. CHAUM, et. alt, *Advances in Cryptology Proceedings of Crypto 82,* Springer US, University of California, Santa Barbara, 1983.
[69]E. HUGES, *A Cypherpunk's Manifesto,* 1993, in www.activism.net, reperibile al seguente link.
[70] Testualmente, i *cypherpunk* si descrivevano nei termini che seguono: "*We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy*

Siffatta filosofia è stata, sin da subito, concretamente attuata dai suoi sostenitori che, anche tra loro, comunicavano attraverso delle *mailing lists* crittografate, pertanto ritenute sicure[71].

Risale al 1997 la creazione da parte di Adam Back di *Hashcash*, un *software* concepito come l'evoluzione di DigiCash, da cui differiva in punto di utilizzo, non richiedendo che gli utilizzatori detenessero un proprio account su *E-Cash,* così aumentando la decentralizzazione dello strumento.

Solo successivamente, tuttavia, nel 1998 si avranno due sistemi di pagamento completamente decentralizzati, autonomamente sviluppati dal programmatore Wei Dai e dal crittografo Nick Szabo.

A Wei Dai si deve la prima valuta virtuale decentralizzata, *B-Money*, le cui caratteristiche sono state successivamente recepite da *Bitcoin*[72]. In particolare, il sistema in parola permetteva a chiunque di *creare* denaro mediante la risoluzione di un algoritmo, che richiedeva una determinata potenza di calcolo. Le transazioni, poi, ancorché servendosi di firme digitali, avvenivano tramite un *network* che permetteva agli utenti di registrarsi con pseudonimi o nomi utente capaci di garantirne l'anonimato[73].

Nello stesso periodo Nick Szabo, crittografo e studente di legge, idea *bit-gold*, valuta virtuale considerata antecedente dell'architettura Bitcoin: proprio come *B-Money* – e come vedremo il Bitcoin – anche il *bit-gold* si basava su calcoli algoritmici effettuati dai processori. In particolare, Szabo descriveva la sua moneta nei seguenti termini: «*is based on computing a string of bits from a string of challenge bits, using functions called variously "client puzzle function", "proof of work function" or "secure benchmark function". The resulting string of bits is the proof of work*»[74]. Più precisamente, i calcolatori ricercavano la *challenge string*, una stringa di *bit,* tramite un processo definito *proof of work*. La moneta *bit-gold* veniva generata tramite la risoluzione di

---

with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money".

[71] G. SABBATINI, *I Cypherpunks da David Chaum a Satoshi Nakamoto*, 2017, in www.nextgenerationcurrency.com, reperibile al seguente link.

[72] N.M. KAPLANOV, *Nerd Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation,* in *Loyola Consumer Law Review*, vol. 25, 2012, pp. 114-115

[73] Vedi WEI DAI, *B- Money,* reperibile al seguente link. Per una traduzione italiano, cfr. S. CAPACCIOLI (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021, pp. 41 ss.

[74] «è basata sull'elaborazione di una stringa di *bit* a partire da una stringa di caratteri, utilizzando funzioni chiamate in vari modi *funzione di puzzle del cliente*, *funzione di prova del lavoro* o *funzione di riferimento sicuro*. La stringa risultante di bit è la *proof of work. Cfr.* N. SZABO, *Money, blockchains, and social scalability*, in https://unenumerated.blogspot.com, reperibile al seguente link. Per una traduzione italiano, cfr. S. CAPACCIOLI (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021, p. 44.

calcoli algoritmici. Di talché, la stringa poteva essere ricercata da un solo utente che corrispondeva a colui che per primo, in ordine cronologico, riusciva a trovarla e, quindi, era autorizzato a spenderla. Solo una volta terminata la ricerca della stringa precedente, l'utente poteva passare alla successiva[75].

Più recentemente, nel 2004, Hal Finney, esperto di crittografia e convinto *cypherpunk*, deceduto nel 2014, ha introdotto il concetto di *Reusable Proofs of Work,* vale a dire un sistema di pagamento centralizzato la cui moneta si basa su un protocollo, denominato *proof-of-work* (POW), volto a verificare, tramite una prova crittografica, le transazioni attuate con tale tecnologia. Tale sistema utilizzava il protocollo di *Hashcash* ideato nel 1997 da Adam Back. È proprio di questa tecnologia che si serve oggi il Bitcoin per verificare le transazioni che avvengono tra utenti.

È l'agosto del 2008 quando viene registrato il dominio *Bitcoin.org* ove, pochi mesi dopo, il 31 ottobre 2008, viene pubblicato da Satoshi Nakamoto, pseudonimo dell'ancora sconosciuto creatore del Bitcoin, un articolo intitolato *Bitcoin: A Peer-to-Peer Electronic Cash System*[76].

Con questo scritto viene presentato, per la prima volta, il Bitcoin, quale sistema di scambio di valore attraverso la rete, completamente decentralizzato.

È interessante notare come la presentazione al mondo di Bitcoin sia pressocché concomitante con la bancarotta della banca di investimento più importante degli Stati Uniti d'America, la *Lehman Brothers* e la conseguente crisi finanziaria del 2008. In tal senso, il *paper* pubblicato da Satoshi Nakamoto pare potersi leggere quale segno della rafforzata volontà del movimento *Cypherpunk* di portare a compimento la decentralizzazione della moneta auspicata sin dagli arbori. Una moneta non solo decentralizzata, ma anche priva di un valore intrinseco, se non quello derivante dalla domanda e dalla offerta, quindi, essenzialmente da *«what people are willing to trade for them»*[77]. Nakamoto, infatti, nel suo *paper* espone nel dettaglio la necessità di un sistema di pagamento elettronico «*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*»[78]; un sistema sottratto all'inflazione

[75] *Ibidem.*

[76] Per una traduzione italiano, cfr. S. CAPACCIOLI (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021, pp. 45 ss.

[77] «Quanto le persone sono disposte ad investire su di essa», *cfr.* N.M. KAPLANOV, *op.cit.*, pp. 115.

[78] «Basato su prove crittografiche anziché, sulla fiducia, consentendo a due parti volontari di negoziare direttamente tra loro senza la necessità di una terza parte fidata», *Cfr.* S. NAKAMOTO, *Bitcoin: A Peer-to- Peer Electronic Cash System*, in www.bitcoin.org, p.1, reperibile al seguente link.

e alla crisi finanziaria non solo in ragione della sua autonomia, ma anche del numero quantitativamente limitato – come vedremo nel prosieguo – di Bitcoin.

Se tutte le innovazioni tecnologiche precedenti, a partire da *E-cash*, passando da *bit-gold* e *B-Money,* non avevano previsto la totale decentralizzazione, intesa come piena libertà da enti di controllo – l'utente per compiere le proprie transazioni doveva necessariamente accedere ad un *server* che serviva per l'autenticazione e che permetteva il contatto, il trasferimento ad un altro utente e quindi il controllo di un ente centralizzato – con Bitcoin l'operazione di decentralizzazione è stata compiuta e la conseguente possibilità di trasferire denaro digitale in maniera completamente decentralizzata, senza il necessario intervento di alcun tipo di ente finanziario o governativo, realizzata.

In detto scritto sono state, altresì, presentate le caratteristiche tecnologiche della criptovaluta, quali la *crittografia*, il *protocollo di comunicazione* e la *rete* peer-to peer[79].

Successivamente, il 3 gennaio 2009 è stato "minato"[80] il primo blocco di Bitcoin (c.d. *blocco 0* o *genesis block)*. Il 12 gennaio 2009 è stata registrata la prima transazione del valore di 10 BTC, effettuata direttamente da Nakamoto a favore di Finney. Proprio questa operazione ha scatenato in molti il pensiero che dietro lo pseudonimo di Satoshi Nakamoto si nascondesse proprio Hal Finney, anche in virtù del fatto che il Bitcoin utilizza la tecnologia del POW da lui introdotta nel 2004.

È bene evidenziare come i Bitcoin, il cui valore era irrilevante, erano inizialmente posseduti unicamente dagli sviluppatori che li avevano generati. Solo successivamente, con la nascita di numerosi forum di scambio di Bitcoin[81] l'utilizzo della criptovaluta ha subito un'espansione con la successiva nascita di un mercato di criptovalute in cui sono direttamente i privati a fissarne il prezzo e il valore.

In questa fase, l'obiettivo principale degli sviluppatori nascosti dietro lo pseudonimo di Satoshi Nakamoto era quello di diffondere la conoscenza della criptovaluta, in modo da coinvolgere sempre più soggetti e rendere il sistema Bitcoin sempre più potente. In particolare, il metodo utilizzato per la diffusione prevedeva che venissero utilizzati i BTC per qualsiasi tipo di transazione: era il 22 maggio 2010 quando Laszlo Hanyecz, sviluppatore, offrì 10.000 BTC, all'epoca pari a circa $25, per due pizze. Si pensi, per comprendere anche la

---

[79]S. CAPACCIOLI, *Criptovalute e Bitcoin: un'analisi giuridica,* Giuffrè, Milano, 2015, p.37; S. CAPACCIOLI (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021, pp. 85 ss.

[80] Vedi *infra* § 3.3. *Mining*.

[81] Inizialmente le compravendite di BTC avvenivano esclusivamente nel forum del progetto Bitcoin: *BitcoinTalk.org* fondato il 22 novembre 2009. Successivamente, nel marzo 2010, è nato *Bitcoin Market*.

crescita che ha avuto Bitcoin negli anni, che al tasso di cambio più alto mai raggiunto dal Bitcoin nel marzo 2024, quando 1BTC valeva $73.737,94 l'acquisto delle due pizze sarebbe valso quasi $ 737.379.400,00; laddove, invece, oggi, nel maggio 2024 l'acquisto delle due pizze sarebbe avvenuto per un valore di circa $ 611.180.000,00 [82].

Il 17 agosto 2010 un BTC aveva un valore pari a 7,69 centesimi di dollaro. Solo nel febbraio 2011 varrà poco più di $1, per arrivare a valere $35 due mesi dopo.

Nonostante una momentanea battuta d'arresto dovuta a un attacco hacker alla *Mt.Gox*[83], una delle piattaforme più importanti di *trading*, a partire dal febbraio 2013 il valore del BTC è cresciuto notevolmente, arrivando a valere $237 nell'aprile 2013 e $1.151,00 alla fine del novembre 2013[84]. Il valore del BTC, come percepibile dai dati ora forniti, ha subito molte oscillazioni negli anni, il massimo storico, come detto, è stato raggiunto nel dicembre 2021 in cui ha toccato il valore di $68.000,00, dopo una progressiva discesa iniziata all'inizio del 2018 – quando il valore del BTC è crollato nuovamente sotto la soglia dei $4.000,00 – e durata sino alla pandemia da Covid-19, che ha riportato in auge il valore delle criptovalute.

È bene evidenziare sin d'ora come, dopo la nascita e la diffusione della criptovaluta Bitcoin sono state sviluppate diverse criptovalute – dette *alternative coin* o *altcoin* –che, pur simili a Bitcoin, si caratterizzano per profili differenti, che verranno analizzati nel prosieguo.

Tra queste le più note sono *Ethereum* ed *Ethereum Based Token, Monero, Litecoin*, *Ripple, Dash* e *Tether*[85].

3. *Il funzionamento delle criptovalute e, in particolare, di Bitcoin.*

Come detto, pur non essendo il giurista un informatico è necessario che questo comprenda, o quanto meno cerchi di comprendere al meglio, i fenomeni di cui si occupa, per poter proporre soluzioni adeguate alle problematiche rilevate nel corso della ricerca. Per questo motivo, di seguito, cercheremo di far luce sul funzionamento e sui meccanismi che su cui si basa il Bitcoin.

Nel *paper* pubblicato da Satoshi Nakamoto è chiaramente spiegato come la tecnologia alla base del Bitcoin – la c.d. *blockchain* – sia pensata per

---

[82] Alla data del 09.05.2024 il valore di 1 BTC è pari a $61.118,00 (euro 56.925,31).

[83] Vedi *infra* § 6.1. *L'acquisto di criptovaluta con moneta avente corso legale*: *gli* exchanger.

[84] M. AMATO, L. FANTACCI, *Per un pugno di Bitcoin- Rischi e opportunità delle monete virtuali*, Università Bocconi Editore, 2016 pp. 27-28; F. GRAZIANI, *Bitcoin, tutti i numeri dell'ascesa*, 2018, in www.masterx.iulm.it, reperibile al seguente link.

[85] Vedi *infra* §4. *Dalla volatilità di Bitcoin alle "stablecoin"*.

soddisfare diverse caratteristiche e diversi scopi ricercati sin dalla nascita del movimento *Cypherpunk* dagli sviluppatori, sintetizzabili nei seguenti punti:

(a) Assenza di banche o intermediari, quindi di qualsiasi terza parte fiduciaria;
(b) Prevenzione della *double spending;*
(c) Possibilità di garantire lo (pseudo) anonimato ai partecipanti.

3.1 *La* blockchain.

Dobbiamo innanzitutto sottolineare come la tecnologia *blockchain* non sia da riferirsi unicamente al Bitcoin, ma sia propria di diversi fenomeni in divenire, tanto che sono molti gli studiosi a sostenere l'utilizzo di detta tecnologia rivoluzionerà molteplici aspetti della vita di ogni persona[86].

Il termine *blockchain* viene utilizzato in numerose accezioni ed ha molteplici significati: in primo luogo la *blockchain* è un sistema *peer-to-peer* distribuito, costituito da una rete costituita da molti computer, definiti *nodi* che rendono accessibili uno all'altro risorse quali la *capacità di calcolo* e la *memoria* in maniera del tutto anonima e decentralizzata. Ne consegue che tutti i computer svolgono il medesimo ruolo e hanno la medesima capacità di accesso nella rete: non vi è un nodo centrale che controlla e regola gli altri. Proprio da qui la definizione di sistema *peer-to-peer*, "tra pari".

In particolare, possiamo definire la *blockchain* come «*un sistema peer-to-peer distribuito di ledger*[87] *che utilizza algoritmi che trattano dati con tecnologie crittografiche e di sicurezza al fine di mantenere l'integrità nel sistema*»[88]. Detta tecnologia soddisfa la stessa funzione del libro mastro, ma in maniera del tutto decentralizzata: grazie alle caratteristiche della *blockchain* è infatti possibile verificare, in assenza di una parte terza che effettui dei controlli, se una transazione sia legittima o meno. Ogni utente della rete, proprio perché si tratta di un sistema *peer-to-peer*, è in possesso di una copia del libro mastro che contiene tutte le transazioni. Di talché ogni soggetto, ogni utente, può richiedere che una determinata transazione sia registrata nella *blockchain*, ma tale richiesta sarà soddisfatta solo se tutti gli utenti saranno concordi rispetto alla sua legittimità[89].

---

[86] Si rinvia a A. ROSATO, *Profili penali delle criptovalute*, Pacini Giuridica, Pisa, 2021, pp. 9 ss.
[87] Con il termine inglese *ledger* si fa riferimento al *libro mastro*, quindi il registro in cui, nell'ambito della contabilità, vengono raccolte le transazioni contabili.
[88] L. FOTI, *Capire Blockchain*, p.5.
[89] È opportuno riferire dell'esistenza di diverse tipologie di *blockchain*. Quella sinora descritta è una *blockchain* c.d. *permissionless*, in ragione della libertà degli utenti di

Si tratta di un controllo automatico, di un libro mastro molto sicuro, capace di resistere ai frequenti tentativi di manomissione da parte di *hacker*[90].

Tale autenticazione è possibile grazie all'utilizzo delle firme digitali, introdotte da Chaum: Capaccioli definisce la firma digitale come «*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici*, *utilizzati come metodo di identificazione informatica*»[91]. La *blockchain* per garantire l'anonimato, ma anche la riservatezza dei messaggi intercorrenti tra diversi utenti, si serve di una crittografia asimmetrica[92], caratterizzata da due chiavi: una chiave pubblica e una chiave privata, entrambe generate da un algoritmo, quindi da un calcolo matematico.

Mentre la *chiave privata* deve sempre rimanere tale, la *chiave pubblica*, invece, viene fornita dall'utente ai soggetti con cui vuole comunicare.

Più precisamente, la *chiave pubblica* (o indirizzo pubblico) è una stringa alfanumerica di lunghezza variabile, necessaria per ricevere le criptovalute: deve essere condivisa con gli altri utenti affinché possano essere svolte le operazioni in criptovaluta. Parte della dottrina ha descritto l'indirizzo pubblico come una sorta di indirizzo IBAN[93]. È bene evidenziare sin d'ora come ciascun utente potrebbe astrattamente detenere più chiavi pubbliche che non siano a lui direttamente associabili.

La *chiave privata* è, invece, necessaria per ricavare una chiave pubblica e permette agli utenti di disporre delle criptovalute abbinate tramite l'utilizzo di firme crittografiche, che ne permettono la spendita e lo scambio. Parimenti a quanto avviene per l'indirizzo pubblico, anche la chiave privata non è contenuta in un registro che la associ direttamente a un utente.

Da un punto di vista figurativo, poi, la *blockchain* è stata descritta come una catena formata da blocchi. Amato e Fantacci spiegano come «*la blockchain si compone di una serie concatenata di blocchi (da cui il nome), i quali registrano per ogni transazione, l'identità del pagante, l'importo trasferito e*

---

accedervi e di potere verificare e consultare tutte le transazioni su di essa operate. Si affiancano la *blockchain privata* e la *blockchain ibrida*. La *blockchain privata* si caratterizza per il suo utilizzo limitato solo a determinati soggetti previamente individuati e autorizzati: solo questi potranno iscrivere e validare le transazioni ivi operate. Nelle *blockchain ibride*, invece, il controllo non è centralizzato ma distribuito, le transazioni possono essere operate sia da determinati soggetti privati sia dal pubblico. Si rinvia a A. ROSATO, op.cit., pp. 21 ss.

[90]P. BOUCHER, S. NASCIMENTO, M. KRITIKOS, *Come La Tecnologia Blockchain Può Cambiarci La Vita, Analisi Approfondita,* EPRS | Servizio Ricerca del Parlamento europeo, European Parliament, 2017, reperibile al seguente link.

[91] S. CAPACCIOLI, *Criptovalute e Bitcoin: un'analisi giuridica,* Giuffrè, 2015, pp. 37 – 38.

[92] U. BUONORA, *op.cit.*, pp. 55 ss.

[93] *Ibidem.*

l'identità del beneficiario» [94]. All'interno di ogni blocco sono infatti contenute tutte le informazioni che riguardano ogni transazione che si sia svolta nell'arco di tempo di dieci minuti, oltre che un riferimento al precedente blocco. Vediamo quindi che, ogni qualvolta un nodo riceve una transazione, questa verrà aggiunta ad un nuovo blocco. Affinché questo sia validato, sarà necessario risolvere un complesso calcolo matematico, la cui soluzione avrà come base il blocco stesso (attività di *mining*). Il blocco viene confermato grazie all'utilizzo di un codice *hash*[95], calcolato sul blocco in questione e su quello precedente. È da qui che si crea una catena di codici definita dal fatto che ogni blocco contiene al suo interno il codice *hash* del blocco precedente. Ogni blocco, quindi, ricondurrà al blocco genesi o blocco 0. Tale sistema, come intuibile, permette una datazione di tutte le transazioni, creando quindi una catena praticamente immodificabile a meno che non si verifichino delle anomalie rispetto alla accettazione o al rifiuto del blocco. In questo caso si determinerà una derivazione che vedrà nascere una o più *blockchain* diverse da quella originaria: si parla in questi casi di *fork*. Un *fork* si verificherà ogni qualvolta vi sarà un blocco danneggiato, non solo a causa di operazioni scorrette da parte degli utenti (vedi il tentativo di *double spending*, di cui si dirà nel prosieguo), ma anche quando si verifichino dei *bug*[96] o aggiornamenti di versione. La *fork* non si considererà valida in quanto si verificherà l'impossibilità di convalida dei blocchi dovuta all'interruzione della catena. I blocchi validi, invece, saranno aggiunti a una parte valida della *blockchain*. La catena originaria, ufficiale, sarà quella con più blocchi validi, quindi, figurativamente, quella più lunga[97].

È di tutta evidenza, dunque, come il sistema *blockchain* sia in ogni istante in grado di fornire una raffigurazione completa di tutte le transazioni

---

[94] M. AMATO, L. FANTACCI, *op.cit.*, p.16.

[95] È un algoritmo matematico per cui a una composizione di caratteri corrisponde un codice univoco di lunghezza fissa. Più precisamente, le funzioni c.d. di *hashing* riescono a ricevere in input una stringa di qualsiasi lunghezza, restituendo una di lunghezza prefissata. Foti riporta il seguente esempio: "Io mi chiamo Lorenzo": hash = 584589034. *Cfr*. L.FOTI, *op.cit.* p.36. Le funzioni di *hashing* si caratterizzano per tre diverse proprietà: 1) se applicata una stessa funzione di *hashing,* uno stesso *input* restituirà sempre lo stesso *output*, generato dall'algoritmo della funzione; 2) pertanto, due input anche solo minimamente differenti restituiranno output differenti; 3) non è possibile risalire dall'*output* all'*input*, perché la funzione di *hashing* non è reversibile. L'utilità maggiore dell'*hashing* consiste nella possibilità di verificare che una data informazione non sia stata alterata e che sia rimasta invariata nel tempo. Si rinvia a S. CAPACCIOLI (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021, pp. 55 ss.

[96] Un *bug* consiste in un errore nella scrittura di un codice che compromette il funzionamento di un programma informatico. Si rinvia a www.ibm.it.

[97] F. CICLOSI, P. GASPARI, *Bitcoin. Genesi e funzionamento di una criptovaluta*, Edizioni Simple, Macerata, 2017, pp. 32-33.

che siano state svolte dagli utenti sin dal principio[98]. Ad esempio, collegandosi al sito *blockexplorer.com* sarà possibile visionare la *blockchain* e ottenere tutte le informazioni riguardanti ciascuna transazione. Proprio per questo motivo Amato e Fantacci definiscono il *distributed ledger* come una *«rappresentazione in scala 1:1 dell'economia Bitcoin»*[99].

Possiamo individuare cinque diverse caratteristiche, alcune già analizzate altre lo saranno nel prosieguo, proprie della *blockchain* così come individuate da Marco Ianisti e Karim R. Lakhani[100]:

(i) *Database distribuito e decentralizzato*: ogni utente ha accesso all'intera *blockchain* e a tutte le transazioni effettuate con la stessa. Non vi è un sistema centralizzato, tutti gli utenti sono uguali tra loro. Tutte le transazioni saranno controllate e verificate direttamente dai partecipanti;

(ii) *La trasmissione* peer-to-peer: tutti gli utenti hanno uguale importanza nel sistema, tutte le comunicazioni avverranno tra pari e non tramite l'intervento di un soggetto intermediario;

(iii) *La trasparenza attraverso la pseudonimizzazione*: tutte le transazioni e il valore ad esse associate sono visibili a chiunque acceda al sistema. Ogni utente sulla *blockchain* possiede un indirizzo alfanumerico composto da minimo trenta caratteri che lo identificano. Questo perché ogni utente può anche scegliere di rimanere anonimo e di non mostrare agli altri la propria identità.

(iv) *Irreversibilità delle transazioni registrate*: una volta che una transazione è stata compiuta, non vi sarà più modo di modificare la stessa. Ciò avviene grazie all'utilizzo di algoritmi molto complessi volti ad assicurare che la registrazione sulla *blockchain* sia permanente, ordinata cronologicamente e visibile a tutti gli altri utenti della *blockchain*. Detta caratteristica è stata voluta con un chiaro intento "anti-frode", volto a rendere più sicure le transazioni intervenute sulla *blockchain*.

(v) *Logica computazionale*: la natura digitale del libro mastro comporta che le operazioni possano essere collegate alla logica computazionale della *blockchain* e programmate così che gli utenti possano configurare gli algoritmi.

---

[98] M. AMATO, L. FANTACCI, *op.cit.*

[99] *Ibidem.*

[100] M. IANSITI, K.R. LAKHANI, *The Truth About Blockchain*, in *Harvard Business Review,* 2017, reperibile al seguente link.

È bene evidenziare come, ad oggi, sono diverse le criptovalute che si basano sulla tecnologia *blockchain*, di volta in volta implementata con caratteristiche differenti a seconda della criptovaluta considerata.

3.2 *Pseudoanonimato.*

La *blockchain*, come abbiamo visto e come espressamente voluto e dichiarato da Satoshi Nakamoto nel suo *paper*, è una rete pubblica e volutamente trasparente. Ciò permette ad ogni utente della rete di visualizzare tutte le operazioni in Bitcoin che sono state effettuate in un determinato periodo di tempo, quindi tutte le informazioni relative ad una determinata transazione.

Un primo problema che si pone però, sebbene dalla maggior parte degli *user* sia visto come un importante vantaggio, è dato dal fatto che sarà difficile risalire alla reale identità dei singoli *user*, proprio in ragione dell'utilizzo delle chiavi digitali, pubbliche e private.

Questo è il motivo per cui si parla di *pseudoanonimato*: nonostante la pubblicità del registro delle operazioni, del libro mastro che è la *blockchain*, gli *user* non saranno identificabili se non per una stringa, composta da una serie alfanumerica, generata in senso casuale, in alcun modo riferibile all'utente[101]. Pertanto, i dati sensibili, il nome e il cognome degli utenti, non saranno mai conoscibili agli altri operatori[102].

Parte della dottrina ha rilevato come, in realtà, l'anonimato *rectius* lo *pseudoanonimato* sarebbe fortemente attenuato per diversi motivi: innanzitutto l'utilizzo degli pseudonimi comporterebbe unicamente la riservatezza dei propri dati personali e sensibili; in secondo luogo, alcune appropriate tecniche di *digital forensics*[103] sarebbero in grado di ricostruire tutto il traffico dati, rendendo in questo modo la *blockchain* effettivamente pubblica e trasparente[104]. Sono molti gli studiosi del fenomeno che, a questo proposito,

---

[101] Da un punto di vista visivo è possibile distinguere due formati di chiavi pubblica, a c.d. "base58" o a base "bech32": nel primo caso, avremo una stringa alfanumerica composta da 25-34 caratteri, ove il primo è rappresentato dal n. 1 o dal n. 3 e al cui interno, proprio per evitare possibile confusione, non è possibile utilizzare i caratteri "l" (elle minuscola), "I" (i maiuscola), "O" (o maiuscola) e "0" (zero). Il formato *bech32*, invece, di più recente introduzione (2017) si caratterizza per avere stringhe che iniziano con "bc1", sì da ottimizzare la memorizzazione delle transazioni. Per un maggiore approfondimento si rinvia a U. BUONORA, *op.cit.*, pp. 55 ss.

[102] G.P. ACCINNI, *Profili di rilevanza delle «criptovalute» (nella riforma della disciplina antiriciclaggio del 2017),* in *Archivio Penale*, Fascicolo n.1, 2018, pp. 5-6, in www.archiviopenale.it, reperibile al seguente link.

[103] Il riferimento è alla disciplina dedita al trattamento dei dati digitali di ogni tipo, al fine di rilevare prove informatiche utili all'attività investigativa. Si rinvia al seguente link.

[104] S.CAPACCIOLI, *Criptovalute e Bitcoin: un'analisi giuridica,* Giuffrè, Milano, 2015, pp. 44 - 45.

hanno sostenuto che, in realtà, il sistema *blockchain* non sia in alcun modo adeguato a garantire l'anonimità in quanto la *blockchain* mostra tutte le operazioni effettuate da un determinato *account*. Ciò comporterebbe che le Autorità competenti potrebbero riuscire a risalire all'effettivo titolare del portafoglio elettronico tramite l'utilizzo di appositi *software*.

E questo è pur vero, come è vero però, che una delle caratteristiche primarie ed essenziali dei Bitcoin – e delle criptovalute in genere – consiste nella possibilità di permettere ad ogni utente di dotarsi di una quantità numericamente indeterminata di chiavi pubbliche che siano associate, a loro volta, a un numero indeterminato di chiavi private. Ciò permetterebbe, e di fatto permette, di utilizzare un identificativo – se così si vuol chiamare la chiave pubblica – diverso per ogni transazione effettuata. Si parla di un numero illimitato di combinazioni.

È di tutta evidenza, dunque, come tale aspetto complichi l'identificazione: qualora un soggetto, dichiaratamente in mala fede, decidesse di utilizzare una molteplicità di chiavi pubbliche per effettuare una molteplicità di transazioni, allora risulterebbe estremamente complicato, se non addirittura impossibile, identificare la provenienza di quella operazione. Alcuni ritengono, che potrebbe divenire arduo perfino accorgersi che si tratti di transazioni sospette, comportando così la giustificata inerzia della Autorità competenti a vigilare. Inoltre, in molti hanno sostenuto che l'anonimato, in ogni caso, verrebbe meno ogniqualvolta i Bitcoin siano scambiati in valuta corrente, in quanto il denaro è gestito da istituzioni finanziarie capaci di conoscere l'identità all'utente. Queste sarebbero in grado di collegare l'*user* alla sua chiave pubblica per ricostruire tutti i passaggi. Ma ciò non risulta essere, in realtà, un'operazione immediata.

E se è pur vero, come sostiene Capaccioli, che in linea teorica le transazioni effettuate con la *blockchain* sarebbero più sicure e meno anonime di quelle effettuate con l'utilizzo di una carta di credito, nella vita reale ciò non è sempre possibile, a causa dello svilupparsi continuo di tecnologie dedite alla completa *anonimizzazione* delle transazioni. Sappiamo, infatti che negli ultimi anni, come evidenziato da diversi organismi nazionali ed internazionali di prevenzione e contrasto al riciclaggio, è aumentata sempre più la creazione di *software* molto complessi, messi a disposizione degli *user* al fine di permetter loro di aumentare la *privacy*, scontrandosi così con quella che dovrebbe essere la natura pubblica e trasparente della *blockchain*.

3.2.1 *I* crypto *mixer.*

I *crypto mixer* o *mixing service* sono *software* che permettono agli utenti di nascondere la cronologia delle transazioni effettuate.

I servizi di mixaggio di criptovalute, pur essendo potenzialmente utili per scopi legittimi di privacy sono divenuti, in ragione delle loro funzionalità, uno strumento ampliamente utilizzato dai *cybercriminal*.

La maggior parte dei mixer, infatti, rende i fondi depositati più difficili da rintracciare, consentendo agli utenti di programmare i loro prelievi in quantità randomizzate e a intervalli randomizzati. Altri cercano di nascondere il fatto che si sta usando un mixer; in genere lo fanno variando la commissione di transazione e il tipo di indirizzo di prelievo.

Ciò avviene grazie all'aggregazione di più trasferimenti: il *software* "mixa" sia l'origine che la destinazione di tutti i pagamenti[105]. Per meglio comprendere il funzionamento di detti sistemi, appare utile riportare l'esempio formulato da Giovanni Paolo Accinni: «*il pagamento da A ad A verrà perciò dirottato su B, e quello da B a B (importo corrispondente al primo) verrà dirottato su A, in modo che risultino confusi i nominativi degli ordinanti e i rapporti di dare e avere tra questi e i riceventi*»[106].

I *mixer,* dunque, raccolgono, accomunano e mescolano in modo pseudo-casuale le criptovalute depositate da molti utenti. In seguito, i fondi vengono prelevati da nuovi indirizzi sotto il controllo di ciascun utente, al netto di una piccola commissione di servizio.

Più precisamente, è possibile utilizzare due diverse tecniche di *mixing*: il trasferimento o il mescolamento.

Il *trasferimento* prevede che un soggetto frammenti le transazioni inviando un iniziale importo di criptovalute a più indirizzi detti "bounce" (di rimbalzo), sì da rendere più complesso il flusso di criptovalute tra più indirizzi. In questo caso, l'utente potrà agire privatamente, senza ricorrere a soggetti intermediari.

La tecnica di *mescolamento*, invece, vede il mescolamento, appunto, di più transazioni riferibili a più soggetti che utilizzano il *mixer* a un indirizzo di raccolta, detto *pool*, che solo successivamente trasferirà le criptovalute ai diversi indirizzi dei destinatari originariamente designati. Il rischio del mescolamento consiste nel passaggio da intermediari che, come vedremo, sono oggi – almeno astrattamente – costretti dalla normativa europea a precisi obblighi informativi e di registrazione degli utenti. Il rischio di individuazione e scoperta dell'utente, rispetto alla tecnica di trasferimento è, pertanto, leggermente maggiore[107].

---

[105] G.P. ACCINNI, *op.cit.*, pp. 5, 6.
[106] Cfr. *infra* Capitolo III, § 2.5. *Riciclaggio*.
[107] A. ROSATO, *op. cit.*, pp. 75 ss.

3.2.1.1 *Tipologie di mixer.*

È possibile distinguere almeno tre diverse categorie cui sono riconducibili la maggior parte dei *mixing service*: I *mixer centralizzati*, i *CoinJoin*, i mixer di *smart contract*[108].

I *mixer centralizzati*, emersi già nel 2011, assumono temporaneamente la proprietà dei fondi degli utenti e sono in genere gestiti da un unico operatore. Non sono particolarmente favoriti dai *cybercriminal* in quanto, essendo *centralizzati* e *custodial*, il loro utilizzo comporta un alto rischio di scoperta. Sono, infatti, spesso bersaglio delle forze dell'ordine, in quanto le agenzie di controllo finanziario li trattano come attività di servizi di denaro non registrate.

Vi sono poi i c.d. CoinJoin, che si caratterizzano per essere incorporati nei *wallet* che vogliono garantire una maggiore privacy all'utente e che, per questo, combinano le monete degli utenti con quelle di altri utenti in un'unica transazione. Gli utenti spesso ripetono questo processo più volte. A differenza dei *mixer* centralizzati, i CoinJoin non sono *depositari* (non custodial), ovvero non detengono mai i fondi degli utenti.

Tra i *mixer* non custodial vi sono anche i c.d. *smart contract*[109] *mixer* che si differenziano dai CoinJoin pechè non si basano sul mescolamento. Ed invero, l'utilizzo di questi *software*, prevede che l'utente invii i propri fondi al *mixer*, che emette una nota crittografica con cui attesta il deposito, che dovrà essere inviata al mixer per ritirare i fondi a un nuovo indirizzo.

Nonostante questi sistemi siano ormai noti, ancora oggi ci si interroga circa la liceità del loro utilizzo; ciò nonostante, non vi è ancora una disciplina che preveda in modo esplicito l'illegalità di simili *software*[110].

---

[108] CHAINALYSIS TEAM, *Crypto Mixers and AML Compliance*, agosto 2022, in www.chainalysis.com, reperibile al seguente link.

[109] Si tratta dei c.d. "contratti intelligenti" basati su tecnologia *blockchain* in cui determinate combinazione di codici informatici corrispondono al linguaggio giuridico. In particolare, gli *smart contract* vengono utilizzati per articolare, verificare e applicare un accordo tra le parti: possono detenere saldi di criptovaluta o controllare, a loro volta, altri programmi di *smart contract*. Una volta creati, possono eseguirsi autonomamente al verificarsi delle condizioni stabilite dai contraenti. Si rinvia a BANCA D'ITALIA, UNIVERSITÀ CATTOLICA DEL SACRO CUORE, UNIVERSITÀ ROMA TRE, *Caratteristiche degli Smart Contract. Draft v.1.0.*, giugno 2023, in www.bancaditalia.it, disponibile al seguente link.

[110] Negli Stati Uniti, il Financial Crimes Enforcement Network (FinCEN) ha confermato che gli individui e le aziende centralizzate che offrono servizi di mixaggio depositario devono registrarsi come trasmettitori di denaro ai sensi del Bank Secrecy Act (BSA) e hanno tre obblighi fondamentali: registrarsi presso la FinCEN, mantenere un programma di conformità antiriciclaggio e di conoscenza dei propri clienti, e soddisfare tutti i requisiti di rendicontazione e conservazione dei documenti. Si pensi che in USA tutti i mixer che vogliono fare affari devono adottare misure per assicurarsi di non trattare con entità sottoposte a sanzioni sia primarie sia secondarie. Si rinvia a CHAINALYSIS TEAM, *Crypto Mixers and AML Compliance*, *op.cit.* (link).

3.3 *Mining.*

Una delle caratteristiche del Bitcoin deve essere ricercata nella capacità degli utenti di sostenere il funzionamento della criptovaluta, tramite la possibilità di "minare" la criptovaluta, dietro un corrispettivo in Bitcoin o frazioni di esso generati *ex novo*.

Più precisamente, nella *blockchain* operano diversi soggetti e sebbene tutti i nodi concorrano a formare la rete Bitcoin e si tratti di un sistema *peer-to-peer,* non tutti svolgono il medesimo compito, la medesima attività: tra questi nodi ve ne sono alcuni definibili "ricercatori di nuovi Bitcoin".

Come abbiamo visto in precedenza, affinché in una tecnologia decentralizzata come quella del Bitcoin siano possibili l'autenticazione e la verifica della legittimità delle transazioni i programmatori hanno deciso di servirsi della tecnologia *blockchain*. La catena *blockchain* altro non è, come detto, che un insieme di blocchi tenuti insieme tra loro attraverso un lavoro computazionale. Tale attività computazionale viene svolta dagli *hardware* di alcuni tra i nodi della rete *peer-to-peer*, tali nodi sono i *miners*. Lo scopo principale del *mining,* però, non è la creazione di BTC, che è una sorta di retribuzione per l'attività svolta, ma è proprio il processo di autenticazione e di autorizzazione in assenza di una centralizzazione.

Il *mining*, quindi, non è solo controllo dell'attività e del sistema Bitcoin, ma è anche l'unica attività che permette l'immissione di nuovi BTC.

Al riguardo, dobbiamo considerare una caratteristica dei Bitcoin non ancora analizzata: non vi è una quantità indefinita ed infinita di criptovaluta, bensì un numero limitato e ben definito della stessa. Il progetto di Satoshi Nakamoto, infatti, ha fin dall'inizio previsto che vi sia una quantità di BTC prestabilita e che gli stessi siano creati o meglio trovati con sempre più crescente difficoltà: se inizialmente c'era bisogno di espandere tale tecnologia e di farla conoscere ai più e quindi l'attività in questione era un'attività poco dispendiosa per i *miner*, Nakamoto ha sin dal principio immaginato che con l'espansione del fenomeno diventasse sempre più complesso ottenere BTC attraverso il *mining*.

In particolare, si parlerebbe di una quantità assoluta di 21 milioni di Bitcoin. Tale quantità non è modificabile né *in peius* né *in melius*[111]. Proprio perché si tratta di risorse limitate, moltissimi studiosi si sono serviti della metafora dei *minatori per* descrivere il fenomeno. Tra questi Nikolei M.

---

[111] M. AMATO, L.FANTACCI, *op.cit,* pp. 54-55.

Kaplanov ha scritto che «*Bitcoin mining (...) is designed to mimic the extraction of minerals*»[112]: come i minatori estraggono rocce e minerali, così i *miner* estraggono BTC. Se i minatori si servono della scure, ciò di cui hanno bisogno i *miner* sono programmi informatici dediti all'attività in questione e potenza di calcolo. Sostanzialmente, infatti, il *mining* consiste in un'attività di risoluzione di problemi matematici molto complessi – gli algoritmi – che in forza della loro complessità richiedono una forte potenza di calcolo (c.d. potere computazionale), che richiede l'impiego di importanti quantità di energia elettrica[113]. Tutti coloro che riescono a decriptare l'algoritmo, a risolverlo, invieranno alla rete una prova di lavorazione (*Proof-of-Work, PoW*) [114] e riceveranno come ricompensa una certa quantità di BTC. Il sistema Bitcoin grazie a tale attività continuerà a funzionare, evitando altresì fenomeni di *double spending*. Come dice il significato stesso delle parole, tale rischio consisterebbe nella possibilità che una stessa somma di Bitcoin, o di criptovaluta in genere, sia utilizzata più volte in transazioni diverse, comportando così una frode per gli operatori. Ciò può avvenire ogni qualvolta

---

[112]«L'attività di minare Bitcoin (…) è stata pensata per imitare l'estrazione dei minerali», *cfr.* N.M. KAPLANOV, *op.cit.* p. 119.

[113] Uno studio pubblicato da CoinGecko – piattaforma *crypto data aggregator* – nell'agosto 2023 (aggiornato nel settembre 2023) ha dimostrato che per minare un singolo Bitcoin erano, allora, necessari in media 266,000 kWh di elettricità. Di talché, per un *miner* solitario detto processo richiederebbe circa sette anni per essere completato, con un consumo mensile di elettricità di crica 143 kWh. All'esito dello studio condotto è stato, quindi, stimato, che nel il costo medio dell'elettricità domestica per estrarre 1BTC, in USA, era pari a 46.291,24 dollari (il 35% in più rispetto al costo stimato nel luglio 2023, in cui per 1BTC era necessario impiegare energia per 30.090,08 dollari. All'epoca si stimava che il costo della medesima operazione in UE si aggirasse attorno a 85.767,84 dollari (= 77.817,8 euro, come da tabella cambi Banca d'Italia al 31.07.2023) stante il costo medio più alto dell'elettricità. A vantare i costi medi più bassi per singolo minatore vi era l'Asia in cui l'operazione di estrazione 1 BTC richiedeva una spesa di energia elettrica paria 20.635,62 dollari. È interessante osservare come l'Italia si assestasse al primo posto nella classifica "The most unprofitable Countries to Mine 1BTC" con un costo pari a 208.560,33 dollari (= euro 189.228,00). Si rinvia a W. AMASE, *Household Electricity Costs to Mine 1 Bitcoin at Home, Around the World*, settembre 2023, in www.coingecko.com , reperibile al seguente link.

È ragionevole pensare che da settembre 2023 a maggio 2024 l'algoritmo da risolvere per minare Bitcoin sia divenuto più complesso e richieda una quantità maggiore di energia elettrica con conseguente aumento dei costi in termini di *energia elettrica* per il *miner*.

[114] La *Proof-of-Work* (PoW) è una prova di lavorazione che consiste nell'incessante attività di risoluzione di algoritmi volta da una parte alla conferma delle transazioni e dall'altra alla produzione di nuovi blocchi della *blockchain*. La *PoW* è alla base del sistema Bitcoin e si serve dell'*hash* SHA- 256: tale funzione si caratterizza per il fatto che la sua risoluzione darà sempre come risultato una stringa alfanumerica formata da 64 caratteri, indipendentemente da quale che sia la stringa di partenza. Tale tecnologia, inoltre, regola anche la velocità con cui la rete genera i nuovi blocchi, mantenendo una velocità media che consenta il corretto funzionamento della *blockchain*.

vi sia un nodo che intenzionalmente provi e riesca ad alterare la *blockchain*, inserendovi un'operazione che risulti ingannevole, capace di creare un problema nella transazione. Al fine di evitare di incappare in simile operazione fraudolenta, l'unico palliativo consiste nella complicazione del processo di validazione[115]. E proprio al fine di garantire la correttezza delle transazioni che gli sviluppatori hanno pensato alla *PoW*.

Si tenga presente che il protocollo Bitcoin è stato immaginato per mantenere una velocità di creazione e di erogazione di nuovi BTC all'incirca ogni dieci minuti. Affinché ciò avvenga, il sistema prevede che la difficoltà di risoluzione dell'algoritmo vari in base al numero di *miners* attivi e quindi alla competizione della rete. Qualora la frequenza di accettazione dei blocchi immediatamente precedenti sia risultata superiore a dieci minuti, vi sarà una diminuzione del livello di difficoltà di risoluzione dell'algoritmo; al contrario, qualora i *miners* dovessero risolvere agevolmente l'algoritmo, il livello di difficoltà di risoluzione dello stesso sarà aumentata. Chiaramente, più *miners* vi sono, più sarà garantita la sicurezza della rete, in quanto la stessa riceverà maggiori validazioni rispetto alla medesima operazione: i programmatori hanno pensato alla ricompensa in Bitcoin proprio per incentivare una vasta presenza di *miners*. Più *miners* sono attivi sulla rete più sarà semplice garantire la sicurezza e la diffusione del sistema Bitcoin. In questo modo, sarà maggiore la fiducia negli utenti in questa criptovaluta[116].

Nonostante ciò, attualmente, non è così semplice ottenere BTC attraverso l'espletamento della attività di *mining*, stante il continuo aumentare della difficoltà dell'algoritmo con conseguente maggiore necessità di potenza di calcolo. Per questo motivo, ad oggi, è assai improbabile che chi usa un *personal computer* riesca a minare nuovi BTC[117]. L'attività di *mining* è diventata un'attività economicamente onerosa per chi la compie proprio a causa degli *hardware e* dell'elettricità utilizzati: più *miner* ci sono, più è resa sicura la *blockchain* e maggiore sarà la difficolta di *mining.* Tale attività, oggi, per essere redditizia richiede l'utilizzo di strumenti informatici particolari e molto costosi, tanto che il *mining* è svolto da imprese diventate specializzate nel settore, spesso organizzate in gruppi, presenti in tutto il mondo, compresa l'Italia in cui il *mining* è divenuto vero e proprio *business*[118].

---

[115] R. GARAVAGLIA, *Tutto su Blockchain. Capire la tecnologia e le nuove opportunità.*, Hoepli, Milano, 2018, p. 80.
[116] F. CICLOSI, P. GASPARI, *op.cit.,* pp. 46-47.
[117] N.M. KAPLANOV, *op.cit.*, p. 119.
[118] M. AMATO, L. FANTACCI, *op.cit.*, p.2.

Si tratta dei c.d. *mining pool*, immaginati da Slush, un utente di BitcoinTalk[119], che per primo ha compreso, da un lato, che maggiore capacità computazionale avrebbe comportato, nell'immediato, un maggiore ritorno in termini di criptovalute; dall'altro lato, ha intuito che con il passare del tempo il *mining* di Bitcoin avrebbe richiesto la risoluzione di calcoli algoritmici sempre più complessi e, quindi, di maggiore potenza computazionale con conseguente necessità di specifici circuiti composti da più *miner*.

L'intuizione si è rivelata corretta: oggi lo spazio di *mining* di Bitcoin è gestito da circa tredici *mining pool*, ognuno composto da migliaia di *miner* provenienti da ogni parte del mondo[120].

4. *Dalla volatilità di Bitcoin alle "stablecoin".*

La decentralizzazione delle criptovalute e l'assenza di intermediari garantita, oltre che dalla struttura della *blockchain* anche dall'attività di *mining,* ha reso Bitcoin una criptovaluta caratterizzata da alta volatilità.

La volatilità è una misura di quanto il prezzo di un particolare *asset* sia salito o sceso nel tempo[121]. Generalmente, più un *asset* è volatile, più viene considerato rischioso come investimento e più potenziale ha di offrire ritorni più alti o perdite maggiori su periodi più brevi rispetto ad *asset* comparativamente meno volatili. La volatilità rappresenta, infatti, uno dei principali fattori che contribuiscono alla valutazione del rischio di investimento. Tradizionalmente, gli investitori assumono un livello elevato di rischio se ritengono che il potenziale guadagno valga la possibilità di perdere parte del loro investimento.

---

[119] Si tratta di uno dei più grandi forum in cui gli utenti possono scambiarsi ogni genere di informazione su Bitcoin.

[120]Tali dati sono quotidianamente aggiornati e consultabili al seguente link. Sulla piattaforma è possibile consultare, quotidianamente, l'operato dei *mining pool* attivi in tutto il mondo. Alla data del 4 marzo 2024 risulta che nell'ultimo mese siano stati operativi 11 *pool* con il predominio di *Foundry USA*.

[121] È necessario distinguere la *volatilità storica* - che fa riferimento allo studio dei prezzi in un periodo di tempo definito (di solito 30 giorni o un anno) – dalla *volatilità implicita* che mira a prevedere la volatilità del mercato nel prossimo futuro. La volatilità può essere quantificata con il metodo Beta, che valuta quanto sia volatile un'azione rispetto al mercato più ampio ovvero misurando la deviazione standard di un asset; quindi, verificando quanto ampiamente il suo prezzo si è discostato dalla sua media storica. I fattori che possono aumentare la volatilità includono coperture mediatiche positive o negative e relazioni sugli utili che sono migliori o peggiori del previsto. Picchi insolitamente alti nel volume di scambi di solito corrispondono alla volatilità. Volumi molto bassi (come nel caso delle cosiddette penny stock che non vengono scambiate sui mercati principali o delle criptovalute più piccole) di solito corrispondono anche ad alta volatilità.

Il valore delle criptovalute –nonostante siano un *asset* particolarmente giovane, sviluppatosi in poco più di un decennio – ha subito una serie di forti aumenti seguiti da cali successivi, al punto da essere considerate una categoria più volatili delle azioni[122].

Ciò nonostante, è stato osservato come volumi di scambio più elevati su Bitcoin (di gran lunga la più grande criptovaluta per capitalizzazione di mercato) e una maggiore partecipazione istituzionale sembrano ridurre la sua volatilità nel tempo.

Se molti investitori sono stati, sin da subito, fortemente attratti dalle criptovalute proprio in ragione dell'alta volatilità – a cui possono conseguire alti rendimenti –, altrettanti hanno inizialmente rinunciato al loro utilizzo.

In tale contesto, sono progressivamente state sviluppate le c.d. *stablecoin* che, al pari di Bitcoin, possono essere utilizzate nei vari servizi finanziari basati su *blockchain* e possono essere utilizzate per pagare beni e servizi, beneficiando delle caratteristiche proprie delle criptovalute – decentralizzazione, (pseudo) anonimato e irreversibilità delle transazioni – senza, tuttavia, incorrere nei rischi connessi alla volatilità. Ed invero, le *stablecoin* sono un tipo di criptovaluta, non generata dal *mining*, il cui valore è ancorato a un riferimento esterno, quale, ad esempio, una valuta fiat come il dollaro statunitense, una merce come l'oro o uno strumento finanziario.

Più precisamente, è possibile distinguere due tipologie le *stablecoin garantite* e le *stable coin algoritmiche*. Mentre i primi sono ancorati a un asset specifico, i secondi si servono di *software algoritmici* per regolare automaticamente l'offerta della criptovaluta in base alla domanda, con l'obiettivo di mantenere un prezzo stabile.

Si presentano, così, come idonea alternativa alle criptovalute ad alta volatilità, svolgendo, proprio in ragione della loro stabilità, un importante ruolo nell'ecosistema delle criptovalute, financo a potersi ritenere che, nel tempo, potranno essere adottate regolarmente come mezzo di scambio nelle transazioni.

---

[122] Il concetto di volatilità non è strettamente collegato alle criptovalute, ma costituiscono un fenomeno proprio dei mercati finanziari. Ad esempio, le *azioni* sono considerate *asset* con una maggiore volatilità, dalla relativa stabilità delle azioni a grande capitalizzazione alle "penny stocks". Le *obbligazioni,* al contrario, sono considerate un asset a minore volatilità che, di solito, subiscono oscillazioni al rialzo e al ribasso meno nette che si verificano su periodi di tempo più lunghi.

4.1 *Gli Altcoin.*

Così descritte le caratteristiche principali della *blockchain* su cui è basata la criptovaluta Bitcoin, appare necessario evidenziare – come già anticipato – l'esistenza di ulteriori criptovalute, sviluppate dopo l'avvento del Bitcoin. Tra queste, le più note sono *Ethereum* e *Ethereum Based Token, Monero, Litecoin*, *Ripple, Dash* e *Tether*[123].

Trattasi di criptovalute *alternative* al Bitcoin – da qui il termine *altcoin* – con caratteristiche proprie e differenti.

4.1.1 *Monero.*

Sia permesso, in *incipit*, un giudizio di valore: Monero appare, infatti, la criptovaluta con le caratteristiche più interessanti, al pari di Bitcoin, nella commissione dei reati economici.

Sebbene, il funzionamento, almeno formalmente, sia molto simile a quello di Bitcoin, prevedendo una *blockchain* in cui le transazioni vengono operate tramite l'utilizzo di chiavi digitali, previa verificazione dell'operazione da parte dei minatori, Monero si caratterizza per essere una criptovaluta *anonima* e non *pseudoanonima.*

La forza di Monero deve essere ricercata nella sua capacità di sfruttare il modello delle *Ring signatures* (c.d. firme ad anello), in cui le chiavi dell'utente che ordina la transazione vengono sostanzialmente sovrapposte a quelle della *blockchain*, che nell'autorizzare la transazione genera una firma unica. Volendo semplificare, è possibile affermare che la firma del mittente viene fusa e sovrapposta a quella di altri soggetti che operano sulla stessa *blockhain*: Monero opera, sostanzialmente, come un *software* di *mixing*.

La struttura della *blockchain* di Monero è, pertanto, circolare diversamente da quella di Bitcoin che si sviluppa verticalmente.

4.1.2 *Litecoin e Dash.*

Litecoin è un progetto di criptovaluta risalente al 2011, fortemente ispirato alla criptovaluta Bitcoin, rispetto alla quale è maggiormente efficiente in punto di conferma della transazione e nella conservazione dei dati. Come accade per Bitcoin, anche in Litecoin è stata prevista una soglia massima di criptovaluta, quantificata in 84 milioni. Diversamente da Bitcoin, Litecoin è basato su uno *script*, anziché sull'algoritmo SHA256. Conseguentemente, i

---

[123] Si rinvia, sin d'ora, a U. BUONORA, S. CAPACCIOLI (a cura di), *Dal Bitcoin agli Stable Coin,* in *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021, pp. 74 ss.

suoi indirizzi sono costituiti da una stringa alfanumerica formata da 34 caratteri, ove il primo è “L”.

Dash, invece, nasce da Litecoin.

Inizialmente noto come X-Coin, poi divenuto Dark Coin, è oggi noto con la contrazione Dash da *Digital Cash,* in ragione della capacità di garantire – almeno astrattamente – transazioni istantanee di criptovaluta. Tra le sue caratteristiche è necessario ricordare la funzione di *InstanSend*, che rende indisponibile per l’utente la quantità di criptovaluta appena spesa, sì da evitare fenomeni di *double spending*. Anche in Dash, come in Bitcoin, è prevista la figura dei *minatori* a cui, diversamente da quanto avviene in Bitcoin, non è devoluto l’intero importo messo in circolazione all’esito dell’attività di *mining*, bensì solo il 45% del suo valore, laddove l’ulteriore 45% è destinato ai c.d. *masternode*, sostanziali intermediari interni al sistema stesso, che rappresentano gli unici utenti della rete Dash a conoscere le informazioni relative ad ogni transazione operata su detta *blockchain*. Vi è, quindi, una possibilità di *deanonimizzazione*, che non rende detta valuta virtuale particolarmente appetibile per commettere reati economici.

Ulteriore caratteristica deve essere individuata nel fatto che il 10% di ogni transazione è destinata al *team* di Dash, composto dagli sviluppatori, dall’assistenza e dal *team marketing*, anche al fine di ampliare l’evoluzione della criptovaluta[124].

4.1.3 *Ethereum e Ethereum Based Token e Ripple.*

Ethereum e Ripple si caratterizzano per essere sistemi più complessi rispetto alla *blockchain* su cui opera Bitcoin.

Quanto ad Ethereum, sebbene sia una valuta virtuale strutturalmente simile a Bitcoin, è anche una tecnologia *open source*, che permette ai suoi sviluppatori di costruire le *dApp,* vale a dire applicazioni decentralizzate. Per questo motivo si parla più che di “semplice *blockchain*” di struttura “cloud computing”, che permette di eseguire non solo transazioni di criptovaluta ma, più in generale, qualsivoglia esecuzione permessa dall’applicazione decentralizzata. Questo permette anche una certa autonomia e automaticità delle transazioni, che non devono essere di volta in volta disposte dall’utente, ma che possono essere determinate dall’Ethereum Virtual Machine (EVM), la struttura su cui si poggia Ethereum.

---

[124] Cfr. U. BUONORA, *op.cit.*, pp. 55 ss.

L'EVM, infatti, ha le stesse funzionalità di un *computer* fisico, permettendo di eseguire qualsivoglia tipo di operazione, come creare nuove valute virtuali anche senza introdurre una nuova e autonoma *blockchain*.

Ulteriore particolarità deve essere individuata nella parziale trasparenza delle transazioni effettuate con Ethereum: è sempre presente un indirizzo *input* e un indirizzo *output* e, inoltre, diversi soggetti – quali *miner* e *exchange* – sono noti ed esplicitamente indicati nelle transazioni.

Venendo, ora, a Ripple, si tratta di un sistema di trasferimento di fondi in tempo reale, che utilizza monete chiamate XRP. È un progetto che si rivolge a banche e istituti finanziari per trasferire fondi in via istantanea, così da permettere pagamenti veloci, a basso costo, anche di natura transazionale. Si tratta, più precisamente, di un *network* di *intermediazione* per trasferimenti di denaro di valute diverse e in tempi brevi.

Ripple si fonda sull'algoritmo Ripple Consensus, utile a registrare tutte le transazioni in maniera sicura.

Differisce da Bitcoin perché non si fonda su una tecnologia *blockchain,* ma sul c.d. *HashTree* in cui la transazione per essere ritenuta valida deve essere convalidata dall'80% – non dal 100% come accade nella *blockchain* – dei *validator*, che forniscono il consenso alla transazione. Non si tratta di un progetto centralizzato, posto che la società che gestisce Ripple detiene solo una piccola percentuale dei c.d. *server validator*, che si contano essere oltre 200.

Inoltre, gli XRP – rilasciati in quantità di 100 miliardi – non sono minati, ma assegnati a coloro che mettono a disposizione la potenza di calcolo su cui si fonda il sistema.

Caratteristiche di Ripple, poi, è rappresentata dalla presenza dei c.d. *gateway* che fungono da sostanziali intermediari tra utenti della rete, permettendo loro lo scambio di valute anche diverse tra loro[125].

4.1.4 *Le stablecoin.*

Tra le *stablecoin* più note troviamo Theter e Terra USD[126].

Theter, fondata nel 2014 e inizialmente denominata *Real Coin,* è stata la prima *stablecoin,* ancorata al valore del dollaro, quindi all'andamento del mercato. È una stablecoin garantita con una capitalizzazione di mercato, nel 2023, di oltre 80 miliardi di dollari, al punto da essere la terza principale valuta virtuale nel mondo cripto, dopo Bitcoin ed Ethereum.

TerraUSD merita di essere nominata in quanto è stata la più importante *stablecoin* algoritmica. Nel maggio 2022 ha, infatti, raggiunto un *market cap*

---

[125] *Ibidem.*

[126] D.ASHMORE, *Stablecoin: cosa sono e come funzionano*, in Forbes Advisor, settembre 2023, in www.forbes.com , reperibile al seguente link.

di oltre 18,7 miliardi di dollari, a cui è seguita una rapida discesa. Invero, il prezzo di TerraUSD era fissato a 1 dollaro attraverso la creazione e la distruzione della crypto Luna: non era garantita, in quanto il valore della criptovaluta funzionava attraverso la coniazione e la combustione algoritmica della criptovaluta Luna ogni volta che veniva acquistata o venduta una TerraUSD.

Oggi la *blockchain* di Terra è sganciata dal dollaro e la criptovaluta è nota come TerraClassicUSD.

5. *Strumenti di detenzione di criptovaluta: i wallet.*

Ulteriore aspetto utile a comprendere le potenzialità criminali delle criptovalute riguarda la modalità di detenzione da parte degli utenti.

È, infatti, bene premettere che caratteristica propria delle valute virtuali è da ricercare nella loro completa immaterialità.

Si rendono, pertanto, necessari alcuni strumenti utili alla detenzione e alla gestione delle criptovalute da parte degli utenti: i *wallet* o *portafogli.*

Oggi conosciamo diverse tipologie di *wallet*, che garantiscono una gestione piuttosto semplice delle valute virtuali tanto in punto di detenzione quanto di esecuzione delle operazioni che interessano all'utente.

Più precisamente, i portafogli di criptovalute permettono di inviare e ricevere transazioni in criptovalute, come se fossero dei "conto corrente". Si distinguono dagli *indirizzi,* che rappresentano le singole unità di accumulo e di trasferimento della criptovalute e che vengono gestiti tramite l'utilizzo dei portafogli.

I *wallet*, infatti, permettono di gestire molteplici *indirizzi*, senza che vi sia una connessione tra loro: vi è un'associazione unicamente figurativa, utile a garantire una migliore gestione del portafoglio da parte dell'utente senza che, tuttavia, un indirizzo possa essere collegato a un altro per il sol fatto di essere detenuti nello stesso *wallet*.

È possibile, ad oggi, distinguere quattro diverse categorie di *wallet* in base alle modalità di utilizzo, di accesso e di gestione delle chiavi private: *wallet online, wallet desktop, wallet mobile* e *wallet hardware*[127].

[127] In materia si rinvia a F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti. Lo statuto delle valute virtuali: le discipline e i controlli*, in *Archivio Diritto penale contemporaneo*, 10, 2018, pp.101 ss., reperibile al seguente link ;U. BUONORA, *op. cit*, pp. 65 ss.

5.1 *I wallet online.*

I *wallet online* rappresentano la categoria più diffusa di portafoglio di criptovalute, in ragione della semplicità di utilizzo e delle caratteristiche di funzionamento.

Caratteristica principale dei *wallet online* deve essere ricercata nella loro accessibilità tramite qualsiasi *web browser* subordinato all'utilizzo di apposite credenziali –tendenzialmente con autenticazione a due fattori in e, in qualche caso, previo inserimento di un *token* numerico generato da apposite *app* (es: Google Authenticator) – il cui inserimento permette all'utente di accedere a una sorta di *home banking*, su cui monitorare il saldo di una o più criptovalute – a seconda del *wallet* – e disporre operazioni di acquisto, rimessa o conversione.

Di regola, i *wallet online* sono *custodial*: la piattaforma gestisce le chiavi private degli indirizzi utenti. In tal senso, l'*user* non eseguirà direttamente le operazioni desiderate, ma si rivolgerà al gestore che le effettuerà materialmente.

La figura del *gestore*, tuttavia, non deve essere confusa con l'*exchanger* soggetto che – come vedremo – permette di convertire le criptovalute in moneta avente corso legale e viceversa. Ciò nonostante, è bene osservare come alcune piattaforme di *wallet* assurgono alla duplice funzione di *gestore* e *intermediario* di criptovalute (ne è un esempio la piattaforma CoinBase). In tal caso, l'*exchanger* dovrà adempiere gli obblighi antiriciclaggio, come previsti, a livello eurounitario, dalla IV e V Direttiva antiriciclaggio. È bene evidenziare sin da subito, tuttavia, che i *wallet online* devono essere distinti dalle piattaforme di *trading* con valute virtuali, che pur permettendo di disporre transazioni con criptovalute, hanno come fine ultimo l'ottenimento di un vantaggio sulla base dell'andamento del mercato.

Ciò detto, sebbene siffatta modalità di detenzione risulti particolarmente favorita dagli utenti, in ragione delle sue caratteristiche, che ne rendono molto semplice l'accesso e l'utilizzo, ha, già in passato, manifestato delle criticità legate al suo funzionamento. Ed invero, poiché la cronologia delle transazioni e le chiavi private sono conservate nel *server provider,* laddove il sito dovesse smettere di funzionare il rischio è che l'*user* possa perdere tutte le criptovalute sino ad allora accumulate. È quanto avvenuto con la piattaforma "QuadrigaCX" a seguito del decesso dell'amministratore, unico a potere accedere materialmente ai fondi degli utenti[128].

[128] E. PAGLIARI, 4 *agenzie investigano sull'* exchange QuadrigaCX, in *The Cryptonomist*, 28 agosto 2019, in www.cryptonomist.ch, reperibile al seguente link.

5.2 *I wallet desktop e i wallet mobile.*

Si tratta di particolari *software* installabili sul *personal computer* (*wallet desktop*) o su dispositivi mobili quali *smartphone* e *tablet* (*wallet mobile*), che permettono agli *user* di generare *indirizzi* da cui inviare e a cui ricevere criptovalute. Rispetto alle altre tipologie di portafoglio, questi portafogli appaiono maggiormente sicuri, ma il loro utilizzo è maggiormente tecnico, più complesso e, quindi, meno accessibile.

Si distinguono dalle altre tipologie di *wallet* sinora analizzate in ragione della loro capacità di custodire le informazioni relative all'utente e alle criptovalute detenute sul disco locale del *pc* o del *mobile.*

Detti *software* permettono, infatti, l'archiviazione delle chiavi private nonché il salvataggio della cronologia completa delle operazioni effettuate sulla *blockchain* nel disco locale. In tal senso, è possibile distinguere i *wallet full node* dai *light wallet.*

Anche in questo caso sarà possibile, a seconda delle caratteristiche del *software* scelto dall'utente, gestire una o più tipologie di criptovalute tramite l'utilizzo di uno stesso portafoglio che contenga i diversi indirizzi.

I primi permettono di scaricare sul disco locale del pc una copia dell'intero registro riguardante tutte le operazioni inserite sulla *blockchain*, sicché l'*user* diventerà un nodo della rete e potrà verificare la legittimità delle transazioni effettuate.

L'utilizzo dei *wallet full node* è, generalmente, piuttosto semplice: l'utente potrà agilmente visionare sia lo stato del proprio portafoglio che effettuare e ricevere le transazioni desiderate la cui cronologia sarà riportata in apposita sezione, sì da potere essere sempre agilmente consultata, anche tramite apposite *categorizzazioni*. Tra i più noti si ricorda "bitcoin Core"[129].

I *light node*[130], invece, noti anche come *Simple Payment Verification* (SPV) si distinguono dai *full node* perché non prevedono la possibilità di scaricare sul disco locale l'intera copia della *blockchain*.

Inoltre, l'autonomia dell'utente è, in tal caso, ridotta: gli indirizzi e le transazioni vengono gestite da *server* intermedi che comunicano con la *blockchain* della criptovaluta cui si riferiscono. Si tratta di uno degli aspetti maggiormente criticati per due ordini di ragioni: innanzitutto, le informazioni, ancorché verificabili direttamente dall'utente proprio in ragione della pubblicità e della trasparenza della *blockchain*, vengono di regola riferite da soggetto terzi, che svolgono il ruolo di *nodi* della rete; in secondo luogo, aspetto

---

[129] Cfr. BITCOIN.ORG, *Running a full node. Support the Bitcoin network by running your own full node*, in www.bitcoin.org, reperibile al seguente link.

[130] Cfr. LEDGER ACADEMY, *Light Node Meaning*, in www.ledger.com, reperibile al seguente link.

maggiormente critico, lo scambio di informazioni tra l'utente e il nodo operante sul *wallet light node* comporterà l'inevitabile rivelazione degli indirizzi detenuti dall'*user,* delle caratteristiche del *wallet* utilizzato nonché dell'indirizzo IP da cui vengono svolte le operazioni: il cliente al fine di accedere alle proprie informazioni dovrà inviare una richiesta contenente l'indicazione degli indirizzi detenuti associando l'indirizzo IP pubblico della connessione utilizzata.

In tal senso, non solo lo pseudoanonimato (o anonimato, a seconda della criptovaluta interessata) potrà venire meno – con riconducibilità degli indirizzi detenuti a un medesimo soggetto – ma l'utente potrebbe irrimediabilmente esporsi al rischio di furto di criptovalute o perdita di fondi.

Diversamente da quanto avviene nei portafogli *online*, nei *desktop wallet* le chiavi private sono gestite direttamente dall'utente. Ciò nonostante, il rischio di non potere più accedere alle proprie criptovalute non è neutralizzato: se è vero che, differentemente da quanto avviene nei *web wallet*, le chiavi private di questi portafogli sono detenute direttamente dall'utente e non affidate a un gestore, è altresì vero che l'accessibilità alle stesse è strettamente legata al corretto funzionamento del dispositivo su cui è installato il *wallet*. Di talché, ove questo dovesse rompersi, essere perso o divenire inaccessibile, non sarebbe più possibile ricavare le chiavi private che permettano all'utente di accedere e utilizzare le criptovalute detenute[131]. Al riguardo, sebbene sia auspicabile l'esecuzione di *backup* volti a permettere all'utente il recupero dei dati persi, non può non osservarsi come anche siffatta operazione possa esporre l'utente ad accessi abusivi al proprio portafoglio da parte di terzi malintenzionati e alla conseguente sottrazione di criptovalute.

5.3 *I wallet hardware.*

A metà tra i portafogli *online* e i portafogli *mobili* troviamo i *wallet hardware*, che detengono tutte le informazioni relative alle criptovalute su appositi supporti fisici.

In questo caso è possibile distinguere portafogli che hanno natura *custodial* e portafogli dalle funzionalità più complesse, che comprendono anche la gestione delle criptovalute tramite la generazione di nuovi indirizzi e la firma delle transazioni operate.

---

[131] A ben vedere, i *software* più recenti permettono di ottenere le c.d. "seed" o "mnmonic seed" – di regola non scelto dall'utente ma generato dall'applicativo – che fungono da strumento di possibile recupero delle criptovalute al pari delle c.d. "parole segrete" utilizzate da diverse filiali di banca per il recupero delle proprie credenziali da parte degli utenti che le abbiano smarrite.

Tra i portafogli *custodial* troviamo i c.d. *paper wallet*, fogli di carta su cui vengono stampate le chiave private e l'indirizzo pubblico di riferimento (ad esempio, tramite QR Code). In questo caso, le transazioni in entrata potranno sempre essere effettuate senza l'utilizzo della chiave privata che, al contrario, sarà sempre necessaria nel caso di transazioni in uscita e che sarà detenuta su appositi supporti. In questo caso, il rischio è legato alla possibile perdita o divulgazione del *paper* con conseguente accessibilità alla chiave private e al portafoglio dell'utente. Le chiavi private possono essere detenute anche su chiavette USB realizzate per generare una chiave private o un indirizzo.

Ulteriore ipotesi dei *wallet hardware* è rappresentata da *pendrive USB* o da *calcolatrici* al cui interno viene inserita la chiave privata. Di regola, questi *wallet* permettono di effettuare transazioni tramite l'abbinamento a *client software* di tipo SPV, che consentono all'utente di gestire le proprie monete. In questo caso, le chiavi private non sono memorizzate sul dispositivo come avviene nell'ipotesi *custodial* appena descritta; l'USB sarebbe necessaria per perfezionare la transazione richiesta, ma senza che venga svelata la chiave privata ad essa associata.

6. *La qualificazione soggettiva delle criptovalute: user, miner, exchanger e wallet provider.*

Abbiamo visto come il Bitcoin e, più in generale, le criptovalute si inseriscono in una realtà decentralizzata tale per cui non vi è un utente superiore ad un altro, un amministratore con un ruolo preponderante rispetto agli altri utenti, ma è proprio dalla comunicazione e dall'interazione tra questi ultimi, soggetti indipendenti, che discende tutto il sistema delle criptovalute. Difatti, tutte le attività svolte dagli utenti all'interno del *network*, seppur diverse tra loro, sono fondamentali e necessarie al funzionamento dello stesso.

La qualificazione soggettiva del Bitcoin si basa su diverse categorie di utenti, con funzioni diverse, tutte fondamentali allo sviluppo del sistema: *user, miners, exchanger e wallet provider*[132].

Gli *user* sono le persone, fisiche e giuridiche che operano nel mercato delle valute virtuali, con fini di scambio o di detenzione, attorno ai quali si sviluppano e agiscono tutti gli altri attori criptovalutari.

È, oggi, possibile distinguere tre diverse modalità che permettono a un soggetto di ottenere criptovalute. La criptovaluta, infatti, può essere 1) acquistata con moneta avente corso legale; ricevuta quale mezzo di pagamento per la vendita di beni o servizi; 3) ottenuta quale regalo o ricompensa.

---

[132] G.P. ACCINNI, *op.cit.*, p. 4.

6.1 *L'acquisto di criptovaluta con moneta avente corso legale: gli exchanger.*

La prima modalità per ottenere criptovaluta vede protagonisti gli *exchanger*: questi soggetti, siano essi persone fisiche o giuridiche, permettono agli *user* di convertire le valute virtuali con moneta legale o metalli preziosi – e viceversa - attraverso l'utilizzo di piattaforme simili alle borse tradizionali.

Gli *exchanger* operanti nel mercato – oggi sottoposti, quantomeno a livello europeo, ad appositi obblighi di controllo e registrazione introdotti con la IV e V Direttiva antiriciclaggio – possono agire con modalità tra loro differenti, offrendo agli utenti diversi servizi.

Ad esempio, tra le piattaforme più conosciute di *exchange* vi era *Mt.Gox* che ha dichiarato bancarotta nel 2014, a seguito di un asserito furto di circa 850.000 Bitcoin, il cui valore, all'epoca, era di circa $450.000.000,00: su questa piattaforma *l'user* poteva direttamente acquistare Bitcoin, caricando nel proprio portafoglio elettronico moneta avente corso legale[133].

Sempre continuando con gli esempi, sulla piattaforma *Camp BX* è permesso agli *user* di fare trattative private con gli altri utenti, stipulando contratti di servizio in cui sono definiti i diritti di ogni parte così da limitare la responsabilità nello scambio[134]. Camp BX, in particolare, è divenuta nota per essere stata la prima piattaforma a permettere operazione di *marging trading* e di *short selling.*

Tra gli strumenti che permettono di ottenere criptovaluta versando moneta avente corso legale vi sono i c.d. "sportelli ATM". Trattasi di sportelli, appunto, in tutto e per tutto assimilabili, quanto a funzioni, agli ordinari ATM bancari, utilizzati quale strumento di scambio di criptovaluta.

A livello globale si conta la presenza di 37.677 ATM. L'installazione è, tuttavia, sempre più diffusa, in particolare negli USA, ove vi sono 31.498,00 sportelli, pari al 91,5% del totale[135].

Detti strumenti sono presenti anche sul territorio nazionale italiano, che oggi conta la presenza di 90 sportelli[136]. Vi sono diverse tipologie di ATM, ma tutti funzionano allo stesso modo, prevedendo la disponibilità sia di acquisto che di ritiro di criptovaluta. L'acquisto si perfezionerà con il semplice inserimento di moneta avente corso legale nell'apposito sportello, che verrà

---

[133] N.M. KAPLANOV, *op.cit.,* p. 122.
[134] *Ibidem.*
[135] Dato aggiornato alla data del 09.05.2024. Per comprendere la portata del fenomeno si pensi che alla data del 20.12.2023 gli USA contavano 27.779,00 ATM. In Europa sono presenti 1.623 ATM. A livello globale, si conta la presenza di 37.677 ATM. I dati sono consultabili al seguente link.
[136] Alla data del 09.05.2024, 54 sportelli sono stati installati nel Nord-Italia. Si rinvia al seguente link.

convertita per il valore corrispondente in criptovaluta e depositata sul *wallet provider* dell'*user* che ne sia dotato o, in alternativa, su un nuovo portafoglio elettronico creato nella medesima operazione.

Detti sportelli permettono anche di effettuare operazioni di criptovaluta utilizzando un *paper wallet:* sarà sufficiente che l'utente, mediante la lettura del QR code, mostri l'indirizzo del proprio portafoglio e digiti l'equivalente di criptovaluta che vuole vendere e convertire in valuta corrente.

Sul sito *CoinRadarMap*, inoltre, è possibile reperire i riferimenti delle attività commerciali che accettano pagamento in Bitcoin[137].

6.2 *La vendita di beni o servizi che prevedano il pagamento in criptovaluta, come regalo o come ricompensa.*

Vi sono poi attività che permettono di vendere beni o servizi dietro il corrispettivo in criptovaluta come avviene, ad esempio, per l'attività di *mining.*

Negli ultimi anni, inoltre, numerose sono le attività in circolazione che accettano il pagamento delle proprie prestazioni anche in criptovaluta: se nel giugno 2018, ad esempio, aveva fatto notizia uno studio di architettura di Milano che aveva pubblicamente dichiarato di accettare pagamenti in Bitcoin e altre criptovalute in cambio delle proprie prestazioni professionali, oggi detta scelta non rappresenta più una novità e, anzi, è favorita da alcune attività commerciali, non solo online, ma anche fisiche.

Vi sono poi i *wallet provider,* soggetti che forniscono agli *user* i portafogli elettronici (*e-wallet*) servendosi della creazione di applicazioni e programmi che consentano agli utenti di detenere, conservare e trasferire criptovalute. Tali soggetti non solo fanno le veci di quello che sarebbe un conto bancario in un sistema centralizzato, ma possono detenere anche le chiavi private del conto stesso così da agevolare le operazioni che avvengono tra gli *user* e gli *exchanger* o i venditori di merci e servizi, gestendo autonomamente le operazioni, come *broker.*

Non da ultimo, è possibile per ciascuno ricevere in regalo criptovalute o come ricompensa anche nell'ambito di giochi virtuali.

7. *La natura giuridica delle criptovalute: premesse.*

Una delle questioni più dibattute riguardo all'argomento trattato concerne la natura giuridica delle criptovalute.

---

[137] M. Porta, *ATM Bitcoin e negozi affiliati: dove sono e come funzionano,* giugno 2019, in www.cryptonomist.ch, reperibile al seguente link.

Ed invero, si tratta di un fenomeno che, sebbene fortemente sviluppato e noto da ormai quindici anni, non trova ancora una disciplina univoca, soprattutto in punto di qualificazione giuridica.

Ciò appare tanto più insolito se si considera che, in generale, operazioni di delimitazione dei fenomeni giuridici – consistente nell'individuazione delle relative caratteristiche, limiti, finalità – debbano necessariamente passare da una profonda comprensione e, quindi, da una qualificazione giuridica idonea ad orientare l'operatore nelle sue riflessioni, anche al fine di comprendere se la novità tecnologica considerata possa essere ascritta all'alveo di istituti già presenti nell'ordinamento di riferimento ovvero vi sia la necessità di idearne di nuovi *ad hoc*.

Al fine di meglio procedere è, anzitutto, necessario precisare come con il termine *criptovalute* si allude a un concetto distinto – ancorché spesso confuso – rispetto alla più ampia categoria delle *criptoattività* (o crypto-asset).

Più precisamente, è possibile evincere la definizione di *crypto-asset* traendo le mosse dalle definizioni rese da Autorità pubbliche internazionali – quali l'*European Securities and Markets* (ESMA), il *Financial Action Task Force* (FATF), ma anche il *Fondo monetario internazionale* (FMI), l'*European Banking Authority* (EBA) e la *European Central Bank* (BCE) – nell'ambito dei propri report.

È, dunque, possibile affermare che con il termine *criptoattività* si intende alludere, genericamente, a tutte le attività digitali basate sull'utilizzo della tecnologia a registro distribuito (più comunemente note come *distributed ledger technology,* DLT*[138])* – qual è la *blockchain*[139] – e sulla crittografia[140].

Rientrano in detta categoria le *valute crittografiche, le valute virtuali*, *le risorse virtuali* e i c.d. token *digitali*, che non sono emessi né garantiti da un'autorità centrale e che gli Stati dovrebbero considerare "*virtual asset as "*property*"", "*proceeds*", "*funds*", "*funds or other assets*", or other "*corresponding value"[141] e che costituiscono "a *digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes; do not include digital representations of fiat currencies, securities and other financial asset that are already covered elsewhere*"[142].

È di tutta evidenza, pertanto, come le criptovalute si pongano rispetto ai *crypto-asset* in un rapporto di *species* a *genus*, in cui sono ricompresi strumenti differenti tanto in punto di caratteristiche quanto di scopi e funzioni[143].

Ciò precisato, è necessario osservare che, sebbene a livello europeo e nazionale sia stata effettivamente elaborata – ancorché in termini strettamente settoriali – una definizione di *valuta virtuale*, essa appare vuota, generica e,

---

[138] Nell'ambito dell'ordinamento giuridico nazionale, ex art. 8-ter, comma 1, d.l. 14 dicembre 2018 n. 135, convertito con modificazioni dalla legge n. 12 del 2019. "Si definiscono "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili".

[139] È bene sottolineare come la *blockchain* rappresenta un particolare tipo di DLT. Nello specifico, si parla di blockchain perché le transazioni memorizzate sono raggruppate in una sequenza di "blocchi" collegati tra loro per via crittografica, creando così una registrazione in ordine cronologico e non modificabile di tutte le transazioni effettuate fino a quel momento. Vi sono altre soluzioni tecnologiche decentralizzate ma alternative alla DLT/blockchain quali, ad esempio, l'*online peer-to-peer* (P2P), o *user-matching* che consente a due controparti in qualità di utilizzatori (ad esempio in un rapporto di credito-debito) di interagire direttamente senza dover ricorrere alla presenza di un intermediario. Una buona sintesi in materia è contenuta in BANCA D'ITALIA, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, giugno 2022, pp. 5-10, reperibile al seguente link.

[140] *Cfr.* ESMA, *Advice to ESMA – Own Initiative Report on Initial Coin Offerings and Crypto-Assets (ESMA22-106-1338),* 19 ottobre 2018, p.3, reperibile al seguente link.

[141] Cfr. *FATF*, *Recommandations update 2012-2023* (update November 2023), p. 78, reperibile al seguente link.

[142] *Ivi,* p. 137.

[143] La dottrina intervenuta in materia, in assenza di una precisa tassonomia, ha ritenuto di potere distinguere le *criptoattività* in diverse categorie elaborate in considerazione della funzione economica dagli stessi svolti. In materia si rinvia a M. PIERRO, *Contributo all'individuazione della nozione di* crypto asset *e suoi riflessi nell'ordinamento tributario nazionale*, in *Rassegna Tributaria,* 3/2022*, p.* 574-611.

pertanto, non soddisfacente ai fini qualificatori, mostrandosi, piuttosto, quale mera descrizione delle caratteristiche relative alla tecnologia in parola.

In tal senso, l'art. 1, comma 1, lett. qq) d.lgs. 231/2007, in materia di antiriciclaggio e contrasto al finanziamento del terrorismo (art. 2, comma 1),– nel recepire la direttiva n. 2018/843 del Parlamento europeo e del Consiglio (c.d. V Direttiva antiriciclaggio) – definisce la *valuta virtuale* come «*rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*».

Detta definizione è stata, poi, sostanzialmente ripresa dal d.lgs. n. 184/2019 (c.d. *Decreto Antifrodi"*[144] – rilevante in materia penale – e nel D.M. 13 gennaio 2022 del Ministero dell'Economia e delle Finanze (MEF), sulla «*Modalità e tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria operatività sul territorio nazionale nonché forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia*»[145].

Sul punto, preme precisare come – diversamente da quanto osservato dall' EBA e dalla BCE, che hanno operato una differenziazione delle criptovalute basata sui *tipi* elaborati partendo dalle loro caratteristiche – sia il formante legislativo sia quello dottrinale hanno, sinora, preferito procedere valutando i diversi contesti in cui le valute virtuali vengono in rilievo, concentrandosi sugli scopi e le funzioni a cui assurgono in ciascuna disciplina, così rinunciando a una qualificazione unitaria del fenomeno considerato[146].

---

[144] L'art. 1, lett. d), *Decreto Antifrodi* definisce la *valuta virtuale* come «*una 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 che può essere trasferita, memorizzata e scambiata elettronicamente*».

[145] All'art. 1, comma 2, lett.f) il MEF ha qualificato la criptovaluta come «*la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*».

[146] M. PASSARETTA, *Le valute virtuali in una prospettiva di diritto privato: tra strumenti di pagamento, forme alternative di investimento e titoli impropri,* in S. CAPACCIOLI (a cura di), *op. cit.*, pp. 95 ss.

Siffatta impostazione appare, tuttavia, inefficiente a garantire una definizione univoca, idonea ad essere applicata trasversalmente in tutti i settori dell'ordinamento giuridico.

Vi è, allora, la necessità di riflettere circa la possibilità di ricondurre le valute virtuali nell'alveo di una – e una sola – delle già note categorie giuridiche, ricorrendo, in particolare, alle definizioni offerte della disciplina civilistica, cui è generalmente necessario ricorrere in mancanza – com'è nel caso di specie – di specifiche regole settoriali ovvero di ripensare l'impostazione sinora proposta a livello dottrinale, immaginando una categoria nuova e autonoma rispetto a quelle conosciute.

Appare, in tal senso, utile approfondire, tra le altre, le nozioni di *bene giuridico*, di *moneta – lato sensu* intesa *–mezzo di pagamento* e di *strumento finanziario* al fine di comprendere se e quale possa essere l'inquadramento sistematico delle criptovalute in ambito penalistico.

Solo così sarà, infatti, possibile, partendo dal dato normativo, nel pieno rispetto del *principio di legalità,* riflettere sull'eventuale rilevanza penale di condotte aventi ad oggetto le criptovalute nonché circa la riconducibilità di queste a fattispecie incriminatrici già tipizzate.

7.1 *Criptovaluta: valuta o moneta?*

Tra le ipotesi di qualificazione giuridica maggiormente dibattute dalla dottrina vi è quella della criptovaluta come *moneta* o *valuta*.

Ebbene, come detto, l'espressione *valute virtuali* allude ad un concetto vago, indefinito e a tratti ingannevole. Contrariamente, in ambito economico è possibile distinguere con chiarezza i concetti di *valuta* e di *moneta.*

Mentre con il termine *valuta* si fa riferimento unicamente alla *moneta avente corso legale*, cui quindi è assolutamente legata l'*efficacia solutoria* prevista dalla legge con riguardo a tutte le obbligazioni pecuniarie, il termine *moneta* comprende il più ampio e generale concetto di *unità di scambio generalmente accettata a livello globale*. È bene evidenziare, tuttavia, come la nozione di *moneta* sia, ancora oggi, fortemente discussa, vedendo contrapposte diverse teorie:

(a) La *teoria statalista*[147] si fonda sull'idea che gli Stati sovrani esercitano un potere sulla moneta in quanto essa viene non solo creata, ma

[147] Detta teoria affonda le sue radici all'inizio del XIX secolo. La sua teorizzazione ha raggiunto l'apice con gli studi condotti da G.F. KNAPP in *Staatliche Theorie des Geldes*, Leipzig, Duncker & Humblot, University of California, 1905. In tale opera, si sostenne per la prima volta l'importanza del ruolo dello Stato nel garantire il corso legale di una moneta, indipendentemente dalla presenza di supporti metallici o preziosi. Più di recente, si rinvia

anche garantita dallo Stato stesso o da autorità ad esso strettamente legate. In particolare, tale teoria fa leva, da un lato, sul *corso legale* della moneta – inteso come la sua capacità intrinseca di mezzo di estinzione delle obbligazioni –, dall'altro lato, sul *corso forzoso* della moneta stessa cui è strettamente connessa l'impossibilità per il creditore di rifiutarla come mezzo di pagamento, stante il «*potere liberatorio universale ipso iure*»[148] .

In tal senso, qualificare le criptovalute alla stregua di moneta avente *corso legale* – e, conseguentemente, riconoscere loro *corso forzoso* – significherebbe costringere un soggetto creditore ad accettare la valuta virtuale quale mezzo di pagamento per estinguere l'obbligazione contratta.

Si aggiunga, peraltro, che se la criptovaluta generalmente intesa è stata creata al fine di permettere alla collettività di beneficiare di una moneta assolutamente decentralizzata, sostanzialmente privata e, in quanto tale, sottratta ai controlli di un ente emittente centralizzato, della banca centrale o di specifici intermediari, non pare possibile ammettere che la stessa risponda ai canoni della *teoria statalista*, basata proprio sul controllo dello Stato.

Ne consegue l'impossibilità di riconoscere alla criptovaluta una natura valutaria.

L'esclusione della criptovaluta dalla funzione di *valuta* non esclude, tuttavia, di per sé, la possibilità di riconoscere alle valute virtuali le funzioni monetarie tipiche della *teoria economica*, che approccia alla definizione di moneta in modo funzionale.

(b) La *teoria economica* definisce la moneta in via più generale e pragmatica, individuandone

il contenuto sulla base di tre diverse funzioni: (i) *mezzo di scambio, (ii) unità di conto e (iii) riserva di valore*, intese, rispettivamente, come le capacità di *assurgere a mezzo di pagamento nelle transazioni commerciali, misurare il valore delle attività in cui viene utilizzata* e *di conservare il medesimo valore rispetto al proprio potere d'acquisto*.

Al riguardo, parte della dottrina ha ammesso la possibilità di riconoscere alle criptovalute la funzione di *mezzo di scambio* e *unità di conto*,

---

a G. LEMME, *Moneta scritturale e moneta elettronica*, Giappichelli, Torino 2003 e G.F. CAMPOBASSO, *Bancogiro e moneta scritturale,* Cacucci Editore, Bari, 1979.

148 G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema*, in *Diritto dell'Informazione e dell'informatica*, Giuffré, Milano, 3, 2015, p. 415.

negandole, tuttavia, la funzione di *riserva* o *stabilità di valore*[149]. Ed invero, è stato osservato come tendenzialmente le criptovalute – fatte salve poche eccezioni come, ad esempio, per la criptovaluta Tether – non sono ancorate a valute reali aventi *corso legale*; anzi, sono caratterizzate da una forte volatilità che incide, nel tempo, sul suo potere d'acquisto con conseguenti criticità in punto di convertibilità della criptovaluta in moneta scritturale. La volatilità delle criptovalute come Bitcoin, intesa come la variabilità nel tempo rispetto al potere di acquisto, rende difficile ammettere che tale criptovaluta svolga la funzione in parola, imprescindibile per applicarvi la disciplina della moneta. Sul punto è stato osservato come, in realtà, la volatilità non inciderebbe in alcun modo sulla funzione di stabilità di valore, stante la presenza nel mercato globale di monete ad alta volatilità. In tal senso deporrebbero, altresì, le teorie che negano la riserva di valore quale funzione propria della moneta, riconoscendone, unicamente, la natura di *mezzo di scambio* e di unità di conto[150].

Altra parte del formante dottrinale ha, invece, negato la possibilità di riconoscere alla criptovaluta le funzioni riconosciute alla moneta dalla teoria economica[151].

Quanto alla *funzione di pagamento* è stato, invero, osservato come la stessa coincida, quantomeno sostanzialmente, con il generale dovere – espresso, nel nostro ordinamento, dall'art. 1277 c.c. – di accettare quale mezzo di scambio moneta avente corso legale, secondo il valore nominale. Non è, invero, previsto a livello statale alcun obbligo di accettare pagamenti in criptovaluta: transazioni aventi ad oggetto valute virtuali hanno natura meramente volontaria.

La *funzione di unità di conto*, poi, intesa come unità capace di misurare in maniera *standard* il valore di flussi, di beni e servizi, non sarebbe soddisfatta dalla criptovaluta a causa delle incertezze del mercato dei cambi.

(c) In piena contrapposizione con le teorie analizzate si pone la c.d. *teoria sociologica*, che riconduce la moneta a un *fenomeno sociale*, quale

[149] N. VARDI, *Criptovalute e dintorni: alcune considerazioni sulla natura giuridica deI Bitcoin*, in *Diritto dell'Informazione e dell'Informatica,* in *Diritto dell'Informazione e dell'informatica*, Giuffré, Milano, 3, 2015*,* p. 443 ss.

[150] M. PASSARETTA, *op. cit.*, p. 102; B. INZITARI, *Le obbligazioni nel diritto civile degli affari*, Cedam, Padova, 2006, p. 471; E. QUADRI, *Specie di obbligazioni pecuniarie*, in P. RESCIGNO (diretto da), *Trattato di diritto privato,* Utet Giuridica, Torino, 1999, p. 435.

[151] R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* in Diritto dell'Informazione e dell'Informatica, fascicolo 1, Febbraio 2017, p. 27 ss.; F. CONSULICH, *Nella* wunderkammer *del legislatore penale contemporaneo:* monete virtuali *che causano* danni reali, in *Diritto Penale e Processo*, 2, 2022, p. 153 ss.

mezzo di scambio utilizzato dalla collettività. In tal senso, sarebbe possibile riconoscere alle criptovalute la natura di *moneta* e, più precisamente, di *valuta* ove la società civile riconoscesse loro la *funzione di pagamento*, in ragione della perdita di fiducia nei confronti dello Stato e della moneta emessa da detta autorità.

7.2 *Criptovaluta e moneta elettronica.*

Molti tra gli studiosi del fenomeno in esame hanno cercato di ricondurre il Bitcoin e, più in generale, le criptovalute all'alveo della *moneta elettronica*, così come definita dalla Direttiva europea 2009/110/CE (EMD2) recepita in Italia con il d.lgs. 16 aprile 2012 n .45, che ha modificato l'art. 1, comma 2, lett. h-ter) TUB.[152].

Sebbene le *valute virtuali* siano, sempre più, utilizzate quale mezzo di pagamento, pare doversi escludere la possibilità di ricomprendere le criptovalute nella categoria considerata.

L'art. 2 n. 2 della Direttiva EMD2 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 dietro ricevimento di fondi per effettuare operazioni di pagamento (…) e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica»*. A questo proposito, la criptovaluta ha, senz'altro, una natura *dematerializzata*, tale che il suo valore è memorizzato in via elettronica ed è accettato da persone fisiche e giuridiche diverse dagli emittenti presenti nell'*e-commerce*: non dobbiamo mai dimenticare la sua caratteristica principale, la decentralizzazione. Il problema che si pone a questo proposito riguarda, ancora una volta, l'*unità di conto* della criptovaluta: essa è completamente virtuale; il suo valore, come sottolineato, è altamente volatile; non vi è un valore intrinseco e perdipiù la base fiduciaria, su cui esso si basa, è davvero molto debole.

[152] Deve darsi atto che in data 28.06.2023 la Commissione europea ha presentato una proposta di Direttiva relativa ai servizi di pagamento e ai servizi di moneta elettronica nel mercato interno, in modifica della direttiva 98/26/CE e abrogazione delle direttive (UE) 2015/2366 e 2009/110/CE. Il pacchetto di riforme comprendente la terza Direttiva sui Servizi di Pagamento (PSD3), il Regolamento sui servizi di Pagamento (PSR) e il quadro per l'accesso ai dati finanziari (FIDA). In pari data, è stato pubblicato altresì il c.d. "Pacchetto Moneta Unica" relativo all'uso del denaro contante e all'euro digitale. Le novità normative sono destinate a sostituire sia la seconda direttiva sui servizi di pagamento (PSD2) sia la seconda direttiva sulla moneta elettronica (EMD2). Sarà, infatti, prevista una disciplina unitaria. La modifica potrebbe interessare anche la materia delle criptoattività.

È noto, poi, come gli studi intervenuti in materia di *moneta elettronica*, hanno riconosciuto a detto strumento di pagamento alcune caratteristiche *positive* e *negative*[153], la cui sussistenza è necessaria affinché un dato strumento possa essere ricondotto in detta categoria giuridica.

Tra le caratteristiche c.d. *positive* rientrano il *valore monetario*, la *memorizzazione elettronica*, l'*accettazione* potenziale da parte di soggetti diversi dall'emittente come mezzo di pagamento e l'emissione di una stringa di *bit* a rappresentazione dello scambio di denaro effettuato con l'emittente, al fine di consentire le operazioni di trasferimento, versamento e prelievo dei fondi.

Quanto, invece, alle condizioni *negative* in presenza delle quali è possibile parlare di *moneta elettronica* il riferimento è al fatto che il valore monetario non può essere utilizzabile unicamente in relazione ad alcuni servizi o per l'acquisto di beni informatici, come avviene invece per le criptovalute che hanno una portata di utilizzo – sebbene in fase di crescente sviluppo – ancora molto limitata.

Ed invero, la *moneta elettronica* rientra tra gli strumenti di pagamento così come definiti dalla Direttiva 2007/64/CE, seppur abrogata dalla successiva Direttiva 2015/2366/CE, di talché la sua spendibilità deve essere generalizzata e resa possibile rispetto ad una molteplicità di servizi o di beni: tale diffusione deve aversi non solo rispetto a ciò che è oggetto di pagamento, ma anche rispetto ai soggetti nei confronti dei quali il pagamento avviene.

Nella Direttiva EMD2, all'art. 1, comma 1 è inoltre stabilito che l'emissione di *moneta elettronica* è riservata unicamente agli Istituti bancari e postali, banche centrali nazionali e Banca Centrale Europea oltre che agli Istituti di moneta elettronica. A questo proposito, risulta superfluo, oltre che ripetitivo, ricordare che la criptovalute oggetto della ricerca si caratterizzano per la loro completa decentralizzazione.

Nell'analisi delle differenze che intercorrono tra la *moneta elettronica* e le criptovalute occorre, poi, far riferimento all'art. 11, comma II, della Direttiva 2009/110/CE che specifica che *«Gli Stati membri assicurano che, su richiesta del detentore di moneta elettronica, gli emittenti di moneta elettronica rimborsino, in qualsiasi momento e al valore nominale, il valore monetario della moneta elettronica detenuta»*[154]: a questo proposito sottolineiamo che una

[153] N. MANCINI, *Bitcoin: rischi e difficoltà normative*, in Banca Impresa Società, Il Mulino – Riviste *Web*, 1, aprile 2016, p.121, in www.rivisteweb.it.

[154] Quanto disposto all'art. 11 della Direttiva, viene ribadito anche nel Considerando 18 della EMD2: "Occorre che la moneta elettronica sia rimborsabile per salvaguardare la fiducia del detentore di detta moneta. (…) Il rimborso dovrebbe essere sempre possibile, in ogni momento, al valore nominale senza che sia possibile stabilire una soglia minima per il rimborso. In generale il rimborso dovrebbe essere concesso gratuitamente. Tuttavia,

delle caratteristiche proprie delle criptovalute e, in particolare di Bitcoin, tra le favorite dalla maggior parte degli utenti che ne usufruiscono in malafede, è proprio l'irreversibilità delle sue transazioni dovuta alle caratteristiche della *blockchain* come sopra descritte. Se, infatti, la *moneta elettronica* si compone di una serie di *bit* cui corrisponde il valore del denaro in possesso dell'utente e, pertanto, è sempre rimborsabile, le operazioni in criptovaluta basata su *blockchain* non potranno mai essere annullate, proprio perché irreversibili.

Per questi motivi, parte della dottrina si è fortemente opposta a detta qualificazione e ha, così, escluso la possibilità di applicare la direttiva 2007/64/CE anche alle criptovalute, rilevando come la richiamata disciplina – in uno con il citato art. 2, n. 2 della direttiva 2009/110/CE – riguardi unicamente la *moneta avente corso legale*, indipendentemente dal fatto che questa si manifesti sotto forma di banconote, di moneta scritturale o di moneta elettronica[155].

Altro orientamento, tuttavia, ha, al contrario, ammesso la riconducibilità delle *criptovalute* all'alveo delle *monete elettroniche*, richiamandosi alla già citata Direttiva 2007/64/CE[156] in tema di *servizi di pagamento*.

Chi ha sostenuto tale tesi ha ritenuto di potere qualificare la criptovaluta, nel caso di specie il Bitcoin, quale *strumento di pagamento* definito dall'art. 1, comma 1, lett. *s)* nel d.lgs. 11/10 come *«qualsiasi dispositivo personalizzato e/o insieme di procedure concordate tra l'utilizzatore e il prestatore di servizi di pagamento e di cui l'utilizzatore di servizi di pagamento si avvale per impartire un ordine di pagamento».* Siffatta definizione si basa su *un accordo tra parti interessate*; pertanto, in quest'ottica, sarebbe possibile ammettere la natura della criptovaluta come *mezzo di pagamento*, così come pensato e definito dalla Direttiva in esame.

---

in casi debitamente specificati nella presente direttiva, dovrebbe essere possibile richiedere una commissione proporzionata e basata sui costi, lasciando impregiudicata la normativa nazionale in materia fiscale o sociale o eventuali obblighi imposti all'emittente di moneta elettronica da altre pertinenti disposizioni comunitarie o nazionali, come le norme antiriciclaggio e in materia di finanziamento del terrorismo, eventuali provvedimenti di congelamento dei fondi o altre misure specifiche legate alla prevenzione e alla lotta alla criminalità".

[155] F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti. Lo statuto delle valute virtuali: le discipline e i controlli, in Archivio Diritto penale contemporaneo*, 10, 2018, pp. 21 ss., reperibile al seguente link.

[156] Abrogata dalla Direttiva 2015/2366, soprannominata "PSD2".

7.3 *Le criptovalute come strumento di investimento: strumenti finanziari, valori mobiliari e prodotti finanziari.*

Nonostante la consapevolezza che la maggior parte degli utenti, sfruttando le fluttuazioni del tasso di cambio con la moneta avente corso legale, detiene, acquista e scambia criptovalute al fine di ricavarne un profitto, si è a lungo dubitato – e, a ben vedere, si dubita tuttora –che le criptovalute potessero essere qualificate alla stregua di *strumento di investimento – lato sensu* inteso – con conseguente applicabilità della relativa disciplina[157].

7.3.1 *L'orientamento negazionista.*

Parte della dottrina ha a lungo negato la possibilità di riconoscere alle valute virtuali una natura finanziaria. Siffatta presa di posizione si fonda sull' art. 1, comma 2, Testo Unico Finanza (TUF).

La norma richiamata, in primo luogo, nel fornire la definizione di *strumenti finanziari*[158], rinvia all'elenco contenuto nella Sezione C, allegato 1 TUF. Si tratta di un elenco tradizionalmente considerato tipico, tassativo e chiuso, al cui interno non figurano le criptovalute.

In secondo luogo, il legislatore ha esplicitamente escluso la possibilità di qualificare i *mezzi di pagamento* alla stregua di *strumenti finanziari*. In tal senso, le criptovalute, in quanto *strumenti di pagamento*, non potrebbero rientrare nella categoria in analisi[159].

Si osserva, al riguardo, come l'attività svolta dalle piattaforme *exchange* e di *portafogli digitali* di criptovalute non possa essere assimilata ai servizi di

[157] I servizi di investimento sono attività volte ad impiegare i risparmi in attività finanziarie. Tali attività sono fornite dagli intermediari, quindi Banche e SIM ed hanno sempre per oggetto strumenti finanziari. Tali attività sono definite nella Direttiva MIFID (2004/39/CE). Si rinvia a M. GENTILE, F. SCALESE, V. CAIVANO, S. DI ROCCO, *Principali tendenze in tema di investimenti sostenibili e criptoattività,* in www.consob.it, reperibile al seguente link.

[158] Gli strumenti finanziari sono particolari *prodotti finanziari e sono costituiti da azioni, obbligazioni, altri titoli di debito, titoli di Stato, altri strumenti finanziari negoziabili sul mercato dei capitali, quote di fondi comuni d'investimento, altri titoli negoziati sul mercato dei capitali e sul mercato monetario, strumenti finanziari derivati. Tra gli strumenti finanziari rientrano* azioni, obbligazioni, titoli di Stato, quote di fondi, contratti e strumenti derivati etc., quindi gli strumenti con cui è possibile effettuare investimenti di natura finanziaria. Questi sono definiti dall'art. 1, comma II, TUF, che rinvia alla Sezione C dell'Allegato I.

[159] P. CARRIÈRE, *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, Fascicolo I, Sezione I, pp.134-135, in www.dirittobancario.it, reperibile al seguente link.

negoziazione *per conto proprio* o *per conto dei clienti* aventi ad oggetto gli strumenti finanziari[160].

7.3.2 *Le criptovalute come strumento di investimento.*

Nonostante le resistenze manifestate da parte della dottrina più tradizionalista, negli anni si è sviluppato un secondo orientamento che, ancorché inizialmente minoritario, ha sempre ammesso la funzionalità finanziaria propria delle criptovalute, ancorché riconducendola a categoria diversa dagli *strumenti finanziari* in senso stretto.

Si tratta, tuttavia, di orientamento non univoco, al cui interno è possibile distinguere tre diverse correnti di pensiero, tra chi ritiene che le criptovalute possano essere qualificate alla stregua di *valore mobiliare*, chi di *prodotto finanziario* e chi propone una valutazione casistica, che tenga conto delle diverse situazioni in cui le valute virtuali vengono in rilievo.

7.3.2.1 *Valori mobiliari.*

È stato osservato come, a determinate condizioni, le criptovalute potrebbero assurgere a *valore mobiliare.*

L'art. 1, comma 1 bis, TUF riconduce alla categoria in esame i "valori che possano essere negoziati nel mercato di capitali". Si tratta di una categoria aperta, non tipica e non tassativa, come suggerisce la formulazione esemplificativa della norma. In tal senso, potrebbero essere qualificate alla stregua di *valori mobiliari* unicamente le criptovalute che, per le caratteristiche intrinseche, possano essere *negoziate*[161].

7.3.2.2 *Prodotti finanziari.*

Per primo Emilio Girino partendo dalla nozione di *prodotto finanziario* contenuta nell'art. 1 lett. u) TUF – e, più precisamente, riferendosi alla categoria di "ogni altra forma di investimento di natura finanziaria" considerata da autorevole dottrina una categoria aperta[162] – ha ritenuto che le criptovalute possano essere considerate strumenti finanziari c.d. *atipici.*

La genericità della definizione di *prodotti finanziari* sarebbe stata, infatti, ricercata e voluta dal legislatore per fare fronte alla "mutevolezza e la

[160] *Ivi,* p. 136.
[161] *Ivi*, p. 141.
[162] F. ANNUNZIATA, *Commento sub art. 94*, in *Commentario Marchetti-Bianchi,* Giuffrè, Milano, 1989; R. COSTI, *Il mercato mobiliare*, Giappichelli, Torino, 2010.

tendenza alla fuga del fenomeno finanziario, per sua natura incline a cercare riparo negli inevitabili vuoti normativi del sistema"[163].

La definizione verterebbe, così, sullo scopo e sulla funzione economica tipici degli strumenti finanziari *sub specie* di *prodotti finanziari.*

In tal senso, la prassi avrebbe permesso di individuare cinque elementi in presenza dei quali sarebbe possibile fare riferimento alla categoria dei *prodotti finanziari*: 1) impiego di capitale; 2) aspettativa di un rendimento di natura finanziaria; 3) assunzione di un rischio direttamente connesso e correlato all'impiego di capitale; 4) prevalenza del connotato finanziario rispetto a quello di godere e disporre del bene acquisito con l'operazione; 5) effettiva e predeterminata promessa, all'atto di instaurazione del rapporto contrattuale, di un rendimento collegato alla *res*. L'autore, partendo dal costante orientamento della Consob in materia, ha rilevato come "investire capitale, attendendosi un ritorno finanziario e assumendosi il rischio di una perdita è l'essenza di qualsivoglia investimento, sia esso incarnato da uno strumento finanziario tipico sia esso avvolto in un involucro innominato"[164].

A fronte dell'applicazione di detti criteri si sono sviluppate due diverse e contrapposte opinioni in materia: Girino ha ritenuto, infatti, di potere riconoscere alla criptovaluta una "oggettiva funzionalità finanziaria[165]".

Al contrario, Carrière, nel valorizzare un approccio funzionale che guarda alla causa concreta del negozio sottostante, ha rilevato come, al fine di qualificare la criptovaluta alla stregua di *prodotto finanziario,* dovrebbe guardarsi, di volta in volta, allo schema negoziale sottostante. Ha, sul punto, osservato come "un'operazione avente ad oggetto una particolare *asset class* non riconducibile ex se agli "strumenti finanziari", può assumere le caratteristiche di offerta di un "prodotto finanziario" solo se siano esplicitamente previsti, anche tramite contratti collegati, ulteriori elementi come, ad esempio, promesse di rendimento e di realizzazione di profitti, obblighi di riacquisto, ovvero vincoli al godimento del bene"[166].

La qualificazione in termini di *prodotti finanziario* determina l'applicabilità alle criptovalute della disciplina prevista per l'offerta al pubblico. Di talché, tanto il proponente quanto l'intermediario dell'operazione finanziaria avente ad oggetto criptovalute dovranno osservare, conformemente al disposto degli artt. 32 e 94 ss. TUF, sia il Regolamento con cui la Consob

---

[163] E. GIRINO, *Criptovalute: un problema di legalità funzionale*, in *Rivista di Diritto Bancario*, 4, 2018, p.760, in www.dirittobancario.it, reperibile al seguente link.
[164] *Ibidem.*
[165] *Ivi,* p. 768.
[166] P. CARRIÈRE, *op.cit.*, pp- 160-161. sicuramente qualificabili alla stregua di *prodotti finanziari* i c.d. *securitu token*.

riserva tali attività solo ai soggetti abilitati sia gli obblighi di trasparenza e di informazione nei confronti degli investitori.

In mancanza, potrebbero venire in rilievo le violazioni dettate, rispettivamente, dagli artt. 166 TUF e 94 TUF.

7.3.2.3 *Il formante giurisprudenziale.*

L'orientamento dottrinale inizialmente minoritario è stato, successivamente, condiviso anche da parte della giurisprudenza che, intervenuta principalmente in materia penalistica rispetto ad ipotesi di abusivismo finanziario, ha sempre qualificato le criptovalute, *sub specie* Bitcoin, alla stregua di *prodotto finanziario*. Non risultano, al contrario, pronunce, volte ad indagare la natura, ad esempio, di moneta, di valuta o di bene delle criptovalute.

Per primo il Tribunale Civile di Verona, con la pronuncia n. 195 del 24 gennaio 2017[167], ha definito le criptovalute "uno strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni *online*", rilevando come tra le parti processuali vi fosse stato un rapporto di intermediazione consistito in una "prestazione di servizi effettuate a titolo oneroso", così ricavando la natura contrattuale dell'operazione di vendita sottoposta all'attenzione della Corte, da qualificare come "attività professionale di prestazione di servizi a titolo oneroso, svolta in favore di consumatori" qualificabile alla stregua di "un'offerta al pubblico di prodotti finanziari o di servizi di investimento in valori mobiliari".

Recentemente, è intervenuta la giurisprudenza penale di legittimità, riconoscendo la possibilità che le criptovalute siano qualificate quali *prodotti finanziari* e negando le teorie dottrinali sino ad allora sviluppatesi, orientate alla negazione della natura finanziaria della criptovaluta. Ed invero, sebbene l'art. 1, comma 2, TUF (nella formulazione all'epoca vigente) non contemplasse la possibilità che strumenti finanziari fossero emessi con tecnologia a registro distribuito – quali sono le criptovalute –, si riteneva possibile condividere la teoria dottrinale espressa da Girino, riconducendo le criptovalute all'ipotesi dettata dall'art. 1 lett. u) TUF, ampliandone la portata normativa.

---

[167] Oggetto della controversia era un contratto di *platform exchange* concluso tra le parti al fine di acquistare valuta virtuale dietro il pagamento di moneta avente corso legale. L'acquirente citava la società di cambiavalute virtuale eccependo la nullità del contratto per violazione del Codice del Consumo, stante la mancata forma scritta del contratto e dell'informativa precontrattuale prevista dall'art. 67 Cod. Consumo. Per un commento alla pronuncia si rinvia a M. PASSARETTA, *Bitcoin: il leading case italiano*, in *Banca borsa e titoli di credito,* Giuffré, 4, 2017, p. 471.

È così che con una prima pronuncia in materia, la n. 26807/2020, la Cassazione penale ha affermato che la vendita *online* di valuta virtuale pubblicizzata quale forma di investimento per i risparmiatori, offrendo loro informazioni circa la redditività dell'iniziativa, deve essere considerata soggetta alla normativa del TUF e, in particolare, agli artt. 91 ss. TUF. In questo caso, la decisione ha preso in considerazione le modalità della condotta sollecitatoria riferita dal proponente all'investitore.

A medesima conclusione è successivamente giunta la Suprema Corte con la pronuncia n. 44337/2022, che ha evidenziato come la criptovaluta – anche nel caso di specie il Bitcoin – possa essere qualificata alla stregua di *prodotto finanziario* ogniqualvolta sia acquistata con *finalità di investimento*, insistendo, dunque, sulla valorizzazione della *causa concreta* dell'operazione di acquisto. Con detto pronunciamento, in particolare, è stata esclusa la possibilità che la valuta virtuale potesse essere qualificata alla stregua di *strumento finanziario* unicamente in presenza di specifiche modalità sollecitatorie rivolte al possibile investitore, riconoscendo maggiore spazio alle *finalità* dell'acquisto, indipendentemente dalle modalità con cui lo stesso si è svolto. In tal senso, deporrebbe, peraltro, la definizione di moneta virtuale introdotta con la V direttiva antiriciclaggio (2018/843/UE) e successivamente recepita a livello nazionale dal d.lgs. 125/2019 che, anzi, ne ha ampliato le maglie includendo le *finalità di investimento*[168].

Dette conclusioni sono state il frutto di una lettura sistematica della disciplina all'epoca vigente in materia di criptovalute a livello europeo e nazionale e, in particolar modo, della disciplina antiriciclaggio contenuta nella IV e nella V Direttiva[169].

È, tuttavia, necessario come con D.L. n. 25/2023, convertito con modificazioni dalla L. 52/2023, ha modificato l'art. 1, comma 2, TUF ammettendo la possibilità che gli strumenti finanziari contenuti nell' Allegato I, Sezione C del TUF possano essere emessi da tecnologia a registro distribuito, così aprendo alla qualificazione giuridica delle criptovalute alla stregua di *strumenti finanziari.*

---

[168] L'art. 2, lett. qq, d.lgs. 231/2007, come modificato dal d.lgs. 125/2019, oggi vigente, definisce la valuta virtuale quale "rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente".

[169] Vedremo come, in realtà, il richiamo alla definizione di valuta virtuale dettata dalla Quinta Direttiva Antiriciclaggio possa indurre ad escludere la sussumibilità delle criptovalute alla stregua di *strumento finanziario*. F. DALAITI, *Cripto-valute e abusivismo finanziario: cripto analogia o interpretazione estensiva?*, in *Sistema Penale, 1, 2021,* pp. 65-70. Si rinvia a Capitolo III, § 5.3.1. *La tutela del mercato finanziario criptovalutario.*

7.3.3 *La categoria degli strumenti finanziari alla luce del regolamento MICA.*

L'incertezza giuridica sorta in materia *dovrebbe* trovare risposta nel Regolamento UE 2023/1114 "Market in Crypto Asset" (c.d. MiCA), approvato in via definitiva dal Parlamento Europeo il 31 maggio 2023 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 9 giugno 2023.

All'art. 1 del MiCA viene definito l'ambito di applicazione del Regolamento, che mira a stabilire "requisiti uniformi per l'offerta al pubblico e l'ammissione alla negoziazione su una piattaforma di negoziazione di cripto-attività *diverse* dagli *utility token*[170], *token collegati ad attività*[171] dai *token* di moneta elettronica[172], nonché i requisiti per i prestatori di servizi per le criptoattività".

Il regolamento, innanzitutto, all'art. 2, introduce la definizione di *cripto-attività* come *una rappresentazione digitale di un valore o di un diiritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga.*

Inoltre, nell'ammettere la possibilità di ricondurre le criptovalute alla nozione di *strumento finanziario*, il regolamento esclude dalla disciplina del regolamento MiCA tutte le cripto-attività rientranti nella nozione di strumento finanziario ai sensi della direttiva 2014/65/UE (c.d. MIFID 2).

Tuttavia, lungi dal definire specificamente il campo di applicazione della MiFID 2 in materia di valute virtuali, al considerando n. 14 incarica l'ESMA "di emanare orientamenti sui criteri e sulle condizioni per la qualificazione delle cripto-attività come strumenti finanziari", "al fine di garantire una chiara distinzione tra, da un lato, le cripto-attività disciplinate dal presente regolamento e, dall'altro, gli strumenti finanziari".

---

[170] Gli *utility token* sono un tipo di criptovaluta utilizzata per accedere a un particolare prodotto o servizio all'interno di un ecosistema basato sulla blockchain. Non sono progettati per essere una valuta o una riserva di valore, ma piuttosto per fornire utilità agli utenti della piattaforma. Ne costituisce un esempio Ethereum, che è utilizzato per pagare le c.d. *gas fee* sulla blockchain di Ethereum, vale a dire le commissioni sulla transazione di ETH o per l'esecuzione di uno *smart contact*. Gli utenti pagano questa tariffa in ETH e i nodi della rete guadagnano una frazione delle tariffe per convalidare le transazioni tramite *Proof of Stake* (PoS).

[171] Si intende un *crypto-asset* diverso da un token di moneta elettronica volto a mantenere un valore stabile facendo riferimento a un altro valore o diritto o a una combinazione dei due, inclusa la possibilità che faccia riferimento a valute ufficiali (cosiddette fiduciarie).

[172] Si intende *un crypto-asset* il cui scopo principale è quello di essere utilizzato come mezzo di scambio e che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale – fiduciaria.

Non resta, dunque, che attendere le determinazioni dell'ESMA per comprendere presupposti e termini della disciplina in materia.

7.4 *Ulteriori definizioni della natura giuridica della criptovaluta.*

Nel continuo interrogarsi sulla natura giuridica da attribuirsi ai Bitcoin e, più in generale, alle criptovalute diverse sono state le ulteriori soluzioni proposte dagli studiosi.

7.4.1 *Criptovalute, beni e cose.*

Nel contesto descritto, parte del dibattito dottrinale e giurisprudenziale ha riguardato la discussione circa la possibilità di ricondurre le criptovalute alla categoria giuridica dei *beni*.

Ed invero, muovendo dall'art. 810 c.c., a mente del quale *sono beni le cose che possono formare oggetto di diritti*, ci si è interrogati sulla capacità della definizione richiamata di accogliere anche gli strumenti propri della criptoattività e, in particolare, le criptovalute.

Sebbene una siffatta ricostruzione sia stata accolta da una certa parte della giurisprudenza[173] , il dibattito dottrinale rimane piuttosto acceso e incerto dividendosi tra chi, sposando una concezione più tradizionalista di "bene" nega la possibilità di ricondurre alla categoria dei *beni* e chi, al contrario, accoglie detta ipotesi proponendo una concezione meno restrittiva e più flessibile del dettato dell'art. 810 c.c.

Un primo orientamento ha rilevato come, tradizionalmente, il nostro ordinamento si fondi sul *principio del numerus clausus* dei diritti ex art. 810 c.c., la cui definizione rappresenta una precisa scelta legislativa, dovendosi, in tal senso, affermare tanto la *tipicità* quanto la *tassatività* dei beni giuridici[174].

---

[173] In questo senso vedi Trib. Firenze, Sez. Fallimentare, sent.18/2019 che, per prima, a livello giurisprudenziale ha condotto le criptovalute alla nozione di *bene*.

[174] In materia, fondamentale ZENO-ZENCOVICH, voce "Cosa" in *Dig. Disc. Priv. Sez. Civ.*, Torino, UTET, 1989, pp.438, ss. Richiamato anche in R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto dell'Informazione e dell'Informatica*, 1, 2017, p. 27. L'autore ha in detta sede ricordato come «*la dottrina c.d. formalistica (M. COSTANTINO, I beni in generale, in Trattato di dir. priv. diretto da Rescigno, vol. VII, Torino, 1982, p.13) osserva che sono beni solo quelle entità o risorse che l'ordinamento giuridico qualifica come tali. I beni giuridici sono, perciò,* numerus clausus *perché solo l'ordinamento giuridico può qualificare delle entità come beni giuridici. Il giudice, perciò, non può creare nuovi beni (A. Belfiore, I beni e le forme giuridiche di appartenenza: a proposito di una recente indagine, in Riv. Crit. Dir. Priv., 1983, pp. 855 e ss.). Questo potere sulle entità del modo esterno, attribuito dall'ordinamento giuridico, è la situazione giuridica soggettiva attiva. Quindi la teoria dei beni si traduce in realtà in una teoria delle situazioni giuridiche soggettive attive, perché il bene non esiste giuridicamente se l'ordinamento non prevede*

In assenza di esplicito riconoscimento legislativo dovrebbe, pertanto, escludersi la possibilità di annoverare le criptovalute tra *le cose che possono formare oggetto di diritti*. Detto orientamento, peraltro, osserva come il nostro ordinamento con il termine *bene* faccia riferimento ad una nozione fortemente legata alla *materialità* della cosa con conseguente impossibilità di riconoscere detta natura alla criptovaluta, evidentemente caratterizzata da immaterialità[175]. Il fatto che le criptovalute, seppur nel possesso di un soggetto della rete definito *user*, rimangano sempre e comunque *cose immateriali* contenute a loro volta in una *rete immateriale*, escluderebbe le stesse dalla definizione in analisi.

Altra parte della dottrina, tuttavia, ha inteso accogliere una nozione più flessibile di *bene*, accogliendo la possibilità di accogliere le *criptovalute* in detta categoria, sulla base di diverse considerazioni.

Tra questi, infatti, c'è chi ha rilevato come, a ben vedere, le criptovalute, in quanto *insieme di informazioni*, siano espressione "di una posizione giuridica su un bene o una pretesa verso un determinato soggetto"[176], potendo, pertanto, formare oggetto di diritti e, quindi, rientrare nella categoria in esame. Inoltre, la materialità delle criptovalute, lungi dal potere essere negata, dovrebbe essere

---

su di esso una situazione giuridica soggettiva attiva. Questo indirizzo a sua volta si distingue in due filoni. Secondo un primo filone, qualunque situazione giuridica soggettiva attiva funge da criterio di qualificazione dell'entità come bene e, quindi, è sufficiente che una norma rechi l'attribuzione fondamentale ad un soggetto, di una situazione giuridica soggettiva attiva, anche se relativa (diritto di credito), perché quell'entità assurga a dignità giuridica di bene (G. Santini, Commercio e servizi, cit., p. 419; V. ZENO-ZENCOVICH, voce *Cosa in Dig. disc. priv. sez. civ., vol. IV, Torino, 1989, p. 446). Secondo altro filone, invece, i diritti di credito non costituiscono criteri di qualificazione delle risorse come beni, perché i diritti di credito risolvono soltanto problemi di circolazione della ricchezza ma non di attribuzione a titolo originario della ricchezza. Occorre, quindi, che vi sia qualche norma che rechi un'attribuzione fondamentale originaria di un'entità ad un soggetto e ciò avviene attraverso l'attribuzione di un potere che si presenti come assoluto e, cioè, erga omnes. In conclusione, solo l'esistenza di una situazione giuridica assoluta su una risorsa del mondo esterno per effetto di una norma dell'ordinamento determina la qualificazione giuridica di quella entità come bene giuridico (Scozzafava, I beni e le forme giuridiche di appartenenza, Milano, 1982, p. 422)*». Cfr., tra gli altri, R. VIGORITA – F. ILACQUA, "*Profili giuridici del Bitcoin: la moneta diventa digitale*", in www.iurisprudentes.it , reperibile al seguente link.

[175] P. IEMMA, et alt., *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute differenze*, in Approfondimenti, 2018, in www.dirittobancario.it, p.12; R. BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* in *Diritto dell'Informazione e dell'Informatica*, 1, 2017, p. 30; R. SCALIA, *Riflessioni su alcuni temi controversi sulla disciplina IVA delle c.d. criptovalute*, in *Giurisprudenza delle imposte,* 1, 2020, pp. 24 ss., in www.assonime.it, reperibile al seguente link.

[176] C. SANDEI, *Le* Initial Coin Offering *nel prisma dell'ordinamento finanziario*, in *Riv. dir. civ.*, CEDAM, Padova, 2, 2020, pp. 391, ss.

ricercata nei supporti in cui le valute virtuali vengono detenute (PC, chiavette USB, hardware…).

Più di recente, è stato osservato – ancorché rispetto ai *cryptoasset lato sensu* intesi – che poiché "le cripto attività costituiscono (…) oggetto di un diritto che attribuisce, a chi ne ha la diponibilità giuridica, di utilizzarle - lo si ripete - come mezzo di scambio, oppure con finalità di investimento, o per fruire di un servizio o per "consumare" un altro bene digitale, o ancora per disporre in via esclusiva di un bene, virtuale o reale, unico (…) si può dunque ragionevolmente ritenere che le cripto attività sono cose – nell'accezione ampia che comprende anche le entità incorporali e i diritti l le quali essendo oggetto di diritti, devono essere considerati beni ai sensi dell'art. 810 del Codice civile. Beni a cui dovrà essere applicata la disciplina ad esse riservata in ogni settore dell'ordinamento giuridico"[177].

Siffatte considerazioni muovono da due diversi ordini di considerazioni, uno più teorico l'altro più pratico e basato su rilievi comparatistici.

In primo luogo, da un punto di vista prettamente teorico, è stato possibile giungere a dette conclusioni facendo proprie le considerazioni di quella parte della dottrina civilistica mostratasi maggiormente aperta a riconoscere alla norma una mutevolezza dettata dall'evoluzione storica e tecnologica che, inevitabilmente, incide sull'ordinamento giuridico, in quanto tale incline a rispondere ai mutamenti sociali ed economici[178] con conseguente apertura ai c.d. *beni immateriali*[179]. Si è osservato, infatti, come "è ben possibile

---

[177] M. PIERRO, *Contributo all'individuazione della nozione di* crypto asset*, op. cit*., pp. 590-591.

[178] T. ASCARELLI, *Ordinamento giuridico e processo economico*, in *Studi in onore di Lorenzo Mossa,* I, CEDAM, Padova, 1961, pp. 51 ss.

[179] Per una ricostruzione dell'evoluzione dottrinale sul punto si rinvia a M. PIERRO, *Contributo all'individuazione della nozione di* crypto asset*, op. cit*., pp. 590 – 592 nella parte in cui ricostruisce il dibattito in materia osservando che: "*Nell'ambito degli studi civilistici è stato messo in dubbio che gli asset immateriali - da alcuni considerati non cose e di conseguenza ('non beni" in senso giuridico, e da altri invece considerati "cose" - possano essere oggetto del diritto di proprietà e di altri diritti reali i quali, per le loro caratteristiche strutturali, risulterebbero ad essi inapplicabili. Precisato che il ricorso alla nozione di proprietà per i beni immateriali e di regola operato in modo improprio, ed essenzialmente allo scopo di identificare la "titolarità" o "l'appartenenza' del bene ad un soggetto, si replicava che è lo stesso legislatore a prevedere che le entità immateriali - quali sono, senza alcun dubbio, il diritto di credito e l'azienda (art. 1265 e art. 2025 del Codice civile art. 2557 e art. 2561) - possano essere oggetto di diritti reali (in particolare del diritto di usufrutto). Non solo. Si osservava che il diritto di proprietà, apparso inadeguato ad esprimere "le modalità d'uso" di beni diversi da quelli materiali, aveva subito nel tempo una costante estensione tale da indurre a ricomprendere sotto il medesimo schema giuridico nuove forme di appropriazione della ricchezza. Di modo si giungeva ad affermare che il concetto di appartenenza - che esprime la relazione tra il soggetto e le "cose" - trovava espressione nella titolarità non solo del diritto di proprietà*

che il diritto concepito come interesse ed utilità, possa formare a sua volta obietto di altri diritti: utilità in senso giuridico può dare sia una cosa corporale che un diritto”[180], in quanto tale non materiale.

---

o di altri diritti reali minori (quid minoris rispetto ai diritti o alle situazioni giuridiche soggettive che lo possono rappresentare), ma anche di diritti relativi».
Prendeva dunque piede la consapevolezza che i diritti a cui l'art. 810 Codice civile fa riferimento, in assenza di una espressa indicazione contraria, sono oltre a quelli reali anche quelli di credito. Ritenere infatti che la norma definitoria, in ragione della sua collocazione sistematica all'interno del codice, intendeva richiamare solo i diritti reali avrebbe dovuto indurre l'interprete a concludere che i diritti relativi non potevano (e non possono) mai avere ad oggetto "cose" - da intendersi solo come entità materiali - con la conseguenza che le entità materiali allorché costituiscono oggetto (mediato) di diritti di credito non sono beni in senso giuridico. Il che naturalmente non era e non è accettabile. Il bene è da considerare tale qualunque sia il diritto di cui è oggetto. Queste considerazioni avevano consentito innanzitutto di ritenere superate - come peraltro molti le ritenevano allora e a maggior ragione oggi - le argomentazioni di quella parte della dottrina che escludeva che gli intangibile asset *potessero essere oggetto di diritti reali, sul presupposto che la titolarità di diritti di esclusiva su una risorsa incorporale dovesse essere espressamente riconosciuta dall'ordinamento, state l'esistenza del principio di tipicità dei* beni immaterialis. *Ma avevano anche permesso di considerare beni in senso giuridico, in base all'art. 810 del Codice civile, tutte le entità, materiali e immateriali, oggetto di un qualsiasi diritto, sia esso reale o relativo. Ma non è tutto. Si era infatti osservato che tra le entità intangibili, percepibili solo intellettualmente, dovevano essere di regola ricondotti anche i diritti, tanto che ci si era domandato se anche questi, allorché oggetto di altri diritti, dovessero essere considerati beni in senso giuridico. L'argomento è stato oggetto di diffusa e mai conclusa riflessione giuridica. ca. Per brevità - rinviando ad altra sedes per eventuali approfondimenti - si segnala che vi è stato chi», partendo dal presupposto che il diritto è uno strumento astratto di tutela o di protezione giuridica e non il suo oggetto, qualificava il fenomeno dell'incidenza di un diritto su un altro diritto come "concorso" di diritti rispetto alla medesima entità, ovvero "concorrenza di più diritti autonomi e diversi, tra loro non incompatibili, in ordine alla stessa res e alla medesima prestazione". Vi sono poi stati altri che invece avevano escluso la reificazione dei diritti, ritenendo al più di poter parlare di beni di secondo grado, ossia di beni rappresentativi di diritti che consentono di garantire un'appartenenza mediata. E infine altri ancora che invece, e in modo condivisibile, avevano sostenuto che il diritto potesse essere considerato un bene quando costituisce oggetto di altro diritto, stante la disposizione dell'art. 813 del Codice civile che equipara alle entità mobili e immobili, i diritti, attribuendo di conseguenza a questi ultimi la natura di bene giuridico. Si affermava infatti che «è ben possibile che il diritto concepito come interesse ed utilità, possa formare a sua volta obiettò di altri diritti: utilità in senso giuridico può dare sia una cosa corporale [e non corporale] che un diritto*»".
Questa ultima argomentazione, alla luce delle considerazioni svolte, appariva, come ancora oggi risulta essere, la più convincente e tale da avvalorare una nozione generale di bene giuridico, applicabile in ogni settore dell'ordinamento», in cui è possibile ricomprendere qualunque entità (anche i diritti), che presenti l'attitudine a essere oggetto di un diritto assoluto o relativo. Ciò in quanto il bene giuridico costituisce il termine oggettivo dei diritti, siano essi reali o relativi, i quali a loro volta rappresentano lo strumento giuridico tramite il quale la ricchezza si manifesta, viene posseduta dal contribuente, e può circolare”.
[180] B. BIONDI, *I beni*, in F. VASSALLI (diretto da) *Trattato di Diritto Civile*, Utet, Torino, 1956, p. 2.

In secondo luogo, è stato osservata come una siffatta impostazione sia stata pacificamente ammessa negli ordinamenti di *common law*, in cui il *diritto di proprietà* esula tanto dai principi di esclusività e assolutezza quanto dalla concezione prettamente *materiale* dei beni, come favoriti dall'ordinamento italiano, coincidendo, piuttosto con i diritti e le facoltà derivanti dall'uso e dal godimento delle cose che ne sono oggetto, indipendentemente dalla loro materialità. È necessario, pertanto, considerare *beni* anche i diritti avente un valore economico patrimoniale, in quanto tali capaci di produrre un'utilità e, quindi, di essere trasformati in denaro. Rilevano, pertanto, i diritti che un soggetto può vantare su una cosa oggetto del diritto (*real property and personal property*).

Si osserva, al riguardo, come siffatti principi siano stati effettivamente recepiti dalla *High Court of Justice* che, chiamata a pronunciarsi in una controversia avente ad oggetto la criptovaluta *Bitcoin*, recependo, da un lato, un precedente giurisprudenziale[181], e accogliendo, dall'altro lato, gli studi svolti da un gruppo di lavoro costituito dal Ministro di Giustizia in materia[182], ha affermato la natura di *personal property* della criptovaluta, così distinguendola dalle c.d. *"chose in possession*" prettamente materiali. Più precisamente, la High Court ha affermato che sebbene "*cryptocurrencies cannot be "things in possession" as due to their virtual nature, they are intangible and cannot be possessed, nor can they be defined as "things in action" as they do not embody any right capable of being enforced by action (...) that did not mean it could not be treated as property"*[183].

7.4.2 *Criptovalute e documento elettronico.*

Parte della dottrina ha, poi, ritenuto di potere qualificare le criptovalute alla stregua di un *documento informatico*, definito dal Codice Amministrazione Digitale come il *«documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»*[184]. In particolare,

[181]Il richiamo è alla pronuncia *National Provincial Bank Ltdv Ainsworth* [1965] AC 1175 (HL) at 1247-1248, in cui il Giudice Lord Wilberforce della *House of Lord* ha precisato come "*before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability*". Si richiama M.PIERRO, *op.cit*., p. 595.

[182] UK JURISDICTION TASKFORCE, *Legal statement on criptoasset and smart contracts*, novembre 2019, in www.blockchain4europe.eu reperibile al seguente link.

[183] Sentenza High Court of Justice, Giudice Bryan. In materia si rinvia a E. CALZOLAIO, *Il Bitcoin come oggetto di* property. *Note a margine di una recente sentenza della* High Court, in *Foro Italiano,* n. 4/2020, p. 494; E. CALZOLAIO, *La qualificazione del* bitcoin: *appunti di comparazione giuridica*, in *Danno e responsabilità*, 2/2021, p. 192 ss.

[184] Art.1, comma 1, lett. p), d.lgs. 7 marzo 2005, n.82

autori come Bocchini[185] e Di Vizio[186] hanno sostenuto la possibilità che le criptovalute – in particolare, il Bitcoin – basate sulla *blockchain*, potessero essere qualificate quale *documento informatico*, in ragione delle caratteristiche proprie della *blockchain*, capace di registrare tutte le informazioni relative alla criptovaluta. Ulteriore conferma della applicabilità alle criptovalute della disciplina del *documento informatico*, è stata poi tratta dalla circostanza che lo stesso – al pari della tecnologia *blockchain* e quindi delle criptovalute su di essa basata – presenta una *firma digitale*[187] definita alla lett. s) del CAD come «*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 o di un insieme di documenti informatici*». In tal senso, Bocchini ha sostenuto che «*Il Bitcoin sarebbe idoneo a garantire, seppur su basi pseudoanonime, la legittimazione e l'adempimento automatico del possessore, in quanto elementi negoziali direttamente incorporati quali dati e rappresentazioni informatiche giuridicamente vincolanti ex ante, e non lasciati al solo (mutevole) giudizio ex post sulla meritevolezza degli scopi economici conseguibili con il loro utilizzo»*[188].

Detta possibilità non è, tuttavia, condivisibile: non è in alcun modo possibile pensare alla criptovaluta come ad un documento informatico solo sulla comunanza della *firma digitale*. Infatti, in CdA descrive il documento informatico come uno strumento privo di un proprio valore, derivante, piuttosto dalla relazione ad altri atti, ai dati e ai fatti dallo stesso.

Al contrario, è possibile riconoscere alle criptovalute un valore intrinseco indipendente dalla sua rappresentazione data da una stringa di *bit*[189].

---

[185] R. BOCCHINI, *op.cit.*, p. 30.
[186] F. DI VIZIO, *op.cit.,* p. 109.
[187] La firma elettronica trova una sua definizione nell'art. 1, comma 1, lett. q) d.lgs. 82/2005: "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica". La firma elettronica qualificata, invece, è definita nel medesimo articolo alla lett. r) come "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica".
[188] R. BOCCHINI, *op.cit.,* p. 30.
[189] A. CAPOGNA, ET AL., *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione.,* in *Diritto mercato tecnologia,* 3,2015, p. 44, in www.dimit.it, reperibile al seguente link.

8. *La natura giuridica delle criptovalute e le loro caratteristiche secondo le Autorità pubbliche europee e nazionali.*

Si è anticipato nei precedenti paragrafi che il fenomeno delle *virtual currency* è divenuto tema di interesse globale.

Al pari della dottrina, anche le Autorità pubbliche europee e nazionali, sin dalle prime manifestazioni della tecnologia cripto valutaria, hanno inteso individuare una disciplina giuridica organica ed uniforme da applicare al fenomeno delle criptovalute.

Ed invero, la nascita di questi strumenti ha destato numerose perplessità in capo ai *regulator* non solo per la complessità del sistema da regolamentare, ma anche per i rischi ad esse connaturati. Si tratta di preoccupazioni dettate non solo da motivazioni strettamente legate all'andamento dell'economia, ma anche, e soprattutto, dovute all'abuso di tale tecnologia da parte dei criminali economici.

A livello nazionale, invece, le Autorità competenti hanno cercato di limitare la materia, circoscrivendone i confini.

8.1 *Le Autorità pubbliche europee e nazionali sulla natura giuridica delle criptovalute: l'intervento della Banca Centrale Europea (BCE) e dell'European Banking Authority (EBA).*

Partendo dalle ipotesi dottrinali sviluppatesi in materia, dal 2012 al 2019, anno di recepimento negli Stati Membri della V Direttiva Antiriciclaggio che ha fornito una definizione – ancorché generica, si è detto – di criptovalute, le autorità pubbliche europee si sono occupate numerose volte della qualificazione giuridica delle valute virtuali.

Siffatto dibattito è stato, infatti, in parte superato dalle risultanze della direttiva 2018/843 UE, a favore di ulteriori valutazioni, ancora attuali, in punto di potenzialità criminale delle criptovalute, che verranno analizzate nel terzo capitolo del presente elaborato.

Appare utile e interessante riportare, in sintesi, le risultanze cui sono giunte BCE e EBA, autorità europee intervenute in materia.

8.1.1 *La Banca Centrale Europea.*

La BCE è stata la prima istituzione dell'Unione Europea ad intervenire in materia, fornendo, negli anni, un *report* – nell'ottobre 2012 – e due diversi *paper* risalenti, rispettivamente, al 2015 e al 2016.

Nell'ottobre 2012 la BCE[190] ha pubblicato il *Virtual Currency* Schemes. Detto *report*, avente ad oggetto le valute virtuali, ha rappresentato la prima presa di posizione in materia da parte di un ente regolatore.

Più precisamente, la BCE ha operato una prima classificazione delle criptovalute esistenti, basata sulle diverse caratteristiche strutturali, ammettendo, per la prima volta, l'esistenza di diverse tipologie di valute virtuali, tra loro divergenti in ragione dell'impatto operato sul sistema economico [191]:

(a) *Moneta Virtuale Chiusa, Tipo 1*: siffatta tipologia di criptovaluta si caratterizza per l'assenza di interazioni con l'economia reale, in quanto non soggetta alla conversione in denaro avente corso legale; può essere acquisita solo tramite attività *online* e spesa unicamente per acquistare beni virtuali od usufruire di servizi offerti all'interno di una certa comunità virtuale. Viene usualmente utilizzata nei giochi *online*. Lo scopo degli emittenti è, in questo caso, la fidelizzazione, oltre che la raccolta di dati personali. L'impatto sull'economia reale è minimo, se non addirittura nullo.

(b) *Moneta Virtuale Unidirezionale, Tipo 2*: contrariamente alla valuta sub *a)*, la moneta virtuale di Tipo 2 può essere acquistata anche con denaro reale, sulla base di un tasso di cambio definito. Potrà essere utilizzata per l'acquisto di beni o servizi siano essi virtuali o reali. Ne costituiscono un esempio le raccolte punti delle carte fedeltà.

L'emittente di questa tipologia di *virtual currency* ha come obiettivi sia la fidelizzazione del cliente sia la raccolta di dati personali, volte all'ottenimento di vantaggi derivanti dalla creazione di diversi depositi di punti prepagati e dalla facilitazione delle attività di acquisto di beni virtuali, in quanto le transazioni di pagamento risultano qui semplificate. Quanto all'impatto sull'economia reale, queste monete creano nuove opportunità di *business*, fortemente connesse all'acquisto di beni reali e virtuali.

(c) *Moneta Virtuale Bidirezionale, Tipo 3*: è una valuta completamente convertibile. Gli utenti potranno acquistarla o venderla con le valute reali sulla base dei tassi di cambio ufficiali. Possono, chiaramente, essere

---

[190] L'acronimo BCE indica la Banca Centrale Europea. Questa è una delle istituzioni dell'Unione Europa. È la Banca dei 19 Stati Membri che hanno adottato l'euro.

[191] BCE, *Virtual Currency Schemes*, Ottobre 2012, p. 5, www.ecb.europa.eu, reperibile al seguente link. Si tenga presente che la struttura stessa della tecnologia è soggetta a modificazioni. R. BOCCHINI, *op.cit.,* pp. 31,32; G. ROTONDO, E. CORAGGIO, *Monete virtuali: tassonomia e inquadramento giuridico*, in *Innovazione Diritto*, 4, 2022, in www.innovazionediritto.it, reperibile al seguente link.

utilizzate per l'acquisto di beni o servizi sia reali che virtuali. Si tratta di una macrocategoria contenente al suo interno due *species* a seconda dell'impatto sull'economia reale. In particolare, è necessario distinguere le *monete globali* (Bitcoin) dalle *monete locali*: le prime, appunto, si pongono in un'ottica internazionale, a dispetto delle seconde che sono fortemente legate all'economia nazionale, se non addirittura regionale o comunale.

Quanto alla natura giuridica del Bitcoin, la BCE con il suo primo paper ha fortemente criticato parte delle teorie dottrinali sopra richiamate.

È stata, innanzitutto, respinta la teoria della criptovaluta come *moneta elettronica*: la BCE, invero, partendo dalla definizione di *moneta elettronica,* quale moneta che deve essere (i) emessa a fronte del versamento di denaro per un importo almeno pari al valore monetario depositato, (ii) memorizzata su un dispositivo elettronico ed (iii) accettata come mezzo di pagamento da parte di soggetti diversi dall'emittente, nega la possibilità di riconoscere alla criptovaluta la prima delle caratteristiche richiamate, rifiutando, pertanto, la qualificazione giuridica nel senso richiamato. In particolar modo, il richiamo principale è al già citato art. 11 della Direttiva 2009/110/CE e all'intrinseca irreversibilità della transazione avente ad oggetto Bitcoin. Inoltre, è stato osservato come le caratteristiche dell'attività di *mining*, che permette di ottenere criptovaluta senza che prima siano depositati fondi, renderebbe inapplicabile alle valute virtuali simili a Bitcoin la disciplina della moneta elettronica.

Rispetto alla possibilità di ricondurre le criptovalute alla categoria dei mezzi di pagamento sub specie di *moneta elettronica*, come disciplinata dalla Direttiva 2007/64/CE, la BCE ha sottolineato come tale Direttiva non prevede una modifica delle regole sull'emissione della moneta né agisce sulla regolamentazione prudenziale degli istituti di moneta elettronica come prevista dalla Direttiva 2009/110/CE. Dovendosi, pertanto, concludere nel senso di escludere il Bitcoin anche dall'ambito disciplinare delimitato dalla Direttiva 2007/64/CE.

Successivamente, nel febbraio 2015, con il *paper "Virtual currency schemes - a further analysis",* la BCE ha sostanzialmente confermato le risultanze del primo *report*, concentrandosi, tuttavia, sulla possibilità di riconoscere alle criptovalute la natura giuridica del *denaro.* Ha, al riguardo, osservato come, da un punto di vista giuridico, è possibile ricondurre nell'alveo della categoria giuridica del *denaro* qualsiasi *cosa* usata come mezzo di scambio nelle operazioni commerciali. È stato, pertanto sottolineato, come nel concetto di "currency" (*valuta*) possano rientrare diverse forme di *denaro.* Pur tuttavia, è stata esclusa la riconducibilità della criptovaluta alla nozione di denaro: in ottica concettuale, invero, con il termine *valuta* – si è detto – si fa principalmente riferimento alla capacità della moneta di avere *corso legale*, di essere riconosciuta universalmente quale mezzo di pagamento. La BCE ha, al riguardo, osservato come sebbene il Bitcoin sia spesso utilizzato a tale scopo – ancorché nell'ambito di un accordo tra privati che accettano che un determinato bene o servizio sia corrisposto in criptovaluta – non è possibile riconoscere una naturale capacità solutaria, tipica della *valuta.* In tal senso, è necessario escludere la natura tanto *valutaria* quanto *monetaria* della criptovaluta, dovendo, al più ammettere una capacità di "contractual money" proprio in ragione della possibilità riconosciuta ai privati nell'ambito della propria autonomia contrattuale di ammettere pagamenti in criptovaluta,

Nell'ottobre 2016, a seguito di distinte richieste da parte del Consiglio e del Parlamento Europeo di elaborazione di un parere[192] in merito alla proposta di una direttiva che modificasse la Direttiva 2015/849/CE, in materia di prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, la BCE si è espressa nuovamente sul tema delle *virtual currencies.*

Già nella proposta di modifica alla Direttiva 2015/849/UE (IV Direttiva AML) le *virtual currency* sono definite come *«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»*. A questo proposito, la BCE ha formulato alcune osservazioni specifiche, rilevando, innanzitutto, l'impossibilità da parte dell'Unione di riconoscere alla criptovaluta una qualsiasi valenza valutaria, stante le previsioni contenute tanto nei Trattati e quanto nel Regolamento CE n. 974/98 del Consiglio, in ragione delle quali l'euro rappresenta la moneta unica dell'Unione Europea, unico strumento adottabile dagli Stati Membri quale valuta.

Viene poi proposto, sulla scorta di altri Paesi non europei intervenuti in materia come il Canada, il Giappone e gli USA, di ricercare una definizione più specifica delle valute virtuali, così che possa essere chiarito espressamente e definitivamente che le criptovalute non costituiscono né moneta né valuta né altro strumento già esistente nell'ordinamento giuridico.

La BCE, in tale contesto, non ha mai negato la *funzione di scambio* riconosciuta alle criptovalute, ammettendo la possibilità di trattarle proprio come *mezzi di pagamento*, riconoscendo, in ogni caso che, concretamente, le criptovalute vengono utilizzate anche con fini diversi da quello del pagamento

[192] Cfr. Parere della Banca Centrale Europea del 12 ottobre 2016 (C-459/3), reperibile al seguente link.

(ad esempio, come prodotti di riserva di valore a fini di risparmio e investimento e strumenti derivati o titoli). È stato, quindi, da ultimo, consigliato di considerare la criptovaluta come uno strumento utilizzato, di volta in volta, con numerosi e diversi fini.

8.1.2 *European Banking Authority.*

Parallelamente, l'EBA ha elaborato ben quattro report dal 2013 al 2019, aventi ad oggetto l'analisi della natura delle criptovalute.

Risale al dicembre 2013 il primo tentativo della *European Banking Authority* di comprendere il fenomeno delle *virtual currencies.* In particolar modo, in questo *paper*, l'EBA ha analizzato i rischi connessi alle criptovalute, cercando però anche di definire la natura giuridica delle stesse. La *virtual currency* è stata inizialmente definita come «*una forma di moneta elettronica non regolamentata, né tantomeno emessa o garantita da una banca centrale, e che può fungere da mezzo di pagamento*»[193], distaccandosi quindi dal primo parere della BCE, sopra analizzato, che prevedeva l'esclusione del Bitcoin dall'alveo della moneta elettronica per le motivazioni già analizzate. L'EBA, inoltre, diversamente dalle altre Autorità non ha mai escluso la possibilità che tali monete virtuali potessero assurgere a mezzi di pagamento.

Nel luglio 2014, tuttavia, con il nuovo parere[194] ha manifestato nuove perplessità circa la possibilità di utilizzare perle criptovalute il termine *virtual currency*, evidenziando come parlare di *currency* assocerebbe, in maniera impropria la criptovaluta alla moneta avente corso legale.

Dovrebbe, dunque, ricercarsi una nuova definizione, che viene rinvenuta in quella già proposta dall'Unione Europea, quale *«rappresentazione digitale di valore non emessa né da una banca centrale né da una pubblica autorità, non necessariamente collegata alla moneta avente corso legale, utilizzata da persone fisiche e giuridiche come mezzo di scambio e caratterizzata dal fatto di poter essere trasferita, conservata o scambiata grazie all'ausilio di supporti elettronici»*.

Tornando sui suoi passi rispetto a quanto accaduto nel 2012 ha, poi, negato la possibilità di ritenere le criptovalute delle *monete elettroniche*, rilevando come, sebbene alcune caratteristiche delle *virtual currencies* richiamino attività o prodotti disciplinati dalla Direttiva sulla Moneta Elettronica (2009/110/CE), in realtà le criptovalute non sono una

---

[193] AUTORITÀ BANCARIA EUROPEA, *Avvertenze per i consumatori sulle monete virtuali,* ABE/WRG/2013/01, 12 dicembre 2013, in www.eba.europa.eu, reperibile al seguente link.

[194] AUTORITÀ BANCARIA EUROPEA, *EBA Opinion on virtual currencies*, ABE/OP/2014/08, 4 luglio 2014, in www.eba.europa.eu.

rappresentazione digitale della moneta avente corso legale, come, invece, avviene per la moneta elettronica. Viene quindi spiegato come l'accostamento alla moneta elettronica fosse stato precedentemente dovuto alla circostanza che le criptovalute – al pari della moneta elettronica – si presentino in forma digitale, siano quindi immateriali, pur non escludendo la possibilità che possano essere rappresentate fisicamente su stampe di carta, piuttosto che su oggetti metallici.

L'EBA, infine, ha riconosciuto nella *volatilità delle* criptovalute, un ulteriore *discrimen rispetto* alla moneta elettronica avente corso legale emessa dalle banche centrali o dalle autorità pubbliche, il cui valore non è ancorato al principio della domanda offerta, ma al valore della moneta avete corso legale cui si riferisce. L'EBA sottolinea come, indipendentemente da quale sia la sua forma, materiale o digitale, la valuta emessa da una banca centrale, piuttosto che da un'autorità pubblica è sempre considerata moneta avente corso legale. Le *virtual currencies*, invece, pur potendo essere legate a una moneta avente corso legale, non prevedono tale caratteristica come intrinseca.

Quanto alla possibilità di prendere in considerazione le criptovalute come *mezzi di pagamento* al fine di ottenere beni o servizi da un soggetto persona fisica o giuridica, l'EBA ha sottolineato la natura privatistica di un accordo che vada in detta direzione, facendo proprie, sostanzialmente, le considerazioni già avanzate dalla BCE.

Nel successivo r*eport* dell'agosto 2016 titolato *Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD) l'*EBA ha affrontato unicamente i rischi e i benefici derivanti dall'uso delle *virual currencies* senza approfondire il tema della natura giuridica delle criptovalute che, ritornerà nell'ultimo report del gennaio 2019[195].

In questo elaborato l'Autorità Bancaria Europea formula una serie di consigli da rivolgere alla Commissione Europea al fine di definire una disciplina adeguata in materia, anche in punto di qualificazione giuridica della criptovaluta. Viene, in questa fase, per la prima volta ammessa la possibilità che la criptovaluta rientri tra gli strumenti finanziari e alla disciplina contenuta nelle già richiamate Direttiva EMD2, Direttiva PSD2 e Direttiva MiFID.

Da un lato, è stata, *en passant*, nuovamente ammessa la possibilità che in determinate circostanze la criptovaluta possa assurgere a *moneta elettronica*, con conseguente applicazione della Direttiva EMD2. Dall'altro lato, è stata presa in in considerazione la possibilità di sottoporre le criptovalute alla

---

[195] AUTORITÀ BANCARIA EUROPEA, *Report with advice for the European Commission,* 9 Gennaio 2019, in www.eba.europa.eu., reperibile al seguente link.

disciplina degli strumenti finanziari e quindi della disciplina MiFID, ma anche a questo proposito l'EBA non raggiunge una soluzione convinta: l'attuale perimetro della disciplina MiFID, infatti, è tale che non può stabilirsi che il *genus virtual currencies* rientri, per intero, nell'alveo di questa; si può però ammettere che alcune *species*, in base alle loro caratteristiche, potrebbero rientrarvi.

Anche l'EBA, al pari della BCE, ha concluso ritenendo che, sulla base dell'analisi svolta, una parte significativa delle attività di impiego delle criptovalute non ricada sotto alcuna normativa europea vigente, dovendosi, pertanto prevedere una regolamentazione *ad hoc.*

8.2 *Le Autorità pubbliche nazionali: Consiglio Nazionale dell'Economia del Lavoro, Banca d'Italia e Consob.*

Anche a livello nazionale, il dibattito interno alle Autorità di vigilanza fortemente concentrato sui rischi derivanti dalle criptovalute è stato piuttosto scarno con riguardo alla natura giuridica delle criptovalute.

Sebbene inizialmente l'attenzione circa il fenomeno delle criptovalute sia sorto solo in ambito europeo, nel gennaio del 2014, in Italia le criptovalute sono apparse per la prima volta in Italia in un documento[196] del Consiglio Nazionale dell'Economia del Lavoro (CNEL), formatosi durante l'Assemblea del 23 gennaio 2014. Più precisamente, in detto scritto è stata ripercorsa l'intera storia della nascita della critptovaluta, corredata dai vantaggi e dai costi di questo nuovo fenomeno.

Dopo oltre un anno dalla redazione del documento del CNEL e a seguito dell'uscita delle raccomandazioni EBA già analizzata in precedenza, anche la Banca di Italia, il 30 gennaio 2015 si è pronunciata con una Comunicazione sulle *virtual currencies* con cui l'Autorità si è espressa sulla natura giuridica delle criptovalute. In tale sede, le valute virtuali sono state definite, parimenti a quanto già accaduto nei report BCE e EBA come «*rappresentazioni digitali di valore non emesse da una banca centrale o da un'autorità pubblica*»[197].

[196] CNEL, *Moneta Elettronica. Osservazioni e Proposte,* 2014, in www.camera.it , reperibile al seguente link.
[197] BANCA D' ITALIA, *Comunicazione del 30 gennaio 2015 - Valute Virtuali,* 2015, in www.bancaditalia.it, reperibile al seguente link.

Anche in questo caso, le Autorità hanno preferito una definizione vaga [198], non precisa, pensata unicamente per rifuggire da tutte le definizioni delle *virtual currency* immaginate dalla dottrina.

La Banca d'Italia ha, invero, escluso categoricamente la possibilità di ricomprendere le criptovalute nell'alveo sia della *moneta avente corso legale* sia della *moneta elettronica*, sottolineando, tuttavia, come le criptovalute sebbene non siano *«necessariamente collegate a una valuta avente corso legale, (...) sono utilizzate come mezzo di scambio o detenute a scopo di investimento e possono essere trasferite, archiviate e negoziate elettronicamente»*[199].

Ciò nonostante, ancora una volta, sulla scorta delle motivazioni già rese dalle Autorità pubbliche europee, è stato riconosciuta la natura di mezzo di scambio della criptovaluta più che di strumento finanziario. Anche in detta sede, inoltre, è stata sottolineato come il mancato riconoscimento alla criptovaluta legale del corso legale proprio della *valuta*, renda liberi i privati di accettare o meno pagamenti in valute virtuali.

Successivamente, nel 2018, la Banca d'Italia è intervenuta nuovamente in materia con la "*Avvertenza per i consumatori sui rischi di valute virtuali da parte delle Autorità europee"*, senza però pronunciarsi sull'aspetto della natura giuridica delle stesse, ma limitandosi, appunto, ai rischi derivanti dal suo utilizzo, che saranno oggetto del prossimo capitolo.

La Consob, infine, non è mai intervenuta in materia con specifici pareri che indagassero la qualificazione giuridica delle criptovalute. Ciò nonostante, parte della dottrina ha inteso interpretare le comunicazioni della Consob in punto di *utilizzo* delle criptovalute alla stregua di strumenti finanziari[200]. In particolare, la Consob in data 19 marzo 2019 ha pubblicato una comunicazione, dal titolo "*Le offerte iniziali e gli scambi di cripto -attività*", nella quale ha ritenuto che le criptovalute potessero essere qualificate quale prodotto finanziario atipico, evidenziando, in particolare, che "vi sono tipologie di *token* che, per le peculiari caratteristiche, integrano la fattispecie degli strumenti finanziari o dei prodotti finanziari (*investment-token* o *security-like-token*). Altri t*oken* presentano un mix variabile di caratteristiche, tanto da venire definiti *hybrid-token*, e sono quelli di più difficile trattazione e inquadramento

---

[198] Cfr. R. SCALCIONE, *Gli interventi delle autorità di vigilanza in materia di schemi di valute virtuali,* in *Analisi Giuridica dell'Economia*, Il Mulino, 1, 2015, in www.rivisteweb.it, reperibile al seguente link.

[199] BANCA D' ITALIA, *Comunicazione del 30 gennaio 2015*, cit.

[200] P. CARRIÈRE, *Le criptovalute sotto la luce delle nostrane categorie giuridiche di strumenti finanziari, valori mobiliari e prodotti finanziari; tra tradizione e innovazione*, *op.cit.*

[200] E. GIRINO, *Criptovalute: un problema di legalità funzionale*, *op.cit.*

rispetto alle vigenti discipline. In particolare, tale ultimo insieme di *token* può presentare un apprezzabile contenuto di tipo finanziario oltre a essere collocati a investitori *retail* con offerte pubbliche”[201].

Siffatta qualificazione è stata successivamente riproposta nel rapporto del 2 gennaio 2020[202], in cui la Consob ha nuovamente ammesso la possibilità che, in determinate circostanze i *cryptoasset* – e, quindi, anche le criptovalute – possano essere assimilati agli *strumenti finanziari.* Proprio in questa sede l’Autorità ha dettato precisi criteri ermeneutici da applicare nella distinzione della criptoattività.

9. *Prime conclusioni.*

Alla luce di quanto sin qui emerso è, sin d’ora, possibile affermare che, quantomeno allo stato, non sia possibile individuare una definizione giuridica univoca di criptovaluta, dovendosi anticipare la natura estremamente versatile della tecnologia in parola.

In tal senso, valuteremo nel prosieguo la capacità delle criptovalute di mimetizzarsi nella disciplina giuridica assurgendo, talvolta, a strumento finanziario, talaltro a bene, altro ancora mezzo di pagamento, a seconda della normativa considerata e delle condotte rilevate.

A fronte di siffatta incertezza, appare in tutta evidenza la difficoltà ermeneutica cui è chiamato l’interprete nella valutazione della possibile rilevanza penale delle condotte tenute con l’utilizzo o a danno della detenzione di criptovalute da parte degli utenti, in un ordinamento incardinato sul principio di legalità. Aspetti, questi, analizzati nel prosieguo.

---

[201] CONSOB, *Le offerte iniziali e gli scambi di cripto-attività*, 19 marzo 2019, in www.consob.it , reperibile al seguente link.

[202] CONSOB, *Le offerte iniziali e gli scambi di cripto-attività. Rapporto finale*, 2 gennaio 2020, in www.consob.it, reperibile al seguente link.

CAPITOLO III

L'UTILIZZO DELLE CRIPTOVALUTE COME STRUMENTO CRIMINALE

Monitoraggio fiscale; 5.3.3. Reati tributari e criptovalute; 5.3.3.1. IVA; 5.3.3.2. Imposte dirette; 5.3.3.2.1. La sottrazione fraudolenta al pagamento di imposte; 6. I reati fallimentari; 6.1. Il caso *BitGrail*; 6.2. L'ampliamento della disciplina dei reati fallimentari; 7. La responsabilità dell'ente e l'utilizzo di criptovalute; 7.1. I soggetti; 7.2. I presupposti della responsabilità; 7.2.1. Interesse e vantaggio; 7.2.2. I meccanismi di imputazione dell'illecito amministrativo; 7.2.3. Il criterio di imputazione: la colpa di organizzazione; 7.3. Le sanzioni; 7.3.1. Le sanzioni pecuniarie; 7.3.2. La pubblicazione della sentenza; 7.3.3. La confisca; 7.4. Reati presupposto e criptovalute; 8. Criptovalute e misure ablatorie; 8.1. La confisca; 8.1.1. La confisca di criptovalute; 8.1.1.1. Il procedimento di confisca; 8.1.1.2. La volatilità; 8.1.1.3. Il trasferimento dei fondi; 8.1.2. Brevi considerazioni conclusive.

1. *Premesse.*

Le caratteristiche strutturali delle criptovalute – quali, in particolare, la decentralizzazione, lo (pseudo) anonimato e l'irreversibilità delle operazioni – hanno, sin da subito, attirato le attenzioni delle Autorità europee e nazionali che, prime tra tutti, ne hanno percepito le potenzialità criminali, redigendo appositi *report* e/o comunicazioni tesi ad informare i consumatori circa i possibili rischi derivanti dal loro incauto utilizzo[203].

In particolare, l'EBA, sin dalla prima storica "Avvertenza per i consumatori sulle monete virtuali"[204] del dicembre 2013, ha individuato le diverse problematiche strettamente connesse all'utilizzo delle criptovalute e riguardanti tutti i soggetti della rete, quali: 1) possibilità di perdere il proprio denaro sulla piattaforma di scambio; 2) possibilità di subire un furto del proprio denaro dal portafoglio elettronico; 3) assenza di tutela per l'utilizzo di monete virtuali come mezzo di pagamento; 4) il valore della moneta virtuale può subire un rapido cambiamento fino a raggiungere lo zero; 5) possibile abuso delle transazioni in moneta virtuale per lo svolgimento di attività criminali, incluso il riciclaggio di denaro sporco; 6) possibili implicazioni fiscali[205].

Tali rischi sono stati poi analizzati anche dalle altre Autorità europee e nazionali che hanno sostanzialmente condiviso l'intervento dell'EBA, approfondendone gli aspetti rilevanti[206].

---

[203] In materia si sono espresse EBA, BCE, *European Securities and Markets Authority* (ESMA), *European Insurance and Occupational Pensions Authority* (EIOPA) a livello europeo; a livello nazionale, Banca d'Italia, la Consob e il CNEL.

[204] EBA, *Avvertenza per i consumatori sulle monete virtuali*, 12 dicembre 2013, in www.eba.europa.eu, reperibile al seguente link .

[205] *Ibidem.*

[206] Per una sintesi si rinvia a CONSOB, *Consob, ESMA, EBA ed EIOPA avvertono i consumatori circa i rischi delle criptovalute*, 9 marzo 2018, in www.consob.it, reperibile al seguente link.

I timori inizialmente solo ipotizzati hanno trovato un preciso riscontro in numerosi casi di cronaca scoperti nell'ultimo decennio, che hanno restituito un quadro pressocché completo – ma, comunque, in evoluzione – circa l'utilizzo delle criptovalute nella commissione dei c.d. *cybercrime.*

Basti pensare che in occasione della pubblicazione del "The 2024 Crypto Crime Report"[207], Chainalysis[208], prendendo in considerazione unicamente le attività illecite compiute direttamente sulla *blockchain*, senza, quindi, considerare i casi "off-chain", per cui le condotte criminose, pur prevedendo uno scambio di criptovalute, non si perfezionano sulla *blockchain* – ha rilevato un volume di transazione illecite pari a 24,2 miliardi di dollari[209].

Ed invero, lo sviluppo della tecnologia *blockchain* e, specificamente, delle *criptovalute* ha fatto emergere nuove modalità di aggressione ai beni giuridici di natura economica già tutelati dall'ordinamento, cui sono conseguite nuove istanze di tutela.

Al riguardo, la dottrina intervenuta in materia ha proposto una classificazione delle condotte considerate, distinguendo le ipotesi in cui le criptovalute vengono in rilievo quale elemento accidentale della fattispecie

---

[207] CHAINALYSIS, *The 2024 Crypto Crime Report*, in www.chainalysis.com, reperibile al seguente link.

[208] Si tratta di una piattaforma di dati *blockchain* che fornisce dati, *software*, servizi e ricerche ad agenzie governative, borse valori, istituzioni finanziarie e società di assicurazione e cybersicurezza in oltre settanta Paesi. Gli studi condotti da Chainalysis alimentano *software* di indagine, conformità e market intelligence utilizzati anche per risolvere alcuni dei casi criminali di più alto profilo al mondo e per aumentare l'accesso dei consumatori alle criptovalute in modo sicuro. È bene evidenziare sin d'ora come le statistiche redatte da Chainalysis sono elaborate sulla base delle transazioni illecite tracciate. In tal senso, è possibile che i dati riportati costituiscano una valutazione al ribasso.

[209] Le stime riportate da Chainalysis evidenziano come le transazioni illecite considerate (c.d. *on chain*) nel 2022 hanno rappresentato lo 0,34% del totale delle transazioni. Il dato, apparentemente innocuo, se raffrontato con le transazioni illecite del 2021, pari allo 0,12%, mostra quasi la triplicazione del volume totale delle transazioni illecite. È bene osservare come, verosimilmente, la stima relativa al 2023 è una stima al ribasso, come può desumersi dagli avvenimenti relativi all'annualità 2022. Ed invero, sebbene nel *report* pubblicato nel febbraio 2023, relativo all'annualità 2022, Chainalysis avesse quantificato in 20,6 miliardi di dollari il volume degli affari criminali *on chain*, nel nuovo report è stato rilevato come, in realtà, a fronte della scoperta di nuovi indirizzi criminali, lo stesso potesse essere quantificato in circa 39,6 miliardi di dollari. È, pertanto, ragionevole ritenere che, in realtà, che possa essere stato di gran lunga maggiore: il 2023 è stato, infatti, un anno di ripresa per le criptovalute oggetto di importanti scandali finanziari nel 2022. Si rinvia a CHAINALYSIS, *The 2023 Crypto crime Report,* in www.chainalysis.com, CHAINALYSIS, *The 2024 Crypto crime Report,* in www.chainalysis.com.

incriminatrice considerata, dalle ipotesi in cui la condotta criminosa prevede un attacco alla *blockchain* o ai *wallet*[210].

Nella prima categoria vengono fatte rientrare le condotte che costituirebbero una manifestazione virtuale di fattispecie incriminatrici originariamente pensate quali illeciti comuni. È questo il caso delle truffe, delle estorsioni, ma anche di condotte in cui le criptovalute rappresentano il profitto del reato ovvero il pagamento richiesto nell'ambito della attività criminosa. Si tratterebbe di ipotesi che non dovrebbero astrattamente causare all'interprete particolari problemi di adeguamento del fatto alla norma, stante la formulazione della fattispecie incriminatrice, che permette un'interpretazione letterale tale da contenere anche condotte che coinvolgano l'utilizzo delle criptovalute.

Diverso è, invece, il caso in cui la condotta ricada direttamente sulla *blockchain* o sul *wallet*. Si tratta, invero, di ipotesi in cui la criptovaluta non fungerebbe da provento del delitto ma, ne costituirebbe, piuttosto, l'oggetto materiale del reato. È questo il caso, ad esempio, del furto di criptovalute, del riciclaggio di denaro e del finanziamento del terrorismo. Ipotesi che impongono una riflessione circa la riconducibilità delle condotte a fatti criminosi già tipizzati senza incorrere nel divieto di analogia in *malam partem* ovvero la necessità di introdurre nuove e diverse ipotesi di reato, che siano maggiormente rispettose del principio di legalità penale[211].

In detto contesto, anche alla luce delle vicende criminose manifestatisi nell'ultimo decennio nonché delle – rare – pronunce giurisprudenziali intervenute in materia (e, per lo più, in fase cautelare di riesame reale), appare necessario indagare, da un lato, la portata criminale delle criptovalute con riguardo alle possibili manifestazioni criminose; dall'altro lato, l'idoneità della normativa vigente quale efficiente strumento di contrasto – tanto in ottica general quanto special preventiva – alla criminalità economica perpetrata con l'utilizzo delle criptovalute.

Stante la particolarità della materia trattata, la trattazione verrà condotta prendendo in considerazione i beni giuridici tutelati dall'ordinamento. Verrà quindi analizzata la casistica manifestatasi nell'ultimo decennio e ci si interrogherà circa la sussunzione delle condotte descritte nelle fattispecie incriminatrici già presenti nell'ordinamento. La riflessione avrà, dunque, ad oggetto la compiutezza del passaggio dal *piano formale* al *piano sostanziale*, sì da indagare se il *crimine* considerato è già previsto come *reato* ovvero, tanto

---

[210] G.P. ACCINNI, Cybersecurity *e criptovalute. Profili di rilevanza penale dopo Quinta Direttiva*, in *Sistema Penale,* 5, 2020, pp.209-232, in www.sistemapenale.it, reperibile al seguente link.
[211] In materia si rinvia a G.P. ACCINNI, Cybersecurity *e criptovalute*, *op.cit*.

nel rispetto del principio di legalità quanto di offensività, sia necessario un intervento del legislatore volto a garantire che condotte offensive di beni giuridici già tutelati dall'ordinamento non rimangano impunite.

In un secondo momento, l'analisi si sposterà sulle ultime frontiere dei crimini economici che possono essere commessi con l'utilizzo di criptovalute. In tal senso, si procederà ad individuare quei reati che, già previsti dall'ordinamento nella loro forma tradizionale, potrebbero venire ad esistenza anche con l'utilizzo di criptovalute, ad oggi ancora rientranti nella c.d. *cifra nera.*

2. *Delitti contro il patrimonio: furto, truffa ed estorsione di criptovalute*

Con riferimento ai *delitti contro il patrimonio* occorre interrogarsi su confini e caratteristiche dei fenomeni comunemente qualificati come "furto", "truffa" con e di criptovalute e "ransomware".

Ed invero, sebbene i casi di cronaca e gli studi statistici siano solite descrivere determinate condotte nei termini richiamati, non sempre le modalità con cui detti fatti si manifestano permettono la sussunzione nelle fattispecie incriminatrici di cui agli artt. 624 c.p. (furto) e 640 c.p. (truffa) dovendo, al contrario, ritenersi che spesse volte detta terminologia sia usata impropriamente.

2.1 *Il "furto" di criptovalute.*

I casi di cronaca susseguitisi nell'ultimo decennio testimoniano molteplici episodi di illecita e fraudolenta *sottrazione di criptovalute* a discapito dei legittimi detentori.

Dai "Report sui crimini *crypto"* redatti da Chainalysis con riferimento alle annualità 2022 e 2023 emerge chiaramente come i "furti" di criptovalute rappresentino una delle modalità favorite dai i *cybercriminal* per ottenere illecitamente criptovalute.

Ed invero, nonostante nell'ultimo anno si sia assistito a una progressiva diminuzione degli episodi di sottrazione delle valute virtuali[212], gli studi condotti con riferimento all'annualità 2023 mostrano come i c.d. "vettori di attacco" che colpiscono la finanza decentralizzata (DeFi)[213] sono diversi e in continua evoluzione.

---

[212] Nel 2023 sono state scoperte sottrazioni di criptovalute per un valore di 1,7 miliardi di dollari, con una dimidiazione rispetto al 2022, in cui sono state rintracciate sottrazioni per un valore pari a 3,8 miliardi di dollari.

[213] Con il termine DeFi si intende fare riferimento a "un ecosistema di applicazioni finanziaria sviluppate sulla base di network blockchain. Più precisamente, il termine

In tal senso, Chainalysis ha proposto una classificazione utile a comprendere la natura delle violazioni.

In particolare, è necessario distinguere i *vettori on-chain* – che hanno origine nella *blockchain* – dai vettori *off-chain* che, quindi, prescindono dalla tecnologia *blockchain*[214].

È bene specificare come i c.d. *vettori di attacco on-chain* non sono costituiti da vulnerabilità intrinseche alla *blockchain*, ma piuttosto da vulnerabilità nei componenti *on-chain* di un protocollo DeFi. La vulnerabilità, ad esempio, potrebbe risiedere nello *smart contract*[215] su cui si basa la transazione (28,3% del valore complessivamente sottratto[216]) o nei c.d. "Governance Attack" (0,5%)[217].Questa tipologia di *vulnerabilità* difficilmente potrà attaccare un servizio centralizzato.

I vettori di attacco *off-chain* derivano, invece, da vulnerabilità esterne alla *blockchain* e possono colpire sia i protocolli DeFi che i servizi centralizzati quali, ad esempio, gli *exchanger* o i *wallet provider*. Ne sono esempio la memorizzazione non sicura delle chiavi private o una soluzione di archiviazione *cloud* difettosa.

Ora, come intuibile dalle caratteristiche della *blockchain* che la rendono una tecnologia particolarmente sicura, dallo studio della casistica analizzata emerge come la maggior parte degli episodi di sottrazione di criptovalute si verifichi a causa di *vettori off-chain* e, più precisamente, dall'utilizzo delle tecniche cibernetiche di *hacking* e *phishing*, che hanno rappresentato, complessivamente, lo strumento utilizzato nel 33,3% dei casi di sottrazione[218].

2.1.1 *Hacking.*

L'*hacking* (più generalmente noto come "attacco *hacker*") permette di ottenere, sfruttando falle del sistema *hardware* e/o *software*, l'accesso non autorizzato a un dispositivo digitale, a un sistema di elaborazione dati o a una

---

"finanza decentralizzata" può riferirsi a un movimento che mira a creare un ecosistema di servizi finanziari *open source*, *permissionless* e trasparente, che sia disponibile a tutti e operi senza nessuna autorità centrale". In particolare, dette applicazioni si caratterizzerebbero per essere completamente decentralizzate, senza alcun contributo da parte di soggetti intermediari. M. SIMBULA, *La finanza decentralizzata o DeFi*, in S. CAPACCIOLI (a cura di), *Criptoattività, criptovalute e bitcoin*, *op.cit.*, pp. 268-270.

[214] CHAINALYSIS, *The 2024 Crypto Crime Report*, *op.cit.*, pp. 38-39.

[215] Si rinvia a BANCA D'ITALIA, UNIVERSITÀ CATTOLICA DEL SACRO CUORE, UNIVERSITÀ ROMA TRE, *op.cit*.

[216] CHAINALYSIS, *"The 2024 Crypto Crime Report"*, *op.cit.*, p. 40

[217] *Ibidem*. È il caso di Lazarus Group di cui si parlerà nel prosieguo con riferimento all'elusione delle sanzioni con l'utilizzo delle criptovalute. Si rinvia a Capitolo III § 2.1.1.1. Lazarus Group nonché, *infra,* § 5.1. Le sanzioni.

[218] *Ibidem.*

rete informatica al fine di entrare in possesso delle informazioni ivi memorizzate.

Detta tecnica può essere impiegata nei confronti sia del singolo utente sia di società di *exchanger*, *wallet providers* e dei c.d. *mining pool*.

Obiettivo dei *cybercriminal* è quello di *appropriarsi indebitamente* delle chiavi private custodite dagli utenti, dalle piattaforme di *exchanger* e di *wallet provider*, sì da potere accedere ai portafogli digitali per sottrarre i fondi ivi contenuti; ovvero di prendere il controllo del *pool*, sottraendo le chiavi private dei *miners*, modificando i relativi indirizzi o accedendo ai loro sistemi, sì da *minare* criptovalute poi dirottate ai propri indirizzi[219]. In quest'ultimo caso, l'attacco è volto, principalmente, a sfruttare il potere computazionale del *pool*, necessario per minare nuove criptovalute.

2.1.1.1 *Lazarus Group.*

Lazarus Group è un gruppo di *hacker* composto da una quantità indefinita di soggetti affiliato, *rectius* assoldato, dal *Reconnaissance General Bureau* del governo nordcoreano per soddisfare gli interessi economici della Corea del Nord.

Più precisamente, si ritiene che gli attacchi informatici sferrati dal Lazarus Group siano principalmente finalizzati a colmare il *deficit* economico-finanziario causato alla Corea del Nord dalle sanzioni imposte a livello internazionali e, quindi, a finanziarne la ricerca e gli studi sui programmi di missili nucleari[220].

Chainalysis, che ha definito *Lazarus Group* "i più prolifici hacker di criptovalute negli ultimi anni"[221], stima che dal 2016 al 2023 gruppi con sede in Corea – presumibilmente riconducibili a Lazarus group – si siano resi responsabili, tramite la tecnica dell'*hacking,* della sottrazione di fondi in criptovalute del valore di oltre 3.543.362.757,00 miliardi di dollari[222].

---

[219] E. REDDY, A. MINNAR, *Cryptocurrency: a tool and target for cybercrime*, in *Acta criminologica: Southern African journal of criminology*, 2018, 31, p. 78, in www.journals.co.za reperibile al seguente link; F. BONCOMPAGNI, S. CAPACCIOLI (a cura di), *Criptoattività*, *op.cit.*, pp. 304 ss.

[220] CHAINALYSIS TEAM, *Russian and North Korean Cyberattack Infrastructure Converge: New Hacking Data Raises National Security Concerns*, settembre 2023, in www.chainalysis.com, reperibile al seguente link.

[221] CHAINALYSIS, *The 2023 crypto crime report, op.cit.*, p. 39.

[222] CHAINALYSIS TEAM, *Russian and North Korean Cyberattack Infrastructure Converge, op.cit*.

In tal senso, rispetto all'annualità 2023 si stima che i fondi sottratti da *Lazarus Group* rappresentino il 29,7%[223] della criptovaluta *rubata* tramite *hacking*[224].

Detti fondi vengono, poi, riciclati con specifiche tecniche che analizzeremo nel prosieguo.

2.1.2 *Phishing.*

Gli attacchi di *phishing* vengono perpetrati tramite l'invio di e-mail o messaggi di testo, effettuazione di telefonate o costruzione di appositi siti *web* fraudolenti progettati per indurre le persone a scaricare *malware*[225] che causino l'indesiderata condivisione di informazioni sensibili (ad esempio, numeri di previdenza sociale e carta di credito, numeri di conti bancari, credenziali di accesso) o che le inducano intraprendere altre azioni idonee ad esporre se stesse e/o le proprie organizzazioni alla criminalità informatica.

Tendenzialmente, il soggetto colpito da *phishing* riceve una *mail* o un messaggio che sembra provenire da soggetti conosciuti o ritenuti affidabili, che invitano il destinatario a cliccare su un *link*, a consultare un sito ritenuto affidabile o ad aprire un file allegato, la cui consultazione viene qualificata come *urgente.*

Con riguardo alle criptovalute, detta tecnica viene utilizzata al fine di ottenere l'accesso ai portafogli digitale della vittima con conseguente sottrazione delle criptovalute ivi contenute.

Detta tecnica è stata utilizzata, ad esempio, nel caso dell'*exchange* "Bittrex": i criminali informatici hanno predisposto un sito con indirizzo simili ed interfaccia identico all'originale, che ha indotto gli utenti ad inserirvi le proprie credenziali, poi utilizzate dai *cybercriminals* per accedere ai fondi corrispondenti[226].

La tipologia di *phishing* descritta deve essere distinta dal c.d. *approval phishing* che, come vedremo, viene comunemente ricondotta all'ipotesi di "truffa" di criptovalute.

---

[223] Il dato, ancorché in calo rispetto al 2022 – quando furono sottratti solo da gruppi nordcoreani 1,65 miliardi di dollari, non è necessariamente indice di una riduzione dell'attività criminale di Lazarus. CHAINALYSIS TEAM, *Russian and North Korean Cyberattack Infrastructure Converge, op.cit*.

[224] *Ibidem.*

[225] Vale a dire qualsiasi codice *software* o programma informatico progettato intenzionalmente per danneggiare un sistema informatico o gli utenti. Quasi tutti gli attacchi informatici moderni coinvolgono qualche tipo di malware. A seconda dell'obiettivo dei criminali informatici, questi programmi dannosi possono assumere molte forme". Si ricordano i *ransomware* e i *adware.* Si rinvia al seguente link.

[226] U. AMIR, *Fake Bittrex cryptocurrency site stealing user funds*, in *HackRead*, 2017, in www.hackread.com, reperibile al seguente link.

2.1.3 *La riconducibilità delle condotte descritte all'art. 624 c.p.*

Come noto, il reato di *furto* è previsto dall'art 624 c.p., che punisce "chiunque si impossessa della *cosa mobile altrui*, sottraendola a chi la detiene, al fine di trarne profitto per sé o per altri".

L'art. 624 c.p. disciplina un delitto, reato comune, a forma libera, di mera condotta, posto a tutela del bene giuridico "patrimonio". Oggetto materiale della condotta è la *cosa mobile altrui*. Elemento soggettivo del furto è il dolo specifico.

In tal senso appare, dunque, necessario preliminarmente interrogarsi sulla nozione di *cosa mobile* e, quindi, sulla possibilità di ricondurvi, tramite interpretazione, il concetto di *criptovaluta*, così ammettendo – o negando – la configurabilità, in termini giuridici e – più strettamente – penalistici, del c.d. *furto di criptovalute.*

La questione non è di immediata risoluzione, ma richiede un preciso sforzo ermeneutico.

È noto, d'altra parte, che la genericità della nozione richiamata ha più volte attirato le attenzioni di dottrina e giurisprudenza, financo a giungere a conclusioni talvolta contrastanti e, comunque, in continua evoluzione.

Tradizionalmente, tanto a livello dottrinale quanto giurisprudenziale, con il termine *cosa* si è sempre inteso far riferimento a qualsiasi entità fisica, materiale e percepibile con i cinque sensi, che possa costituire oggetto di diritti, facoltà, poteri o rapporti giuridici. Da un'analisi sistematica in combinato disposto del codice civile e del codice penale dovrebbe desumersi che una particolare categoria di diritti propri della *cosa* è quella dei *diritti reali*; di talché sarebbe *cosa* qualsiasi entità fisica, materiale e percepibile con i cinque sensi, che possa costituire oggetto di diritti reali[227].

Al riguardo, Ferrando Mantovani ha osservato come detta nozione di *cosa* è coerente con la nozione civilistica fornita all'art. 812 c.c. (*sono beni le cose che formano oggetto di diritti*) ancorché "ad un tempo più ristretta e più ampia. Più ristretta perché non comprende i beni immateriali e i diritti anche se relativi a cose. E più ampia, perché il concetto penale di cosa mobile, essendo la mobilità determinabile in funzione della circolazione materiale, della sottraibilità, della cosa, e perciò fuori da ogni presunzione ed assimilazione civilistiche comprende anche cose immobili *mobilizzate.* Cioè originariamente immobili, ma che, *distaccate* per mano dell'agente dal complesso immobiliare

[227] In materia, si rinvia a S. PUGLIATTI, voce *Cosa in senso giuridico* (teoria generale), in *Enc. dir.,* Milano, Giuffrè, vol. XII, 1962, pp.1 ss.

cui aderiscono o *trasformate* n altro bene (es.: calore, energia), vengono in tal modo rese suscettibili di tale circolazione, di sottrazione"[228].

In tal senso, si è sempre ammessa la riconducibilità alla categoria in analisi unicamente ai beni materiali, escludendo i beni immateriali. Una siffatta impostazione troverebbe conferma, *a contrariis*, dalla previsione dell'art. 624, comma 2, c.p., che eccezionalmente qualifica quale *cosa mobile* "anche l'energia elettrica e ogni altra energia che abbia un valore economico"[229].

Di talché, esclusa la possibilità di qualificare le criptovalute alla stregua di *beni materiali*, non sarebbe corretto e possibile parlare di "furto di criptovalute".

Tuttavia, l'evoluzione dei crimini informatici ha rappresentato una nuova occasione di riflessione in ordine alla necessaria *materialità* del bene qualificabile alla stregua di *cosa.*

In particolare, in una recente pronuncia, la Seconda Sezione penale della Suprema Corte di Cassazione ha aperto alla possibilità di qualificare i *file* – considerati nel corpo del provvedimento alla stregua di dati informatici – come cose mobili, così aprendo alla possibilità che la loro sottrazione possa configurare tanto ipotesi di furto (art. 624 c.p.) quanto di appropriazione indebita (art. 646 c.p.), di cui la cosa mobile pure costituisce oggetto materiale del reato. Più precisamente, la Corte – che, si ripete, utilizza (erroneamente[230]) il termine *dati* quale sinonimo di *file* – osserva che "*il file, pur non potendo*

[228] F. MANTOVANI, *Digesto delle Discipline Penalistiche,* V, UTET, 2004, pp. 367-368.

[229] Dalla lettura della *Relazione di accompagnamento ai lavori preparatori del codice penale* si desume come detta previsione si sia resa necessaria proprio in ragione della difficoltà di ricondurre, in vigenza del codice Zanardelli, l'energia elettrica al concetto di *cosa mobile*, ammettendo, quindi, la possibilità che questa potesse essere oggetto di furto. Si rinvia a "L*avori preparatori del codice penale e del codice di procedura penale. Progetto definitivo di un nuovo codice penale con la relazione del guardasigilli On. Alfredo Rocco*, vol. V, parte II, Roma, Tipografia delle Mantellate, 1929, p. 439: "a giustificare una esplicita dichiarazione legislativa sulla soluzione da dare all'importante dibattito, stia la constatazione che in dottrina sono tuttora contro la tesi accolta dalla giurisprudenza autorevoli scrittori, i quali sostengono che l'utilizzazione illegittima di energia, senza l'impossessamento della materia da cui pervengono o in cui sono accumulate, non può costituire il delitto di furto. Sono quegli scrittori, che ritengono essere le forze naturali, come l'energia elettrica, utilità speciali provenienti dalla cosa, non cose aventi entità materiali autonome".
È bene, osservare, tuttavia, come a livello civilistico l'art. 814 c.c. considera come beni mobili *le energie naturali che hanno valore economico*. In materia si rinvia a S. PUGLIATTI, *op.cit.*, p. 88.

[230] Si condividono, di seguito le considerazioni contenute in C. PAGELLA, *La Cassazione sulla riconducibilità dei file al concetto di "cosa mobile"oggetto di appropriazione indebita: un caso di analogia in malam partem?*, in *Sistema Penale*, 4 marzo 2021, in www.sistemapenale.it, reperibile al seguente link, secondo cui "i *file* sono "contenitori" di dati; questi ultimi, invece, sono informazioni, che viaggiano nello spazio virtuale utilizzando dei vettori (tra cui, appunto, i *file*)".

essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla grandezza dei dati che lo compongono, come dimostrano l'esistenza di unità di misurazione della capacità di un file di contenere dati e la differente grandezza dei supporti fisici in cui i files possono essere conservati e elaborati"[231]; e ancora che " *la considerata la capacità del file di essere trasferito da un supporto informatico ad un altro, mantenendo le proprie caratteristiche strutturali, così come la possibilità che lo stesso dato viaggi attraverso la rete Internet per essere inviato da un sistema o dispositivo ad un altro sistema, a distanze rilevanti, oppure per essere "custodito" in ambienti "virtuali" (corrispondenti a luoghi fisici in cui gli elaboratori conservano e trattano i dati informatici); caratteristiche che confermano il presupposto logico della possibilità del dato informatico di formare oggetto di condotte di sottrazione e appropriazione.*

In conclusione, pur se difetta il requisito della apprensione materialmente percepibile del file in sé considerato (se non quando esso sia fissato su un supporto digitale che lo contenga), di certo il file rappresenta una cosa mobile, definibile quanto alla sua struttura, alla possibilità di misurarne l'estensione e la capacità di contenere dati, suscettibile di esser trasferito da un luogo ad un altro, anche senza l'intervento di strutture fisiche direttamente apprensibili dall'uomo"[232].

L'adesione a siffatta impostazione dovrebbe, dunque, permettere di affermare la possibilità di ricondurre le condotte di sottrazione di criptovalute, come sopra descritte, alla nozione di *cosa mobile* e, pertanto, ove ne sussistano gli ulteriori elementi oggettivi e l'elemento soggetti, alla fattispecie incriminatrice dettata dall'art. 624 c.p.

Detta ricostruzione, tuttavia, – ancorché ipotetica, posto che non risulta essere ancora stata proposta e discussa dalla giurisprudenza con riguardo alle criptovalute – non pare ammissibile in quanto lesiva del principio di legalità *sub specie* di tassatività. Ed invero, solo forzando il significato letterale di *cosa mobile* potremmo ricondurvi le valute virtuali.

Al riguardo, è bene precisare come, per le medesime ragioni appena esposte, non pare configurabile neanche il reato di appropriazione indebita, che per il suo perfezionamento richiede che la condotta appropriativa ricada, appunto, su una *cosa mobile*.

---

[231] Cass. pen., Sez. II, sent. n. 11959/2020 (ud. 7.11.2019), p. 6.
[232] *Ivi*, p. 7

2.1.4 *Una possibile soluzione: la frode informatica.*

Così ricostruiti i termini della questione, occorre ora indagare se vi sia una fattispecie incriminatrice già presente nel nostro ordinamento idonea ad accogliere le condotte di *sottrazione di criptovalute* – e non già di potenza computazionale – ovvero sia necessario l'intervento del legislatore.

Orbene, parte della dottrina ha proposto di ricondurre tali condotte alla fattispecie incriminatrice dettata dall'art. 640 *ter* c.p., rubricata *Frode informatica*[233].

L'art. 640 *ter* c.p., introdotto con L. n. 547/1933, punisce "Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno".

Si tratta di un delitto, reato comune, a forma libera, di danno e di evento, posto a tutela del patrimonio individuale, del regolare funzionamento dei sistemi informatici e la riservatezza dei dati in essi contenuti, che si pone in rapporto di specialità con il reato di truffa, disciplinato all'art. 640 c.p.

A differenza di quanto avviene nel reato di truffa, affinché vi sia frode informatica, non è necessaria l'induzione in errore della vittima, in quanto l'attività fraudolenta investe il sistema informatico – e non l'uomo – e consiste nella sua alterazione, comunque realizzata, o nell'intervento, senza averne diritto, con qualsiasi modalità, sui relativi dati, informazioni, o programmi[234]. Più precisamente, mentre l'*alterazione* si concretizza "in ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'hardware che sul software*",* la condotta di intervento consiste in "una illecita condotta intensiva ma non alterativa del sistema informatico o telematico[235]".

Ciò detto, appare possibile ricondurre le condotte comunemente descritte come *furto di criptovalute* all'art. 640 *ter* c.p.

Preliminarmente, occorre indagare la natura di *sistema informatico* della *blockchain*.

Per fare ciò è necessario guardare alla definizione proposta all'art. 1 Convenzione di Budapest del 23.11.2001, attuata in Italia con L. n. 48/2008, a mente del quale con sistema informatico si indica "qualsiasi apparecchiatura o

---

[233] F. BONCOMPAGNI, *op.cit.*, pp. 304 ss; M. RIVERDITI, G. COSSAVELLA, *Criprovalute e NFT. Gli aspetti penali*, in *Diritto ed economia dell'impresa*, 6, 2022, pp. 646 ss.
[234] Cfr., *ex multis*, Cass. pen., Sez. II, sent. n. 32894/2020; Cass. pen., Sez. VI, sent. n. 8755/2009.
[235] Cfr., Cass. pen., Sez. II, sent. n. 9891/2011.

gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati".

Ora, come detto, la *blockchain* è un sistema *peer-to-peer* distribuito, costituito da una serie di computer, chiamati *nodi*, che rendono accessibili uno all'altro risorse quali la capacità di calcolo e la memoria in maniera del tutto anonima e decentralizzata. Può, pertanto, essere qualificata alla stregua di *sistema informatico*.

Ciò precisato, abbiamo visto come la *sottrazione di criptovalute* può avvenire tramite *hacking* o *phishing* e, più precisamente, si configura a seguito dell'impossessamento da parte del criminale informatico delle chiavi digitali dell'utente – sottratte all'utente direttamente, al *wallet provider* o all'*exchanger* –, così rendendo possibile l'accesso al portafoglio digitale, da cui vengono sottratti tutti i fondi, successivamente inviati a indirizzi appartenenti ai *cybercriminal*.

Ora l'art. 640 *ter* c.p., prevedendo una condotta a forma libera, ben può ricomprendere le condotte descritte, posto che l'*hacking* consiste in un'attività manipolativa dei dati, idonea ad incidere sul regolare funzionamento dell'*hardware* e del *software*, mentre il *phishing* può essere qualificato alla stregua di *intervento* sul sistema informatico.

In tal senso, le chiavi digitali private costituiscono le *informazioni* su cui incidono le condotte richiamate, mentre le criptovalute rappresentano il profitto procurato dal *cybercriminal* che, dopo avere ottenuto le chiavi private, ha avuto accesso al portafoglio digitale dell'utente a cui ha sottratto i fondi.

Siffatta ricostruzione ha, da ultimo, trovato riscontro nell'art. 2, comma 1, lett. c), d.lgs. n. 184/2021, con cui il legislatore ha modificato l'art. 640 ter, comma 3, c.p., introducendo un'ipotesi aggravata di frode informatica ogni qualvolta la stessa produca un trasferimento di valuta virtuale.

2.1.4.1 *Mining pool e "furto" di potenza computazionale.*

Una particolare ipotesi di sottrazione di valute virtuali si verifica nel caso in cui, tramite la tecnica di *hacking,* il *cybercriminal,* non si impossessi di criptovalute già esistenti o di chiavi digitali private degli utenti, ma si introduca nel sistema informatico di un *mining pool*, al fine di sfruttare la potenza computazionale del gruppo sì da ottenere dalla *blockchain* le criptovalute previste come ricompensa per l'attività di validazione delle transazioni e di estrazione di nuove criptovalute, svolte dal gruppo di minatori.

Parte della dottrina ha ricondotto anche detta ipotesi alla fattispecie ex art. 640 *ter* c.p.

Siffatta impostazione merita alcune riflessioni in ragione delle particolari modalità in cui si concretizza la condotta di sottrazione di criptovalute.

Ed invero, in tal caso, la condotta di *hackering* dei *mining pool* prevede l'illecito utilizzo di potenza computazionale – concretamente coincidente con una copiosa quantità di *energia elettrica*, resa possibile dalla presenza di un *pool* di *miner* con apposite apparecchiature – volta ad impossessarsi delle criptovalute riconosciute dalla *blockchain* al *pool* per l'importante ruolo svolto in qualità di *validatore* delle transazioni e di *estrattore* di nuove criptovalute.

Sostanzialmente, dunque, si verifica un furto di energia elettrica volto ad ottenere le criptovalute riconosciute dalla *blockchain*.

Come anticipato, l'art. 624, comma 2, c.p. annovera espressamente nell'alveo delle *cose mobili* anche l'energia elettrica o ogni altra energia che abbia un valore economico.

Si è detto che il reato di furto è un reato a dolo specifico in cui il soggetto agente persegue il fino di profitto.

Occorre, dunque, comprendere se la condotta descritta possa essere qualificata alla stregua dell'art. 624, comma 2, c.p.

La dottrina intervenuta in materia ha escluso detta possibilità, evidenziando come sia necessario distinguere tre diverse frazioni della condotta descritta: la prima frazione della condotta si concretizzerebbe nell'*hackering*; quindi, nell'impossessamento dell'energia elettrica – sub specie di *potenza di calcolo* – a scapito del *pool*. Si avrebbe, poi, una terza frazione della condotta coincidente con l'impossessamento delle criptovalute ottenute per l'attività svolta. È stato, al riguardo osservato, osservato che "l'impossessamento indebito dell'energia elettrica, condotta tipica del delitto di cui all'art. 624 c.p., altro non è che l'"altrui danno" del delitto di frode (nel quale, oltre al vantaggio mediato dello sfruttamento dell'energia elettrica altrui, viene perseguito e conseguito come vantaggio principale l'impossessamento delle criptovalute appena minate)"[236].

È stato, invero, precisato che sebbene "entrambe le fattispecie (624, comma 2, c.p. e 640 ter c.p. – ndr) sono poste a tutela del patrimonio della vittima, (…) il delitto di frode ha quale ulteriore bene giuridico la sicurezza del sistema informatico"[237]; inoltre, "si ritiene che in concreto la fattispecie di furto venga assorbita dal reato di frode informatica"[238].

A conforto di detta impostazione deporrebbe, altresì, la giurisprudenza di legittimità che, intervenuta in materia di *frode informatica*, ha precisato che

---

[236] F. BONCOMPAGNI, *op.cit.*, p. 311.
[237] *Ibidem*.
[238] *Ibidem.*

questa si differenzia dal reato di *truffa* "solo per il fatto che l'attività fraudolenta non investa la persona inducendola in errore ma il sistema informatico di sua pertinenza attraverso una manipolazione"[239]. Nel *furto*, invece, al pari della *truffa* – da cui si differenzia in ragione delle modalità con cui la condotta si manifesta[240] – la condotta ricade sull'uomo.

Ebbene, detta distinzione pare assottigliarsi se si ha riguardo a quanto affermato dal formante giurisprudenziale con riguardo all'ipotesi di furto aggravato dall'uso fraudolento (artt. 624, 625, n.2, c.p.)., in cui è possibile prescindere dall'effettiva *induzione in errore della vittima* che, effettivamente, non si realizza nell'ipotesi di *attacco hacker.* È stato, invero, osservato, come "il *furto aggravato dall'uso del mezzo fraudolento è caratterizzata da un'aggressione unilaterale del reo* – quale deve considerarsi l'attacco *hacker* – al *patrimonio della persona offesa e l'impossessamento della cosa avviene eludendo, grazie al mezzo fraudolento, la vigilanza del detentore contro la sua volontà.* (…) *in caso di uso del mezzo fraudolento, l'azione delittuosa prescinde dall'induzione in errore del soggetto passivo* – che, effettivamente, non si verifica nell'ipotesi di *hackering* – e *mira all'impossessamento della cosa mediante utilizzo di un mezzo che sorprenda o soverchi con l'insidia la contraria volontà del detentore, violando le difese e gli accorgimenti che questi abbia apprestato a custodia della cosa*"[241].

E allora, la riconducibilità della condotta descritta all'art. 640 *ter* c.p., non sembra doversi affermare tanto in ragione della formulazione letterale della norma quanto, piuttosto, guardando, oltre che alla condotta, anche e soprattutto all'elemento soggettivo sussistente in capo all'autore del reato nel momento in cui decide di *hackerare* il *pool* per usufruire del potenziale di calcolo in suo possesso al fine di ottenere la criptovaluta rilasciata dalla *blockchain* quale ricompensa dell'attività svolta.

---

[239] Cass. pen., Sez. II, sent. n. 32894/2020.

[240] Come più volte chiarito dalla giurisprudenza di legittimità, "per qualificare il carattere dell'offesa e stabilire se essa integri gli estremi del furto o quelli della truffa, deve aversi riguardo alla fase risolutiva del processo causale: si configura un'ipotesi di furto, e non di truffa, qualora il reo abbia compiuto attività preparatorie finalizzate ad operare il trasferimento a sé del bene col ricorso a mezzi fraudolenti nei confronti della vitti, ma tra l'atto dispositivo di questa ed il risultato dell'impossessamento si inserisca l'azione del predetto con carattere di usurpazione unilaterale"[240]. Ed invero, mentre nella *truffa* c'è un coinvolgimento attivo della vittima che viene indotta a prestare il proprio consenso all'operazione proposta dal truffatore, nel *furto* la persona offesa è vittima passiva della condotta del soggetto agente, che non la coinvolge in alcun modo nello svolgimento dell'azione di cui la persona offesa è esclusivamente destinataria (cfr. Cass. pen., Sez. V, sent. n. 36864/2020).

[241] Cass. pen., Sez. II, n. 47394/2008.

Se è vero – come è vero – che oggetto del dolo è il fatto tipico, antigiuridico e colpevole, la qualificazione giuridica del fatto non può prescindere dall'analisi della effettiva *volontà* – intesa anche come reale *obiettivo* della condotta tenuta – del reo.

Nel caso di specie, il criminale informatico, in quanto criminale economico, intende procurarsi un profitto consistente nelle criptovalute rilasciate per l'attività di *mining* e non semplicemente impossessarsi della potenza computazionale di cui dispone il *pool*.

In tal senso, l'attacco *hacker* indirizzato nei confronti del *pool* – integrante la condotta di alterazione del sistema informatico di riferimento – non è finalizzato al mero *furto di energia elettrica* e al successivo sfruttamento della potenza di calcolo che, invece, rappresentano unicamente le modalità con cui il soggetto si procura il profitto costituito dalle valute virtuali rilasciate dalla tecnologia.

2.2 *La "truffa" di criptovalute.*

È sostanzialmente possibile distinguere diverse tipologie di condotte comunemente note come *truffa di criptovalute*, che si differenziano tra loro per le modalità con cui i *cybercriminal* riescono a trarre profitto. In tali ipotesi, le valute virtuali possono fungere da *mezzo di pagamento*, da *oggetto materiale della condotta* ovvero quale *artifizio* utilizzato per indurre in errore la persona offesa.

Nel *report* relativo all'annualità 2023 Chainalysis ha qualificato come *truffa* "all scam activity to involve a target failing to receive what they understood they were being promised by the perpetrator, or otherwise being misled by the perpetrator as to an expected outcome"[242].

2.2.1 *La tecnica "approval phishing".*

Con detta tecnica i *cybercryminal*, non accedono abusivamente a un sistema informatico tramite l'invio di un *malware* alla persona offesa, ma la inducono ad autorizzare – tramite app decentralizzate (c.d. dApp) che svolgono la stessa funzione delle app generatrici di OTP nei sistemi bancari– l'accesso al proprio portafoglio digitale, sì da entrare in possesso di tutte le criptovalute presenti nel *wallet* che vengono, così, dirottate su di un altro portafoglio digitale che fa capo al truffatore.

Tale tecnica si basa sull'impiego di vettori *on chain*: molte transazioni truffaldine si basano su *smart contract* dal contenuto apparentemente innocuo

[242] CHAINALYSIS, *op.cit.*, 2024, p.105.

che, in realtà, prevedono che l'utente autorizzi tramite dApp, anziché la transazione che è convinto di compiere, il completo accesso al proprio portafoglio. È bene evidenziare come le approvazioni concesse da dApp sono generalmente sicure perché gli *smart contract* adeguatamente progettati possono utilizzare detta modalità di approvazione solo ove previamente concordata tra le parti del contratto intelligente. I *cybercriminal* fanno leva proprio su questo processo di approvazione: gli utenti credono di stare autorizzando una precisa operazione ma, in realtà, ne validano un'altra.

Il successo dell'*approval phishing* si basa sulle capacità dei criminali cibernetici di individuare le vittime in base alle proprie caratteristiche personali, abitudini d'acquisto, alle proprie passioni e alle proprie debolezze, spesso carpite dai profili *social network* o tramite la sottrazione dei c.d. *big data*.

Non è un caso, infatti, che la tecnica in analisi sia utilizzata nelle c.d. "*romance scam*", in cui la persona offesa è convinta di stare inviando criptovaluta a una persona, mai vista prima, con cui crede, tuttavia, di avere intrapreso una relazione e che paventa importanti ed improvvise difficoltà economiche; nelle *charity scam* in cui le criptovalute vengono astrattamente devolute dall'utente per fini benefici o, ancora, nelle c.d. *investment scam*, in cui l'*user* crede di stare impiegando le proprie criptovalute in un'operazione finanziaria. In questi ultimi due casi il soggetto viene indotto in errore non tanto dal rapporto personale stretto con il truffatore, ma dall'abitudine a compiere transazioni analoghe che non presentano profili illeciti.

2.2.2 *Criptovalute: solo uno "specchietto per le allodole".*

La casistica emersa negli ultimi anni suggerisce che, talvolta, le criptovalute vengono utilizzate unicamente quale strumento per attrarre soggetti da indurre in errore e realizzare truffe tradizionali, senza che le valute virtuali vengano mai effettivamente coinvolte.

È questo il caso in cui i truffatori si presentano come *broker* e utilizzano le valute virtuali quale strumento per attirare aspiranti investitori nella finanza decentralizzata che, tuttavia, finiscono col corrispondere denaro senza che questo venga mai effettivamente impiegato in transazioni DeFi. Talvolta, siffatte operazioni si servono anche di finte sponsorizzazioni da parte di noti personaggi del mondo dello spettacolo – coinvolti loro malgrado – che promettono importanti rendimenti. Ad esempio, noto in Italia è il caso che ha visto il conduttore televisivo Gerry Scotti, a sua insaputa utilizzato come *sponsor* di un'operazione finanziaria in criptovalute, poi rivelatasi una truffa in cui gli asseriti *broker* si erano limitati ad impossessarsi del denaro versato dagli "investitori", senza che l'investimento in criptovalute fosse stato realizzato.

Ulteriore ipotesi si verifica nei c.d. "*giveaway* di criptovalute" sui *social network*. Tale tecnica prevede la pubblicazione sulle principali piattaforme *social* (Instagram, Facebook, TikTok…) di post con cui l'utente viene indotto ad acquistare dei beni o dei servizi, dietro la promessa che l'acquisto gli garantirà la partecipazione a una fortunata estrazione, in cui il premio consiste in una determinata quantità di criptovalute (tendenzialmente Bitcoin), da cui potrà derivare un importante profitto. Inutile dire che, di regola, non solo il soggetto non riceverà il bene asseritamente acquistato, ma neanche prenderà parte all'estrazione che non verrà mai effettuata.

Si tratta, dunque, di ipotesi in cui gli utenti vengono indotti a credere che, a fronte di un versamento in denaro, potranno ricevere – oltre al bene o al servizio acquistato – criptovalute che, tuttavia, non verranno mai realmente trasferite né agli investitori né agli acquirenti.

2.2.3 *Criptovalute come mezzo di pagamento.*

L'ipotesi più semplice di "truffa" in cui vengono in rilievo le criptovalute si ha quando l'utente viene indotto a versare una determinata somma in criptovalute per acquistare o garantirsi un bene o un servizio. In questi casi, le valute virtuali assurgono a mezzo di pagamento.

Un esempio piuttosto noto ha riguardato annunci di lavoro in cui l'accesso al colloquio con l'azienda veniva subordinato al versamento di una somma in criptovaluta, utile a sostenere le successive spese di formazione professionale.

2.2.4 *La riconducibilità delle condotte descritte all'art. 640 c.p.*

Orbene, le condotte appena descritte paiono sussumibili nella fattispecie di truffa, prevista dall'art. 640 c.p.

Ed invero, la norma richiamata punisce "Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno".

La truffa è un reato istantaneo e di danno, che si perfeziona nel momento e nel luogo in cui alla realizzazione della condotta tipica da parte dell'autore fa seguito la *deminutio patrimonii* del soggetto attivo[243].

Si tratta di un reato a forma vincolata, che richiede per la sua consumazione il necessario manifestarsi di una condotta ingannatoria positiva. Detta condotta deve concretizzarsi, alternativamente o cumulativamente, in un *artificio* – vale a dire in una alterazione della realtà esterna, simulatrice dell'inesistente o dissimulatrice dell'esistente, che crea una falsa apparenza

[243] Cass. pen., Sez. II, sent. n. 17322/2019.

materiale – o in un *raggiro,* inteso come una menzogna corredata da ragionamenti idonei a farla scambiare per verità. Entrambe le ipotesi devono costituire mezzi idonei a fondare un erroneo convincimento nella persona offesa. Tuttavia, mentre l'artifizio richiede un'alterazione della realtà esterna con conseguente valenza oggettiva; il raggiro opera direttamente sulla psiche del soggetto, incidendo, dunque, sulla realtà soggettiva della vittima[244].

È di tutta evidenza, quindi, come le condotte sopra descritte possano essere ricondotte anche in senso giuridico, al fenomeno della *truffa*. Ed invero, l'utilizzo delle criptovalute, in tal caso, non incide sulla qualificazione giuridica delle condotte descritte, che integrano i presupposti del reato considerato a prescindere dal coinvolgimento delle valute virtuali.

Le criptovalute, d'altra parte, a seconda delle modalità con cui la condotta truffaldina viene posta in essere dal soggetto agente, possono rilevare quale *ingiusto profitto* (*approval phishing*), quale mezzo di pagamento (acquisto di beni e servizi) o come *artifizio*.

Deve, tuttavia, rilevarsi come, a, dovrà riconoscersi alle criptovalute un diverso rilievo nella fattispecie incriminatrice richiamata.

Le valute virtuali possono, infatti, rappresentare l'ingiusto profitto (*approval phishing*), il mezzo di pagamento (*acquisto di beni e servizi*) o come artifizio o raggiro (*giveaway).*

2.3 *Estorsione di criptovalute.*

Sin dagli arbori le criptovalute sono apparse ai *cybercriminal* come un tule strumento per semplificare e accelerare i fenomeni estorsivi eludendo, da un lato, i controlli delle banche circa i prelevamenti di denaro contate da parte dei clienti vittime di estorsione e, dall'altro lato, rendendo più favorevole il rapporto costi-benefici con opportunità di guadagno più ricche a fronte di rischi di scoperta pressocché nulli.

La diminuzione dei rischi di scoperta, d'altra parte, ha stimolato la fantasia dei *cybercriminal*, che si sono profusi nell'immaginazione di nuove modalità estorsive, favoriti, in questo, anche dal sempre più pregnante ruolo assunto dai *device* nelle nostre vite. Strumenti, questi, divenuti fondamentali e prescindibili in ogni ambito della vita di ciascuno, privata e professionale.

In tal senso, negli ultimi anni si sono verificate poliedriche richieste di pagamento di criptovalute volte a riottenere dati personali e *file* criptati o sottratti, impedire la pubblicazione di notizie o immagine intime, ma anche la liberazione di persone sequestrate nonché ad impedire che i propri cari potessero essere vittime di violenza fisica.

[244] [244] Cfr., *ex multis*, da ultimo, Cass. pen., Sez. II, sent. n. 46209/2023.

2.3.1 *Ransomware.*

Tra i fenomeni che maggiormente causano richieste estorsive in criptovalute rientrano i c.d. *ransomware.*

Dalla lettura del report redatto da Chainalys avente ad oggetto l'annualità 2023 emerge chiaramente come il fenomeno criminale maggiormente manifestatosi *on chain* nell'ultimo anno è rappresentato dai *ransomware*, che hanno assicurato ai *cybercriminal* introiti per oltre un miliardo di dollari, superando di gran lunga le stime relative alle annualità precedenti[245].

Con il termine *ransomware* si fa riferimento a un programma informatico dannoso (c.d. *malware* che può "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese, "ransom") necessario affinché siano restituiti al legittimo proprietario[246] ovvero affinché determinati contenuti – tendenzialmente riguardanti l'intimità dei soggetti colpiti ovvero informazioni che non possono essere divulgate (si pensi, ad esempio, ai dati sanitari sottratti in Italia alle diverse ASST ovvero alle informazioni capaci di svelare il *know how* di un'azienda) – non siano diffusi e resi pubblici.

È possibile distinguere i *ransomware* c.d. *cryptor* –che criptano i file contenuti nel dispositivo rendendoli inaccessibili – dai c.d. *blocker*, che non permettono l'accesso al dispositivo infettato.

Anche se in alcuni casi, piuttosto rari, il r*ansomware* può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (ne è un esempio il *trojan,* che permette un controllo da remoto del *device*), questo tipo di *software* malevoli si diffonde soprattutto tramite la tecnica di *phishing*[247]

---

[245] CHAINALYSIS, *The 2024 crypto crime report*, *op.cit.*, pp. 11 ss. Nel 2022 gli introiti derivanti da *ransomware* si sono aggirati attorno ai 567 milioni di dollari, registrando un'importante diminuzione rispetto al 2021, quando erano state intercettate operazioni *ransomware* per quasi 1 miliardo di dollari. È,peraltro, ragionevole ritenere che, in realtà la quantificazione operata costituisca solo una stima parziale del fenomeno effettivamente verificatosi. Ad esempio, nel 2022, si riteneva che i *ransomware* avessero raggiunto la cifra di 457 milioni di dollari, salvo poi ulteriori scoperte che hanno comportato una correzione al rialzo del 24,1%.
Chainalysis precisa, inoltre, come la quantificazione non comprende anche l'impatto economico relativo alla perdita di produttività e dei costi di riparazione associati agli attacchi (lucro cessante) – talvolta superiori al danno emergente –, ma unicamente il danno emergente, inteso come le somme effettivamente pagate come "riscatto".

[246] Si rinvia a www.ibm.com.

[247] Si rinvia a www.garanteprivacy.it.

o attraverso *app* e giochi installati sul *device* gratuitamente, che infettano il dispositivo.

Ulteriore tipologia di *ransomware* è il c.d. "zero-day exploit"[248] in cui il *cyberattacco* sfrutta una falla di sicurezza sconosciuta o non risolta presente nel *software*, nell'*hardware* o nel *firmare* di un *computer.*

Una volta contratto il *malware* causato dal *ransomware,* nella maggior parte dei casi, la richiesta di pagamento con le relative istruzioni compare in una finestra che si apre automaticamente sullo schermo del dispositivo infettato. All'utente viene minacciosamente comunicato che ha poche ore o pochi giorni per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo.

Si tratta di strumenti particolarmente potenti in ragione, in primo luogo, della loro pervasività dovuta alla capacità di contagiare numerosi dispositivi sfruttando sistemi di archiviazione *cloud* ovvero tramite invio automatico di *link* infetti ai contatti contenuti nel *device* colpito; in secondo luogo, la velocità con cui si evolvono rende più difficile attuare idonee tecniche di prevenzione informatica. Si pensi che dagli ultimi studi condotti in materia emerso come, solo nel 2023, sono state sviluppate almeno 538 nuovi ceppi di *ransomware* con un proporzionale aumento di autori di attacchi cibernetici, tra soggetti indipendenti e gruppi assoldati dagli Stati come, ad esempio, Lazarus Group.

Inoltre, con il passare degli atti l'utilizzo dei *ransomware* sta divenendo sempre più accessibile. Con l'evoluzione dei *market darknet* sono sempre più i criminali informatici che agiscono su commissioni di soggetti che, da soli, non sarebbero in grado di perpetrare un siffatto attacco. Ne è un esempio la diffusione del c.d. "initial access broker" (IABs), quale figura che penetrano nelle reti delle potenziali vittime per poi vendere, dietro il pagamento di poche centinaia di dollari, l'accesso a soggetti che siano interessati ad inserire un *ransomware*; nonché la diffusione del *ransomware as a Service model* (RaaS), inteso quale modello di *business* adottato dalla criminalità informatica che prevedono la vendita di *malware* sì da semplificare e velocizzare il processo di esecuzione degli attacchi informatici, senza che il *criminale informatico* debba procedere alla creazione di un nuovo *ransomware.*[249]

---

[248]Il termine "zero day" si riferisce al fatto che il fornitore del software o del dispositivo ha zero giorni per correggere la falla perché i malintenzionati possono già utilizzarla per accedere ai sistemi vulnerabili. È bene precisare che a seconda delle modalità con cui agisce l'hacker si potrà avere una condotta di *sottrazione di criptovalute* tramite *hacking* ovvero di un'ipotesi di *estorsione di criptovalute* a seguito di *ransomware.* Si rinvia a www.ibm.it. Cfr. *supra*, Capitolo III, § 2.1.1. *Hacking*.

[249] Si rinvia a www.ibm.it.

2.3.2 *Il riscatto come prezzo per la liberazione di un soggetto sequestrato.*

Tra le notizie di cronaca degli ultimi anni vi è anche un caso di sequestro di persona a scopo di estorsione di criptovalute. Nel 2017, infatti, in Ucraina veniva rapito da una banda armata il sig. Pavel Lerner, cittadino russo dirigente di una società attiva nel settore criptovalutario. In tale occasione, il rilascio venne subordinato al versamento di Bitcoin per il valore di un milione di euro. Il sig. Lerner venne effettivamente liberato, ma la polizia ucraina non è mai riuscita a risalire agli autori del sequestro, nonostante la pubblicità dell'indirizzo a cui fu inviato il riscatto in valute virtuali[250].

2.3.3 *La riconducibilità delle condotte descritte agli artt. 629 c.p. e 630 c.p.*

La sussumibilità delle condotte descritte nelle fattispecie incriminatrice disciplinate agli artt. 629 e 630 c.p. non pare comportare particolari problematiche.,

L'art. 629 c.p., rubricato *estorsione,* punisce "*chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno*".

Si tratta di un reato comune, a forma vincolata, di danno e di evento, plurioffensivo in quanto posto a tutela sia del bene giuridico *patrimonio* sia della *libertà di autodeterminazione della vittima.*

Affinché vi sia estorsione è necessario che il soggetto agente si procuri un ingiusto profitto costringendo la vittima con violenza o minaccia e, quindi, annullandone le facoltà volitive[251].

La giurisprudenza di legittimità intervenuta in materia ha chiarito che "ai fini della configurabilità del reato, sono indifferenti la forma o il modo della minaccia, purché comunque idonea, in relazione alle circostanze concrete, a incutere timore ed a coartare la volontà del soggetto passivo. La connotazione di una condotta come minacciosa e la sua idoneità ad integrare l'elemento strutturale del delitto di estorsione vanno valutate in relazione a concrete circostanze oggettive, quali la personalità sopraffattrice dell'agente, le circostanze ambientali in cui lo stesso opera, l'ingiustizia della pretesa, le particolari condizioni soggettive della vittima, vista come persona di normale impressionabilità, a nulla rilevando che si verifichi una effettiva intimidazione del soggetto passivo"[252].

Quanto all'ingiusto profitto, questo si individua in qualsiasi vantaggio, non solo di tipo economico, che l'autore intenda conseguire.

---

[250] G.P. ACCINNI, *Cybersecurity, op.cit.*, p. 216; BBC, *Exmo Bitcoin exchange manager kidnapped in Kiev*, 28 dicembre 2017, in www.bbc.com, reperibile al seguente link.

[251] Cass. pen., Sez. II, sent. n. 11453/2016.

[252] Cfr. *ex multis* Cass. pen., Sez. V, sent. n. 9848/2013.

Alla luce di quanto sin qui affermato è di tutta evidenza come l'ampiezza della fattispecie permetta di affermare la riconducibilità delle condotte di *ransomware* all'ipotesi di estorsione anche quando la richiesta estorsiva abbia ad oggetto il pagamento in criptovalute.

Parimenti, saranno qualificabili alla stregua di *estorsione* tutte le richieste perpetrate con violenza o minaccia in cui sia richiesto il pagamento in criptovalute.

Per le stesse ragioni deve affermarsi la sussumibilità nella fattispecie ex art. 630 c.p. di condotte consistite nel sequestro di persona al fine di estorcere criptovalute, come avvenuto nel caso del sig. Pavel.

2.4 *…in concorso con l'art. 615 ter c.p.*

Tanto le condotte di *frode informatica*, quanto quelle di *truffa* e di *estorsione*, come sopra descritte, possono concorrere con il reato disciplinato dall' artt. 615 ter, c.p., posto dal legislatore a tutela del sistema informatico.

2.4.1 *L'art. 615 ter c.p.*

L'art. 615 ter c.p. disciplina il reato di *accesso abusive ad un sistema informatico*, che punisce "chiunque abusivamente si introduce in un sistema informatico telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto di escluderlo".

Come detto, la *blockchain* appare qualificabile alla stregua di *sistema informatico*, ai sensi dell'art. 1 Convenzione di Budapest.

Ed invero, deve ritenersi che la condotta descritta concorre, oltre che in tutte le ipotesi di *frode informatica*, anche nei casi di truffa perpetrata con la tecnica dell'*approval phishing* nonché nell'estorsione realizzata con l'utilizzo di *ransomware.*

2.4.1.1 *Accesso abusivo e frode informatica.*

La giurisprudenza di legittimità, chiamata ad intervenire in materia, ha affermato il concorso di reati tra la fattispecie dettata dall'art. 615 ter c.p. e la fattispecie tipizzata all'art. 640 ter c.p.

Al riguardo, la Suprema Corte ha affermato che "Il delitto di accesso abusivo ad un sistema informatico può concorrere con quello di frode informatica, diversi essendo i beni giuridici tutelati e le condotte sanzionate, in quanto il primo tutela il cosiddetto domicilio informatico sotto il profilo dello "ius excludendi alios", anche in relazione alle modalità che regolano l'accesso dei soggetti eventualmente abilitati, mentre il secondo contempla e sanziona l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto”[253].

Parte della dottrina intervenuta in materia, nell’affermare la configurabilità dell’accesso abusivo nell’ipotesi di frode informata tramite attacco *hacker,* ha sollevato dei dubbi circa la riconducibilità a detta fattispecie della condotta di frode perfezionata con la tecnica del *phishing*. È stato, infatti, osservato che in detta seconda ipotesi l’accesso abusivo riguarderebbe i portafogli digitali con la conseguente necessità che, affinché si configuri il reato in questione, i *wallet* possano essere qualificati alla stregua di *sistemi informatici*[254].

Posto che la struttura dei portafogli digitali ben può rientrare nella definizione di *sistema informatico*, non pare né rilevante né condivisibile l’osservazione sollevata da Boncompagni[255].

Ed invero, non vi è dubbio che tanto nell’ipotesi di *hacking* quanto in quella di *phishing* si verifichi un accesso abusivo a un sistema informatico. Le due tecniche, infatti, incidono sulle modalità con cui il soggetto agente tiene la condotta di accesso e non sull’effettiva configurazione della stessa: mentre con l’*hacking* il *cybercriminal* sfrutta falle dell’*hardware* o del *software* indipendentemente dalla condotta tenuta dalla persona offesa, nel *phishing* è la vittima, indotta in errore, ad autorizzare contro la sua volontà, l’accesso dell’agente al sistema informatico, da cui poi verranno sottratte le chiavi digitali ivi detenute. L’accesso al portafoglio digitale, in tal senso, rappresenta – al più – una nuova e diversa ipotesi di accesso abusivo. Ma non si può escludere *tout court* la prima condotta di accesso, che sicuramente si verifica e che ricade sul sistema informatico da cui la persona offesa clicca sul link, o apre l’allegato fraudolento.

2.4.1.2 *Accesso abusivo, truffa con approval phishing e ransomware.*

Sebbene in assenza di pronunce giurisprudenziali in materia stante, per l’altro, l’innovatività del fenomeno considerato, pare potersi affermare il concorso di reati tanto tra l’art. 615 ter c.p. e l’art. 640 c.p. quanto tra l’art. 615 ter c.p. e l’art. 629 c.p.

Siffatta affermazione appare coerente con il ragionamento proposto dalla Suprema Corte di Cassazione rispetto alla *frode* informatica, posto a tutela del medesimo bene giuridico protetto – il patrimonio – anche nelle fattispecie di *truffa* e di *estorsione*.

---

253 Cfr. *ex multis* Cass. pen., Sez. V, sent. n. 17360/2020.

254 F. BONCOMPAGNI, *op.cit.*, p.309.

255 I*vi*, p.310.

Al pari di quanto avviene nella *frode informatica* e nella *truffa* deve, infatti, ritenersi che le due fattispecie incriminatrici, in quanto poste a tutela di beni giuridici diversi, possano concorre, non potendo ritenersi che la prima parte della condotta costituisca un antefatto non punibile.

2.5 *Riciclaggio.*

Il fenomeno del riciclaggio di denaro, *rectius* di criptovalute, ha rappresentato la prima manifestazione criminosa delle valute virtuali che, sin da subito, hanno attirato le attenzioni della criminalità organizzata, quale strumento utile a *ripulire* i capitali illeciti, riducendo di molto – se non addirittura azzerando – il rischio di scoperta. Ed invero, a livello europeo, almeno sino al 2015 – quando è stata emanata la IV Direttiva antiriciclaggio – le criptovalute non erano sottoposte alla disciplina antiriciclaggio, di fatto permettendo che i proventi di reato potessero essere immessi impunemente nel mercato economico e finanziario.

Nonostante sia passato quasi un decennio dall'introduzione della prima disciplina normativa in materia, ancora oggi il fenomeno in analisi assume una rilevanza centrale nel mercato criptovalutario.

In tal seno, gli studi condotti da *Chainalysis* mostrano come, solo nell'ultimo anno, sono state tracciate sulla *blockchain* transazioni aventi ad oggetto operazioni di riciclaggio per un valore pari a 22,2 miliardi di dollari. È bene evidenziare come, sebbene si tratti di un *trend* discendente rispetto al 2022 – quando il valore delle criptovalute riciclate è stato pari ad almeno 31,5 miliardi di dollari[256] – le attività riciclatorie continuano a rappresentare un'importante manifestazione del *cryptocrime* su scala mondiale.

Non è un caso, d'altra parte, che la disciplina normativa intervenuta in materia, sia a livello nazionale sia sovranazionale, abbia riguardato quasi esclusivamente il fenomeno in analisi.

Per questo motivo, nel prosieguo, oltre che la riconducibilità delle condotte descritte a fattispecie incriminatrici tradizionali, si valuterà tanto l'efficienza quanto l'efficacia, soprattutto in ottica general preventiva, della normativa introdotta in materia.

Al riguardo, preme precisare sin d'ora come, ad oggi, né a livello europeo né a livello nazionale è stata introdotta una fattispecie incriminatrice di *cybericlaggio* – né quale fattispecie autonoma né quale circostanza

---

[256]Nell'ultimo anno c'è stata una diminuzione del 14,9% del volume totale delle transazioni illecite, le operazioni che hanno avuto ad oggetto attività di riciclaggio paiono diminuite del 29,5% sul totale.

aggravante – dovendosi, pertanto, ricorrere alla normativa tradizionale in materia.

2.5.1 *Il fenomeno criminale.*

Da un punto di vista prettamente fenomenologico è importante sottolineare come con il termine *riciclaggio* i criminologi e gli statisti facciano riferimento al processo di ripulitura di capitali illeciti, che vengono immessi nel flusso economico-finanziario sì da celare le origini criminali dei fondi.

Si tratta di un procedimento particolarmente complesso, in ragione, da un lato, della necessità di rendere *anonimo* il capitale illecitamente prodotto, tanto con riguardo all'operazione criminosa da cui deriva quanto al soggetto che ha tenuto la condotta criminosa; dall'altro lato, della volontà del riciclatore non solo di occultare le origini dei proventi riciclati, ma di rinvestirle in operazioni lecite, idonee a completare l'operazione di *money laundering*[257].

Tradizionalmente, da un punto di vista prettamente criminologico, è stato elaborato un preciso modello c.d. "di ripulitura", che si sostanzia in tre diverse fasi: 1) *Placement stage o Immersion*; 2) *Layering stage o Heavy soap*; 3) *Integration o Spin dry o Repatriation*[258].

La prima delle tre fasi è costituita dal c.d. *placement stage* (fase di *collocamento*) che può essere compiuta tramite *smurfing*. Tale pratica consiste nell'esecuzione di molteplici operazioni di versamento e di cambio con una cadenza progressiva nel tempo, tra loro collegate e riconducibili, nella modalità e nelle quantità, alla volontà di passare inosservate ai controlli previsti dalla legge in materia di riciclaggio di denaro. Lo *smurfing* può essere attuato o direttamente presso istituti bancari ovvero collocati presso cambiavalute clandestini o direttamente sul mercato, sì da eludere i controlli previsti dalla normativa antiriciclaggio. Ed invero, in questa fase, lo scopo principale perseguito, infatti, è quello di rendere il contante *moneta scritturale* rappresentata dai saldi attivi dei rapporti venuti *in nuce* con gli intermediari finanziari.

Nella seconda fase, detta di *layering stage*, i proventi delle attività illecite vengono sottoposti al c.d. *insaponamento,* necessario a rimuovere tutti i collegamenti diretti che possano ricondurre il denaro riciclato all'attività criminale da cui è derivato. La ripulitura vene attuata mediante complesse operazioni di natura principalmente finanziaria, volte a dotare le ingenti

---

[257] R. COSTI, P. D'AGOSTINO, *Trattato di diritto penale dell'impresa. Volume III, I Reati bancari*, Padova, CEDAM, 1992 pp. 221- 222.

[258] S. D'AURIA, *Riciclaggio e terrorismo*, in *GNOSIS - Rivista italiana di Intelligence*, 1, 2013, p.26, in www.gnosis.aisi.gov.it.

quantità di denaro di una parvenza di legittimità. Le tecniche utilizzate sono diverse e in continua evoluzione.

Nella terza e ultima fase si verifica l'*integrazione* dei proventi del delitto nel circuito finanziario legale, con un conseguente mescolamento delle ricchezze illecite con proventi leciti: i capitali vengono investiti in attività commerciali e investimenti.

Dette fasi come vedremo, si sono manifestate anche nel riciclaggio con e di criptovalute.

2.5.2 *Riciclaggio e criptovalute.*

La casistica manifestatasi nell'ultimo decennio ha permesso di individuare e distinguere tre diversi schemi di riciclaggio che coinvolgono le valute virtuali: 1) criptovaluta sporca – denaro pulito; 2) denaro sporco – criptovalute pulita; 3) criptovaluta sporca – criptovaluta pulita.

Dette operazioni possono essere compiute o ricorrendo ai servizi di intermediari – *exchanger*, *wallet provider, mixing service* e *cross-chain bridges* – o ai c.d. "*fiat off-ramping service*", tra cui rientrano, tra gli altri, le operazioni di scambio tra privati, gli ATM di criptovalute e il c.d. *crypto gambling*[259]. Si tratta, dunque, rispettivamente, di riciclaggio *on chain* e di *riciclaggio off chain.*

In entrambi i casi, si tratta di modalità di scambio essenzialmente lecite, che vengono alterate nelle loro finalità dai criminali economici.

2.5.2.1 *Riciclaggio e servizi di intermediazione.*

2.5.2.1.1 *Exchanger: il caso Liberty Reserve.*

Tra le piattaforme di *intermediazione* implicate in operazioni di riciclaggio rientra sicuramente *Liberty Reserve* che – insieme al *market darknet* Silk Road – ha rappresentato il primo caso acclarato di riciclaggio di proventi illeciti realizzato con le criptovalute.

Lo schema applicato era duplice: sia *criptovaluta sporca – denaro pulito* sia *denaro sporco – criptovalute pulita*.

Liberty Reserve era una società di intermediazione mobiliare avente sede legale in Costa Rica accusata, nel maggio 2013, dal Dipartimento di Giustizia degli Stati Uniti d'America, di aver concorso nel reato di riciclaggio di oltre 6 miliardi di dollari derivanti da attività delittuosa, avendo agevolato

---

[259] Detta pratica consiste nell'utilizzare le criptovalute per giocare nei casinò online. Le valute virtuali diventano, quindi, oggetto di scommesse, depositi e prelievi su piattaforme di gioco autorizzate.

1.000.000 di clienti in tutto il mondo a compiere transazioni anonime e non tracciabili[260].

Dalle indagini svolte era, infatti, emerso che la società era stata costituita con il solo e unico scopo di fornire alla criminalità organizzata un supporto nel riciclaggio di proventi derivanti da delitti, sia "tradizionali" – quali il furto di identità, il narcotraffico, la clonazione di carte di credito, ma anche di pornografia minorile – sia dal *cybercrime*.

Liberty Reserve contava 1.000.000 di clienti in tutto il mondo e gestiva un portafoglio di oltre 55 milioni di transazioni illegali.

L'intero sistema di riciclaggio si basava sull'utilizzo della valuta digitale "LR", emessa da Liberty Reserve, peraltro periodicamente quotata in dollari statunitensi.

Per utilizzare la valuta digitale di Liberty Reserve, comunemente chiamata "LR", l'utente doveva innanzitutto aprire un conto attraverso il sito web di Liberty Reserve. Per fare ciò, al momento della registrazione, era sufficiente fornire informazioni identificative di base, come nome, indirizzo e data di nascita, la cui veridicità, tuttavia, non veniva volutamente verificata. I conti potevano quindi essere aperti facilmente utilizzando identità fittizie o anonime.

Una volta creato un conto presso Liberty Reserve, l'utente poteva effettuare transazioni con altri utenti iscritti alla piattaforma, inviando o ricevendo transazioni aventi ad oggetto LR, a cui veniva applicata una commissione dell'1%.

Ed invero, il sistema di Liberty Reserve era stato progettato in modo che i criminali potessero effettuare transazioni finanziarie sotto molteplici livelli di anonimato, evitando così di essere individuati dalle Forze dell'ordine.

Per garantire un ulteriore livello di anonimato, Liberty Reserve – oltre a non verificare le informazioni dichiarate dall'utente in fase di registrazione – da un lato, non prevedeva la possibilità per l'utente di operare autonomamente sulla piattaforma trasferendo o prelevando direttamente denaro dai conti di Liberty Reserve; dall'altro lato, non permetteva agli utenti di interagire direttamente tra loro per scambiare criptovaluta, denaro o altri beni.

Liberty Reserve si serviva, a sua volta, di piattaforme *exchange* affiliate che intrattenevano rapporti finanziari diretti con Liberty Reserve.

In tal senso, le entità terze acquistavano e vendevano LR in cambio di valuta corrente, gestendo così le operazioni tra Liberty Reserve e gli utenti finali e tra gli utenti stessi. I conti di Liberty Reserve venivano, quindi,

---

[260] Si rinvia a L.J. TRAUTMAN, *Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?* , in *Richmond Journal of Law and Technology,* Vol. 20, No. 4, 2014, revised 2017, in www.jolt.richmond.edu, reperibile al seguente link.

alimentati tramite valuta corrente trasmessa alla piattaforma per il tramite degli intermediari[261].

Una volta ricevuto il pagamento dell'utente, l'*exchanger* accreditava il conto Liberty Reserve dell'utente con un importo corrispondente di LR, trasferendo LR dal proprio conto a quello dell'utente. Allo stesso modo, se un utente di Liberty Reserve avesse desiderato prelevare fondi dal proprio conto, avrebbe dovuto trasferire LR all'*exchanger*, che avrebbe poi trattato con la piattaforma affinché convertisse le valute virtuaòo in moneta avente corso legale.

Era, inoltre, possibile pagare un'ulteriore "tassa sulla privacy" di 7 centesimi per transazione, per nascondere anche il numero di conto Liberty Reserve durante il trasferimento di fondi, rendendo di fatto il trasferimento completamente irrintracciabile, anche all'interno del già opaco sistema di *exchange*.

Il sistema offerto da Liberty Reserve forniva un livello di sicurezza tale che, nonostante gli utenti creassero conti con nomi falsi, spesso utilizzavano *nickname* espliciti, da cui era possibile evincere la natura criminale delle operazioni svolte (è questo il caso, ad esempio, degli account "Russia Hackers" e "Hacker Account").

A fronte di ciò, gli utenti di Liberty Reserve hanno effettuato transazioni criminali con un'impunità che sarebbe stata impossibile nel sistema finanziario legittimo.

Liberty Reserve è stata, inoltre, utilizzata quale *market darknet*: il sito web offriva un "interfaccia carrello" che i siti web dei "commercianti" di beni e di servizi illegali potevano utilizzare per accettare la valuta LR come forma di pagamento.

2.5.2.1.2 *Mixing service e cross-chain bridge.*

Le piattaforme di *mixing service*[262] permettono di riciclare *criptovaluta sporca* per ottenere *criptovaluta pulita* tramite le tecniche di *trasferimento* e *mescolamento*.

---

[261] Più precisamente, Il sito web di Liberty Reserve raccomandava una serie di cambiavalute "pre-approvati". Questi cambiavalute tendevano a essere aziende di trasmissione di denaro senza licenza che operavano senza una significativa supervisione o regolamentazione governativa, concentrate in Malesia, Russia, Nigeria e Vietnam. Per i loro servizi, i cambiavalute applicavano commissioni di transazione che in genere ammontavano al cinque per cento o più dei fondi scambiati. Tali commissioni erano molto più alte di quelle applicate dalle banche tradizionali o dai processori di pagamento per trasferimenti di denaro analoghi.

[262] CHAINALYSIS TEAM, *Crypto Mixers and AML Compliance*, *op.cit.*

Il processo di ripulitura può servirsi anche dei *cross-chain,* che consentono agli utenti di spostare fondi da una *blockchain* all'altra convertendo, ad esempio, Bitcoin in Ethereum o Bitcoin in Monero. Si tratta di una pratica piuttosto in uso, fortemente favorita dai *cybercriminal* nell'ultimo anno. Ed invero, Chainalysis ha stimato che, complessivamente, nel 2023, i protocolli *bridge* hanno ricevuto 743,8 milioni di dollari in criptovalute da indirizzi illeciti nel rispetto ai 312,2 milioni di dollari del 2022.

In entrambi i casi, tuttavia, si tratta di attività che avvengono *on chain* e che, quindi, nonostante le difficoltà, possono essere potenzialmente tracciate.

Per questo motivo, sempre più spesso, le due tecniche vengono fuse tra loro per dare luogo a un processo di ripulitura più complesso che trae origine dai *mixing service* e prosegue tramite i *cross-chain bridges* per approdare ai *servizi di cambio valuta*, che permettono di convertire le criptovalute ormai pulite in moneta avente corso legale.

Detta pratica di riciclaggio è stata particolarmente apprezzata anche da Lazarus Group che ha, così, potuto ripulire le criptovalute *sottratte* ed *estorte* tramite l'*hacking* e i *ransomware*[263].

In particolare, Lazarus Group utilizza una specifica tecnica di riciclaggio di criptovalute, sintetizzabile in 5 passaggi[264]:

1) La criptovaluta sottratta o estorta viene inviata a *wallet provider*;
2) Il *wallet provider*, utilizzando i *mixing service* opera il mescolamento o il trasferimento di criptovaluta;
3) La criptovaluta ottenuta all'esito della procedura di *mixing* viene convertita in un'altra tipologia di criptovaluta tramite la tecnica del *cross-chain bridges*;
4) La criptovaluta ottenuta dal *cross-chain bridges* viene trasferita tramite *batches*[265] ai servizi di cambio;
5) I servizi di cambio convertono la criptovaluta in moneta avente corso legale, che viene così immessa nell'economia reale.

---

[263] *Cfr. supra*, Capitolo III, §§ 2.1.1. *Hacking*, 2.3.1. *Ransomware.*

[264] E. PLANTE, *$30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit*, settembre 2022, in www.chainalysis.com, reperibile al seguente link.

[265] Il c.d. *batch crittografico* è un metodo di pagamento su *blockchain* che permette di elaborare tramite una sola operazione molteplici transazioni di criptovalute contemporaneamente destinate a più indirizzi *blockchain*. Tale tecnica viene utilizzata in ambito criminale per riciclare grosse somme di valuta virtuale senza operare transazioni che, per il loro valore, possano essere segnalate come *sospette* nell'ambito dei controlli antiriciclaggio cui sono sottoposti oggi gli intermediari finanziari.

Detta tecnica è stata, ad esempio, utilizzata nel caso Qubit.

Qubit era un protocollo di prestito DeFi con sede in Corea del Sud basato sulla *blockchain* BNB Chain.

In particolare, Qubit operava utilizzando QBridge, un protocollo associato, che permetteva agli utenti di utilizzare criptovalute legate ad altre *blockchain* come garanzia del prestito richiesto, senza effettivamente spostare l'*asset* su BNB Chain, che venivano garantite tramite *smart contract.* Per le sue caratteristiche Qbit era qualificato alla stregua di *cross-chain bridge.*

Gli hacker hanno trovato una falla nel codice di QBridge e hanno, così, sottratto 80 milioni di dollari in criptovalute. L'exploit scoperto dagli hacker ha permesso loro di coniare dal QBridge un numero illimitato di qXETH, un asset destinato a rappresentare gli Ether collegati dalla *blockchain* di Ethereum, senza depositare effettivamente alcun Ether. Gli hacker hanno utilizzato i qXETH sottratti come garanzia per "prendere in prestito" tutti gli asset detenuti dal protocollo, principal- mente monete BNB ma anche diversi token BEP-20, per un valore di circa 80 milioni di dollari al momento del furto.

Una volta trasferiti i fondi da BNB Chain a Ethereum, Lazarus Group ha inviato i fondi al mixer Tornado Cash, che ha rilasciato Ether puliti. A questo punto, parte della criptovaluta ottenuta è stata inviata a un *exchange* decentralizzato affinché la sostituisse con diversi token ERC-20; il resto degli Ether è stato spostato in indirizzi di deposito in vari *exchange* centralizzati e trasformato in moneta avente corso legale[266].

2.5.2.1.2.1 *Da Tornado Cash a Sinbad.io a YoMix*.

Proprio tra le piattaforme preferite di Lazarus troviamo Tornado Cash che, costruito sulla *blockchain di* Ethereum, rappresenta il principale esempio di *mixer* basato su *smart contract*, pertanto c.d. *non custodial*.

Dall'agosto 2019, quando è entrato in funzione, Tornado Cash ha ricevuto oltre 7,6 miliardi di dollari di Ethereum, gran parte proveniente da fonti illecite o ad alto rischio.

L'attività di Tornado Cash si è fortemente ridotta a seguito delle sanzioni OFAC a cui è stata sottoposta nell'agosto 2022[267].

---

[266] CHAINALYSIS, *The crypto crime report 2023, op.cit.*, pp. 42 ss.

[267] È bene evidenziare come, trattandosi di *mixing service* basato su *smart contract* alla sanzione non può seguire la chiusura della piattaforma come avviene per le piattaforme centralizzate (ne è un esempio il market darknet Hydra). Ed invero, Il codice dello *smart contract* può continuare ad essere eseguito in perpetuo senza la necessità di manutenzione da parte degli sviluppatori: Roman Semenov, co-fondatore di Tornado Cash, ha affermato che in ragione delle caratteristiche della tecnologia il mixer non può essere chiuso. Poiché Tornado Cash può tecnicamente continuare a funzionare, i regolatori e i *team* di conformità criptovalutaria devono rimanere vigili per garantire che le piattaforme di cui sono

Più precisamente, la piattaforma di *mixing* è stata inserita dall'OFAC tra i soggetti sottoposti a sanzione *primaria* per avere contribuito a riciclare oltre 620 milioni di dollari in criptovalute sottratte da Lazurus, con le stesse modalità del caso Qubit, dal protocollo Ronin Bridge nel più grande *hack* di criptovalute di sempre, da Harmpmy Bridge e da Noman Bridge[268].

A seguito delle sanzioni OFAC, Tornado Cash ha visto la sua attività ridursi notevolmente a favore della piattaforma di *mixing* Sinbad.io., divenuta la preferita di dei gruppi di hacker con base in Corea del Nord. Sinbad è un servizio di *mixing service* operante su *blockchain* Bitcoin che oscura i dettagli delle transazioni per nascondere il flusso di fondi sulla catena.

Chainalysis ha sistemato che tra il dicembre 2022 e il gennaio 2023 Lazarus Group ha utilizzato Sinbad per riciclare circa 1.429,6 Bitcoin per un valore, all'epoca, pari a circa 24,2 milioni di dollari, in parte derivanti dall'*hacking* di Axie Infinity[269].

Inoltre, Sinbad è noto per avere mixato fondi associati ad altre attività nefaste, tra cui traffico di droga, l'acquisto di materiale per abusi sessuali su minori (CSAM), vendite illecite su *mercati darknet*[270] ed evasione delle sanzioni[271].

Al pari di Tornado Cash, Sinbad.io nel novembre 2023 è stato sanzionato dall'OFAC[272].

Detta operazione, tuttavia, non ha fermato i *cybercriminal* e, in particolare, Lazarus Group, che ora utilizzano il *mixer* YoMix basato su Bitcoin. Non è un caso, infatti, che gli stessi indirizzi di Sinbad.io siano ora attivi su YoMix che, peraltro, ha registrato un'enorme crescita nel 2023, con un aumento degli afflussi di oltre 5 volte nel corso dell'anno.

In base ai dati di Chainalysis, d'altra parte, circa un terzo di tutti gli afflussi di YoMix provengono da portafogli associati a *hacking* di criptovalute.

---

responsabili non effettuino transazioni con il *mixer* ora sanzionato, pena l'irrogazione di sanzione secondaria nei loro confronti. In tal senso, si precisa, come la sottoposizione a sanzione da parte degli USA, ancorché non comporti la chiusura fisica della piattaforma, rende sostanzialmente inservibili dette piattaforme che si basano sul dollaro americano e che, quindi, non verranno più utilizzate da nessuno, pena la sottoposizione a sanzione secondaria.

[268] S. KESSLER, B.BETZ, *Crypto Bridge Nomad Drained of Early $200M in exploit*, agosto 2022, in www.coindesk.com, reperibile al seguente link.

[269] CHAINALYSIS TEAM, *U.S. Sanctions crypto mixer Sinbad.io for Role in North Korean Laundering Activities*, novembre 2023, in www.chainalysis.com, reperibile al seguente link.

[270] *Cfr. infra,* Capitolo III, §3. *Market Darknet e Fraud Shop.*

[271] *Cfr. infra,* Capitolo III, §5.1. *Le sanzioni.*

[272] CHAINALYSIS TEAM, *U.S. Sanctions crypto mixer Sinbad.io, op.cit.*

È interessante notare come la crescita di YoMix e la sua adozione da parte di Lazarus Group costituiscano un esempio della capacità dei *cybercriminal*, colletti bianchi del XXI secolo, di adattarsi alle novità e di trovare servizi di offuscamento sostitutivi quando quelli precedentemente utilizzati vengono chiusi o resi inservibili.

2.5.2.2 *Riciclaggio e fiat off-ramping service.*

Accanto alle tecniche di riciclaggio c.d. *on chain*, vi sono le pratiche *off-chain*, che consistono nelle operazioni di scambio tra privati, prelevamento e versamento in ATM di criptovalute e *crypto gambling*[273].

Non si tratta di modalità di riciclaggio che pongono particolari problemi, se non per il fatto che, non passando da servizi di intermediazione – che, come vedremo, sono oggi sottoposti a precisi obblighi informativi e di controllo degli utenti – potrebbero essere più difficilmente tracciabili, soprattutto ove l'utente faccia uso di più portafogli, ciascuno facente capo a una chiave pubblica diversa, con conseguente possibilità di *spacchettare* le transazioni illecite.

Come si preciserà nel prosieguo, nonostante in passato si credesse che i *cybercriminal* preferissero utilizzare dette tecniche per effettuare le operazioni di *ripulitura* dei proventi del delitto, recenti studi intervenuti in materia hanno dimostrato come, in realtà, la maggiore parte delle transazioni riciclatorie avvenga *on chain*[274].

2.5.3 *Il fenomeno normativo.*

Il *riciclaggio di denaro* è una figura delittuosa di "secondo grado", in quanto avente ad oggetto i proventi di altre attività criminose, c.d. "reati presupposti*"*.

Definito per la prima volta nel 1990 con la Convenzione di Strasburgo, ratificata in Italia con L. 328/1993, il *riciclaggio* consiste in operazioni di *sostituzione* e/o *trasferimento* di denaro, beni o altre utilità derivanti da attività criminose volte a dissimularne l'origine illecita dei proventi, nella volontà di far apparire la loro origine lecita.

Si tratta di un procedimento particolarmente complesso, in ragione, in primo luogo, della necessità di anonimizzare il capitale illecitamente prodotto,

---

[273] Detta pratica consiste nell'utilizzare le criptovalute per giocare nei casinò online. Le valute virtuali diventano, quindi, oggetto di scommesse, depositi e prelievi su piattaforme di gioco autorizzate.

[274] M NAZZARI, *From payday to payoff: Exploring the money laundering strategies of cybercriminals, Trends in Organized Crime,* in *Trends in Organized Crime,* 2023, reperibile al seguente link.

tanto con riguardo all'operazione criminosa da cui deriva quanto al soggetto che ha tenuto la condotta criminosa; e, in secondo luogo, della volontà del riciclatore di fare fruttare i proventi reinvestendoli in operazioni lecite, così completando l'operazione di *money laundering*[275].

Il reato di riciclaggio, in ragione degli interessi tutelati, ai sensi dell'art. 83, par. 1, comma 2, TFUE, costituisce una delle sfere di criminalità su cui il Parlamento europeo e il Consiglio possono stabilire, tramite l'emanazione di apposite direttive, norme minime relative alla definizione dei reati.

La disciplina dettata dall'Unione Europea in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, anche in recepimento dei principi internazionali consolidatisi in materia, è costituita da cinque Direttive susseguitesi nel tempo.

2.5.3.1 *La disciplina vigente.*

Attualmente, il riciclaggio in Italia è disciplinato dal D.lgs. 231/2007, così come, da ultimo, modificato dal d.lgs. 90/2017 attuativo della Quarta Direttiva Antiriciclaggio (849/2015/UE) e dal d.lgs. 125/2019, attuativo della Quinta Direttiva Antiriciclaggio (843/2018).

La Quarta e la Quinta Direttiva antiriciclaggio si pongono in linea con la Raccomandazione del GAFI-FAFT[276] del 2012, che ha dettato i principi

---

[275] R. COSTI, P. D'AGOSTINO, *Trattato di diritto penale dell'impresa. Volume III, I Reati bancari*, CEDAM, 1992 p. 221, 222. S. D'AURIA, *op.cit.*, p.26.

[276] Il GAFI-FATF è un organismo intergovernativo nato nel 1989 a Parigi, in occasione del G7, con la finalità di promuovere strategie di contrasto al delitto di riciclaggio dei proventi derivanti da attività illecita. Le sue competenze sono in continua evoluzione: nel 2001 ha acquisito competenza in materia di prevenzione del finanziamento al terrorismo e nel 2008 vi è stata l'estensione della stessa anche in materia di contrasto del finanziamento delle proliferazioni di armi di distruzione di massa. Tale organismo, di cui fanno parte 37 membri operativi, tra cui l'Italia che ne ha detenuto la presidenza nell'anno 2011-2012, in rappresentanza di Stati e di organizzazioni regionali) e altri membri osservatori tra gli organismi finanziari internazionali e del settore, ha diverse funzioni: in primo luogo, nel suo primo rapporto annuale evidenzia la concentrata attenzione dell'intera comunità internazionale circa la rilevanza della lotta al riciclaggio. Tale passo avanti è evidenziato dall'elaborazione di 40 *Raccomandazioni*, più volte modificate tra il 1996 e il 2001, poi integralmente riscritte prima nel 2003 e poi nel 2016, volte ad emanare *standard* minimi per contrastare le attività finanziarie illecite a livello internazionale, analizzandone anche tecniche ed evoluzione grazie a un continuo controllo dei sistemi nazionali. Nella sua attività, individua le lacune dei sistemi di prevenzione, oltre che di contrasto del riciclaggio in modo da elaborare efficaci attività di contrasto nella lotta al fenomeno in parola. Risale alle origini della sua formazione l'elaborazione di 40 raccomandazioni, innovate nel 2012 e successivamente aggiornate nel 2016, con la definizione di note interpretative in cui sono descritti gli standard internazionali in materia. Esse non hanno un valore vincolante ma costituiscono comunque norme di indirizzo sulla strategia complessiva dei controlli tanto che sono state riconosciute come *standard internazionali* dalla Banca mondiale, il Fondo

fondamentali in materia di prevenzione e contrasto del riciclaggio e finanziamento del terrorismo, istituendo un approccio "basato sul rischio", che deve essere svolto periodicamente. Inoltre, nel 2012 il GAFI ha ampliato il catalogo dei c.d. reati presupposto, includendo anche le violazioni fiscali.Sul fronte prettamente penalistico il d.lgs. 231/2007 deve essere letto alla luce della Direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale" e della disciplina codicistica dettata dagli artt. 648 bis c.p. (Riciclaggio), 648 ter c.p.

2.5.3.1.1 *La Quarta Direttiva antiriciclaggio.*

Nel 2015 l'Unione Europea ha emanato la direttiva 2015/849/UE, cosiddetta Quarta Direttiva antiriciclaggio, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. In particolare, tale atto normativo è intervenuto a modifica del Regolamento UE n. 648/2012 del Parlamento Europeo e del Consiglio, abrogando la Direttiva del Parlamento Europeo e del Consiglio 2005/60/CE, c.d. Terza Direttiva antiriciclaggio, e la Direttiva della Commissione 2006/70/CE.

Le azioni considerate illecite dalla normativa europea in tema di riciclaggio sono molteplici. Tra queste annoveriamo: a) la *conversione* o il *trasferimento di beni* intenzionalmente volti a dissimulare l'origine illecita del denaro, bene o altre utilità coinvolte; b) l' *occultamento* o la *dissimulazione* della reale natura e provenienza dei beni o dei diritti coinvolti nelle operazioni di riciclaggio, oltre che l'*acquisto,* la *detenzione* o l'*utilizzazione* degli stessi nella consapevolezza della loro provenienza criminosa; c) l'*associazione* finalizzata al riciclaggio e il *tentativo* di consumazione; d) il concorso nel reato consistente nell'*aiuto, istigazione* o *consiglio* rivolto a un soggetto per agevolare o commettere l'esecuzione del fenomeno, oltre che il *favoreggiamento* dei soggetti coinvolti nelle operazioni di riciclaggio affinché questi possano evitare le conseguenze giuridiche derivanti dalla commissione del fenomeno criminoso in analisi[277].

La Direttiva in esame si compone di sette Capi all'interno dei quali sono dettate norme comuni volte ad evitare, in ottica preventiva, la circolazione di capitali illeciti nei circuiti finanziari e nei flussi economici, cui si accompagna un'efficiente previsione repressiva. In tutta la sua disciplina viene ribadita e spiegata la minaccia costituita dal denaro illecito per il mercato economico:

---

monetario internazionale e il Consiglio di sicurezza dell'ONU nonostante il loro valore giuridico di *soft law*.

[277] O. SALVINI, *Il contrasto all'abuso del sistema finanziario per scopi di riciclaggio e finanziamento del terrorismo: la IV Direttiva (EU) 2015/849, tra coordinamento e cooperazione*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 2016, p. 149.

l'inserimento di flussi di denaro provento del delitto, infatti, non ne mina unicamente l'integrità, ma ne altera anche il funzionamento oltre che la reputazione.

2.5.3.1.2 *Risk Based Approach.*

La particolarità della Quarta Direttiva antiriciclaggio è deve essere ricercata nella scelta del legislatore europeo, sulla scia della Raccomandazione del GAFI – di affrontare il fenomeno in parola con un *approccio basato sul rischio*[278]. In particolare, nei Considerando 22, 23 viene esplicitato come: "Dovrebbe essere adottato un approccio olistico basato sul rischio. [Questo,] non costituisce un'opzione indebitamente permissiva per gli Stati membri e per i soggetti obbligati: implica processi decisionali basati sull'evidenza fattuale, al fine di individuare in maniera più efficace i rischi di riciclaggio e di finanziamento del terrorismo che gravano sull'Unione e su coloro che vi operano». «Sostenere l'approccio basato sul rischio è una necessità […] per individuare, comprendere e mitigare i rischi».

In particolare, il cosiddetto *Risk Based Approach* viene applicato distintamente su tre livelli: 1) *europeo,* 2) *nazionale* e c) con riguardo ai *soggetti obbligati.*

a) A *livello europeo* (art. 6, IV Direttiva), viene richiesto alla Commissione Europea di individuare le minacce transfrontaliere che potrebbero causare potenziali impatti negativi sui mercati nazionali. Quindi l'elaborazione di una relazione che analizzi in profondità i rischi identificati e che sia aggiornata ogni due anni e posta a disposizione degli Stati membri, a cui la Commissione deve indicare, tramite Raccomandazioni, le misure da adottare per affrontare i rischi rilevati.

b) A *livello nazionale* (art. 7, IV Direttiva), gli Stati membri dovranno individuare, analizzare ed affrontare i rischi di riciclaggio. Al fine di coordinare il *Risk Assessment* viene indicata agli Stati Membri la necessità di istituire un'Autorità che svolga periodicamente le analisi necessarie per prevenire il rischio di riciclaggio[279].

---

[278] S.GALMARINI, C.SABA, *IV Direttiva Antiriciclaggio e approccio basato sul rischio,* Gennaio 2018, in www.dirittobancario.it, reperibile al seguente link.

[279] Un ruolo fondamentale in materia è svolto dalle *Financial Intelligence Units.* Sono unità centrali nazionali competenti, previsti in ogni Stato europeo ed extraeuropeo, nella lotta al riciclaggio di denaro, nella ricezione e nell'analisi di segnalazioni riguardanti operazioni sospette che abbiano ad oggetto la consumazione del fenomeno del riciclaggio o dei connessi reati presupposto. Tali unità, quindi, si occupano di raccogliere i risultati delle analisi e di individuare i fattori di rischio e di condividerli, in un'ottica di cooperazione internazionale, con gli alti Paesi affinché anche essi possano intervenire rispetto al rischio in oggetto. Tale funzione è divenuta fondamentale per l'analisi di flussi che interessano una pluralità di giurisdizioni, come sempre più frequentemente avviene.

Quanto alla capacità delle FIU di scambiarsi tra loro le informazioni acquisite, vediamo che è direttamente autonoma senza la necessaria previsione di trattati internazionali tra i diversi governi. Qualora una FIU dovesse necessitare di protocolli di intesa nello svolgimento di una collaborazione con la FIU di un altro paese, questi, definiti anche *Memoranda of Understanding* dovranno essere negoziati e sottoscritti nel minor tempo possibile. Si tenga presente che, qualora risultasse necessario, la UIF sarà autorizzata a scambiare informazioni su operazioni sospette, derogando sia il segreto d'ufficio che eventuali protocolli di intesa. In tal caso, potrà attingere anche dalle informazioni detenute dalle Autorità investigative.
Sulla base di queste regole, negli anni si è sviluppata una fitta rete di collaborazione internazionale capillare, basata sull'utilizzo di sistemi telematici di comunicazioni molto rapidi e sicuri. Al fine di favorire tale cooperazione, gli *standard* internazionali stabiliti nelle Raccomandazioni del GAFI-FAFT richiedono che le FIU possano provvedere a trasmettere in maniera efficiente ed efficace tutte le informazioni utili a un'altra FIU, sia che essa lo richieda esplicitamente sia che lo ritenga spontaneamente necessario. In ambito comunitario si è scelto di realizzare una rete di comunicazione decentrata, cosiddetta FIU.NET, che permetto lo scambio di informazioni in modo immediato e sicuro.
Può assumere diverse nature: amministrativa, o investigativa, quindi costituita all'interno delle forze di polizia o tra l'Autorità giudiziaria. Non sono esclusi modelli misti. In Italia l'Unità di Informazione Finanziaria è stata istituita con il d.lgs. 231/2007, presso la Banca di Italia in posizione di indipendenza e autonomia funzionale nel ruolo di autorità centrale antiriciclaggio. Il legislatore italiano ha scelto di servirsi di un modello amministrativo, al fine di distinguere l'analisi finanziaria svolta dall'UIF, dall'analisi investigativa svolta dalle Autorità competenti. Difatti, l'UIF, più che una funzione di repressione ha una vera e propria funzione preventiva, tanto che potremmo definirlo *organo filtro*.
Il suo funzionamento trova disciplina nel *Regolamento del Governatore della Banca di Italia*, emanato per la prima volta nel 2007 e modificato nel 2014. Il responsabile della gestione dell'UIF è il Direttore, nominato dal *Direttorio della Banca di Italia*, su proposta del Governatore, il quale sceglie tra professionisti dotati di adeguati requisiti di onorabilità, professionalità, oltre che di approfondite conoscenze finanziarie. La Banca di Italia fornisce all'UIF tutti i mezzi necessari per svolgere adeguatamente le funzioni ad esse attribuite. Ad essa si affianca un Comitato di esperti con funzioni di consulenza, composto dal Direttore e da altri quattro membri nominati dal Ministro dell'economia e delle finanze, sentito il Governatore.
L'UIF riceve, ricerca e acquisisce informazioni aventi ad oggetto ipotesi di riciclaggio di cui dovrà poi effettuare l'analisi finanziaria e valutarne la rilevanza ai fini della trasmissione dei dati raccolti agli organi investigativi e della collaborazione con Autorità Giudiziaria. Si tenga presente che le segnalazioni raccolte sono effettuate dai soggetti obbligati, laddove la sua attività di ricerca e acquisizione concerne comunicazioni oggettivi di operazioni a rischio di riciclaggio, individuate o grazie all'utilizzo di criteri oggettivamente previsti nelle istruzioni attuative o tra le segnalazioni aggregate effettuate da parte dei soggetti obbligati, tra cui ritroviamo gli *intermediari finanziari* e, a partire dalla V Direttiva antiriciclaggio, i *prestatori di servizi di cambio* tra valute virtuali e valute legali e i *wallet providers*.
L'attività svolta deve essere dettagliatamente descritta con apposito Rapporto annuale. Tale documento, entro il 30 maggio di ogni anno, deve essere trasmesso dal *Comitato di Sicurezza Finanziaria* al Ministro dell'economia e delle finanze dal Direttore dell'Unità. Tale *report* deve, inoltre, essere allegato alla Relazione presentata al Parlamento in cui si analizza lo stato dell'azione di prevenzione del riciclaggio (sempre unitamente al finanziamento del terrorismo). La trasmissione del *report* è prevista anche nei confronti della Direzione Nazionale antimafia e antiterrorismo. Alla relazione dell'UIF si unisce

c) A *livello dei soggetti obbligati* (art. 8, IV Direttiva), viene previsto che questi svolgano il *Risk Assesment* interno, adottando misure idonee volta ad individuare ed analizzare il rischio di riciclaggio. Tali valutazioni devono necessariamente essere documentate e aggiornate, quindi poste a disposizioni delle Autorità competenti alla valutazione del rischio.

Con la Quarta direttiva antiriciclaggio si è, dunque, passati da un sistema casistico del rischio a un *modello flessibile*, volto a valutare le situazioni e le problematiche concrete. Vi è un approccio meno teorico e più orientato alla realtà. Sicché, il legislatore non dovrà più definire in modo casistico e predefinito le situazioni di rischio, ma dovranno essere i *soggetti obbligati* a valutare, di volta in volta, di caso in caso, le situazioni che è necessario regolare e, quindi, gli adempimenti e la frequenza con cui questi si devono svolgere al fine di prevenire o, nel peggiore dei casi, combattere il fenomeno del riciclaggio.

In questa fase un ruolo fondamentale è svolto dalle Autorità europee e, in particolare, dal GAFI-FAFT e dalla Commissione Europea sulle base della analisi redatte dagli altri Stati membri, in un'ottica di cooperazione internazionale.

Il Comitato congiunto delle Autorità di vigilanza europea EBA, EIOPA ed ESMA, nel novembre 2016, nel documento denominato *Orientamenti sulla vigilanza basata sul rischio*, ha previsto un processo ciclico costituito da quattro fasi:

(1) in una prima fase vi sarebbe l'*identificazione dei criteri di rischio* con i quali le autorità, sia a livello nazionale che sovranazionale, conoscono le minacce esistente;

(2) la seconda fase riguarda il *risk assessment* nel corso del quale la valutazione del rischio tiene conto dei soggetti sottoposti a vigilanza;

(3) nella terza fase i soggetti interessati devono, poi, definire *l'attività ispettiva*;

(4) la quarta e ultima fase consiste nella *revisione della attività ispettiv*a così da adeguarne il contenuto al rischio rilevato.

In materia, altre linee guida sono state pubblicate dal Comitato di Basilea nel giugno 2017. In particolare, esse sono volte a facilitare le operazioni antiriciclaggio delle banche. Queste dovranno avere un adeguato sistema di *governance* composto da tre linee di difesa: la prima linea è composta dalle

anche la relazione della Banca di Italia avente ad oggetto i mezzi finanziari e le risorse attribuite all'Unità stessa.

politiche e dalle *procedure scelte*. Le stesse dovranno essere comunicate e spiegate a tutto il personale che dovrà svolgere tutti gli adempimenti ivi previsti; bisognerà, inoltre, che vi sia un *responsabile* che verifichi l'effettivo adempimento degli obblighi richiesti alla banca nella lotta al riciclaggio. La terza e ultima linea di difesa è rappresentata, in fine, dall'*internal audit* inerente all'adeguatezza delle politiche e delle procedure scelte per contrastare il fenomeno in esame, ma anche l'efficacia del personale, adeguatamente formato, nell'attuazione delle stesse oltre che dei sistemi di *compliance* e *quality control.* Il *risk based approach*, non è unicamente un principio generale, ma deve essere concretamente utilizzato dai soggetti obbligati della gestione del rischio. Si individuano, in particolare, due diversi processi: *strutturale* ed *esterno.*

L'approccio basato sul rischio *strutturale* prevede che i soggetti obbligati svolgano il *risk assessment*, cosiddetto *interno* con cui valutino i rischi a cui è esposto l'esercizio delle proprie attività così da adeguare a questi procedure e rischi individuati in astratto: vi sarà quindi una prima fase di *identificazione del rischio*, quindi l'*individuazione di eventuali vulnerabilità,* e l'*adeguamento delle procedure* dove necessario.

L'approccio basato sul rischio *esterno*, invece, incide non solo sull'astratta valutazione dei rischi a cui è sottoposto il soggetto interessato nella sua attività, ma è molto più concreto in quanto le misure rilevate come idonee e necessarie per la prevenzione del fenomeno di riciclaggio devono essere proporzionate all'entità dei rischi. Tale *proporzionalità* è definita in base a molteplici criteri: natura giuridica del soggetto cui le misure devono essere applicate, attività da questo svolta, comportamento, area geografica di svolgimento attività e così via.

2.5.3.1.3 *Il d.lgs. 90/2017.*

La Quarta Direttiva Antiriciclaggio è stata recepita in Italia con il d.lgs. 90/2017 che, nel modificare il d.lgs. 231/2007, ha, inoltre, anticipato le risultanze della Quinta Direttiva antiriciclaggio.

In tal senso, all'art. 2, lettera qq) è stata fornita, per la prima volta a livello europeo, la definizione giuridica di *valuta virtuale* intesa 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".

Inoltre, all'art. 3, comma 4, lett. i) sono stati inclusi nella categoria dei *soggetti obbligati* anche "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”.

2.5.3.2 *La Quinta Direttiva antiriciclaggio.*

La Quinta Direttiva antiriciclaggio, 2018/843/UE, è stata pubblicata nella Gazzetta Ufficiale UE il 19 giugno 2018, in modifica della Direttiva 2015/849/UE, già recepita in Italia con il d.lgs. 90/2017. Recepita in Italia con il d.lgs. 125/2019 è attualmente in vigore.

La Direttiva in parola vuole garantire, ulteriormente, a fronte delle nuove tecnologie utilizzate nella commissione del reato di riciclaggio, la trasparenza generale del sistema economico e finanziario dell’Unione[280].

Ai nostri fini, è necessario notare come le novità introdotte dalla Quinta Direttiva in modifica della Quarta Direttiva sono sostanzialmente due: in primo luogo, l’art.2, §1, punto 3, lett. g) nel senso che tra i *soggetti obbligati* rientrino anche i “prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso forzoso*”* e, dei *wallet provider,* ossia “i prestatori di servizi di portafoglio digitale”, definiti come coloro che forniscono *“*servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*”.* Viene, inoltre, previsto in capo a detti soggetto un obbligo di registrazione in un apposito elenco affinché si possa garantire una prima forma di controllo sul loro operato.

In tal senso, è stata ampliata la platea a cui si rivolgono i c.d. *obblighi antiriciclaggio*, sostanzialmente consistenti nell’adeguata verifica della clientela, nella loro identificazione e della natura delle transazioni operate; conservazione dei dati e segnalazione delle operazioni sospette[281].

In secondo luogo, all’art. 3 della Quarta Direttiva antiriciclaggio, è stata introdotta, per la prima volta a livello eurounitario, la definizione di valuta virtuale, da intendersi come “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*”.*

---

[280] Si rinvia a M. NADDEO, *Criptovalute e diritto penale*, in M. LORENZINI, M. ZULBERTI, C. IMBROSCIANO (a cura di), *Criptovalute. Profili storico-economici e giuridici*, Giappichelli, Torino, 2023, pp. 274 ss.

[281] Si rinvia a F.I. BIXIO, *La quinta direttiva antiriciclaggio, la normativa nazionale e il lavoro del FAFT-GAFI*, in S. CAPACCIOLI (a cura di), *Criptoattività*, *op.cit.*, p. 283 ss.

È interessante notare come detta definizione abbia sostanzialmente escluso la natura giuridica di *valuta o moneta* delle criptovalute.

Nonostante le modifiche introdotte, l'Unione Europea si è sin da subito mostrata consapevole delle difficoltà di introdurre una normativa in materia, che possa essere effettivamente *efficace* ed *efficiente.*

In tal senso, al considerando n. 9 della Direttiva 2018/849 Il Parlamento Europeo e il Consiglio hanno dato atto che "L'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. L'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato. Per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate".

2.5.3.2.1 *Il D.lgs. 125/2019.*

Sebbene l'Italia, con il d.lgs. 90/2017, avesse già previsto parte della disciplina poi oggetto della Quinta Direttiva Antiriciclaggio, questa è stata recepita in Italia con il d.lgs. 125/2019 che ha ulteriormente modificato il d.lgs. 231/2007.

Ad oggi, l'art. 1, comma 2, n.3.2, lett. ff) definisce *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"; alla lett. ff-bis) viene fornita la definizione di *prestatori di servizi di portafoglio digitale* intesi come "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".

L'art.,1 comma 2, lett. qq) definisce la *valuta virtuale* come "la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente".

2.5.3.3 *La Direttiva 2018/1673/UE sulla "lotta al riciclaggio mediante il diritto penale".*

Pubblicata in Gazzetta Ufficiale dell'Unione Europea del 12 novembre 2018 e da recepirsi negli Stati Membri entro il 3 dicembre 2020, la Direttiva 2018/1673 definisce delle norme *minime* relative alla definizione di reati e di sanzioni in materia di riciclaggio. Il provvedimento è caratterizzato da disposizioni penalistiche volte al contrastare l'immissione di risorse finanziarie di dubbia provenienza nel flusso economico mondiale.

In una prima parte la direttiva introduce norme di definizione dei reati di riciclaggio, delle ipotesi di concorso, istigazione e tentativo. Gli Stati membri, dunque dovranno punire le condotte, intenzionalmente tenute dai soggetti criminali, che prevedano la *conversione* o il *trasferimento di beni*, oltre che l'*occultamento* della provenienza delittuosa di denaro, beni o altre utilità, anche quando tale condotta sia tenuta allo scopo di aiutare un soggetto coinvolto nel fenomeno del riciclaggio. Inoltre, saranno punite anche le condotte di *acquisto, detenzione, utilizzazione* di beni di provenienza criminosa di cui, al momento della ricezione, si conosca o si sospetti l'origine o la natura.

La seconda parte della direttiva, invece, prevede le sanzioni da applicarsi in materia di riciclaggio: le *persone fisiche* che si renderanno colpevoli delle condotte analizzate saranno sottoposte a sanzioni penali effettive, proporzionate e dissuasive quali la pena detentiva massima non inferiore a 4 anni, oltre alla possibilità di applicare misure e sanzioni aggiuntive. Sono inoltre previste circostanze aggravanti. Quanto alle *persone giuridiche*, è previsto che esse possano essere ritenute responsabili di taluni dei reati di riciclaggio quando commessi a loro vantaggio. Saranno previste, al proposito, sanzioni penali e non, tra cui l'esclusione dal godimento di un beneficio o di un aiuto pubblico.

Vengono poi fornite delucidazioni in materia di *giurisdizione* e di *strumenti investigativi*: è infatti individuato lo Stato membro a cui spetta la competenza giurisdizionale, oltre che alcune indicazioni rispetto alle modalità di cooperazione internazionale e di partecipazione ad Eurojust. Rispetto alla giurisdizione, vediamo che questa è definita in primo rispetto al *locus commissi delicti*, anche se lo stesso si è realizzato solo in maniera parziale sul territorio, quindi nel rispetto del criterio della *cittadinanza.* È inoltre previsto che gli Stati membri possano ampliare la propria giurisdizione quando l'autore del reato risieda abitualmente sul territorio o se il reato è commesso a vantaggio di una persona giuridica stabilita sullo stesso.

Al fine di evitare conflitti di giudicato o casi di *bis in idem*, il legislatore europeo ha stabilito che nel caso di conflitto di giurisdizione positivo che veda due o più Stati dichiararsi competenti per i medesimi fatti, essi dovranno collaborare al fine di stabilire l'unica giurisdizione competente sulla base dei parametri congiuntamente elaborati.

Nonostante la direttiva in esame sia intervenuta dopo la Quarta e Quinta Direttiva antiriciclaggio, che avevano dato conto dell'evoluzione del riciclaggio con l'utilizzo delle valute virtuali, con la Direttiva 2018/1673 il Parlamento e il Consiglio si sono limitate a dar conto, al considerando n. 6 che "L'uso delle valute virtuali presenta nuovi rischi e sfide nella prospettiva della lotta al riciclaggio. Gli Stati membri dovrebbero garantire che tali rischi siano affrontati in modo adeguato", senza dettare norme minime in materia, che potessero garantire l'armonizzazione della disciplina penalistica delle criptovalute.

A livello nazionale, la Direttiva è stata recepita con il d.lgs. 195/2021, entrato in vigore il 15 dicembre 2021. Il decreto di attuazione, composto da soli due articoli, ha modificato le fattispecie di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e di autoriciclaggio. È stato, in particolare, previsto (a) l'ampiamento del catalogo dei reati presupposto, al cui interno rientrano oggi anche i delitti colposi e le contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi; (b) una diversa comminatoria della pena a seconda che il reato presupposto sia un delitto o una contravvenzione.

Inoltre, il legislatore è intervenuto sulla fattispecie di autoriciclaggio prevedendo che l'art. 648 ter.1., comma 2, c.p. sia una circostanza attenuante comune e non un'attenuante ad effetto speciale. È stata, infine, eliminata la condizione di procedibilità della richiesta del Ministro della giustizia prevista dall'art. 9 c.p. quando il reato sia commesso da un cittadino italiano all'estero.

2.5.3.4 *Il Regolamento (UE) 2023/1113.*

In data 9 giugno 2023, è stato pubblicato in Gazzetta Ufficiale dell'Unione europea il Regolamento UE/2023/1113, che ha modificato al Quinta Direttiva Antiriciclaggio.

Obiettivo della *travel rule* è garantire la tracciabilità dei trasferimenti aventi ad oggetto *cripto-asset* – tra cui rientrano anche le criptovalute – al dine di bloccare le transazioni sospette, al pari di quanto avviene anche per le altre operazioni finanziarie.

La regola c.d. della *travel rule*, già presente nella finanza tradizionale, mira a fare sì che le informazioni riguardanti tanto il mittente quanto il destinatario della transazione siano visibili per tutta l'operazione e siano conservate da entrambe le parti.

Più precisamente, con l'introduzione della *Travel Rule* i fornitori di servizi di *asset* virtuali saranno tenuti a condividere il nome e l'indirizzo del mittente, il nome del destinatario, le informazioni sulla transazione, quali l'*importo,* l'*asset* oggetto della transazione e la *blockchain* su cui questa è stata inserita.

La *travel rule* incomberà, oltre che su tutti i prestatori di servizi criptovalutari, già sottoposti agli obblighi di registrazione e controllo tipici dell'AML, anche sui i c.d. *self-hosted wallet* che, pur non essendo gestiti da un soggetto intermediario, interagiscano con portafogli detenuti su piattaforme *exchange* e *wallet*.

In definitiva, non saranno soggetti a *travel rule* unicamente i trasferimenti che avvengono tra privati, senza l'intervento di un *provider.*

2.5.3.4.1 *La Legge delega n. 15/2024*

Con Legge delega n. 15/2024, entrata in vigore il 21 febbraio 2024, il Parlamento, all'art.18 ha delegato il Governo ad adottare, entro il 21 febbraio 2025, uno o più decreti legislativi idonei ad adeguare la normativa nazionale al regolamento UE 2023/1113 del Parlamento e del Consiglio, in modifica della Quinta Direttiva Antiriciclaggio.

2.5.4 *Il riciclaggio di criptovalute.*

2.5.4.1 *Art. 648 bis c.p.*

L'art. 648 bis c.p. punisce chiunque, fuori dei casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto o da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

È un reato comune, a forma libera, di mera condotta e di pericolo concreto, posto a tutela del bene giuridico *patrimonio*. Parte della dottrina, tuttavia, ha sostenuto che si tratti di un delitto *plurioffensivo* posto a tutela dell'amministrazione *della giustizia*, l'*ordine pubblico* e l'*ordine economico*[282].

Si tratta di un reato commissivo in cui la condotta può, alternativamente, consistere nella *sostituzione* o nel *trasferimento* di *denaro, beni o altre* utilità provenienti da delitto doloso e – a fare data dall'entrata in vigore del d.lgs. 195/2021 - da delitto colposo o da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi; o nel *compimento di altre operazioni* volte ad occultare la provenienza delittuosa dell'oggetto materiale della condotta.

Nel concetto *sostituzione* rientrano tutte le operazioni di *heavy soap* volte ad allontanare il *provento del reato* dalla commissione del reato presupposto. Al riguardo, la giurisprudenza di legittimità ha chiarito che "*sostituire* nell'ambito dell'art. 648 *bis* c.p., significa rimpiazzare (il denaro o i valori "sporchi" con quelli "puliti")"[283].

Il *trasferimento* – che si pone in un rapporto di *genus* a *species* con la *sostituzione* – consiste nello spostamento da un soggetto ad un altro o da un luogo ad un altro del provento del delitto, che sarà quindi ripulito tramite strumenti negoziali o giuridici, senza che la sua *natura* muti.

La condotta – il cui oggetto materiale può essere *denaro, beni* o *altre utilità provenienti da delitto* – deve essere compiuta *in modo da ostacolare l'identificazione della provenienza delittuosa*, da un soggetto diverso rispetto a quello che ha commesso il reato presupposto.

Ed invero, la giurisprudenza di legittimità ha chiarito come "la disposizione di cui all'art. 648 *bis* c.p. pur configurando un reato a forma libera, richiede che le attività poste in essere sul denaro, bene od utilità di provenienza delittuosa siano specificamente dirette alla sua trasformazione parziale o totale, ovvero siano dirette ad ostacolare l'accertamento sull'origine delittuosa della *res*, anche senza incidere direttamente, mediante alterazione dei dati esteriori, sulla cosa in quanto tale"[284]. In tal senso, "integra il delitto di riciclaggio il compimento di operazioni volte non solo ad impedire in modo definitivo, ma anche a rendere difficile l'accertamento della provenienza del denaro, dei beni

[282] Altra parte della dottrina ha contestato la possibilità che il bene giuridico tutelato al proposito possa essere il *patrimonio*, dal momento che potrebbe mancare il danno patrimoniale; altra, invece, ha sostenuto che il bene giuridico tutelato dovrebbe rinvenirsi nella *tutela del risparmio*. In realtà, si è evidenziato come la *plurioffensività* della fattispecie in parola si verificherebbe solo se il riciclaggio presentasse sempre la sua portata plurioffensiva: l'unico bene offeso con costanza sarebbe l'*amministrazione della giustizia*. Si rinvia a E. DOLCINI, G. MARINUCCI, G. L. GATTA, *Art. 648 bis*, Riciclaggio, in *Codice Penale Commentato,* Wolters Kluwer, 2015, p. 1322.

[283] Cass. pen., Sez. IV, sent. n. 6350/2007.

[284] Cass. pen., Sez. II, sent. n. 15092/2007.

o delle altre utilità, attraverso un qualsiasi espediente che consista nell'aggirare la libera e normale esecuzione dell'attività posta in essere"[285].

Ne consegue che "per la punibilità del reato di riciclaggio (…) è necessaria la sussistenza del reato presupposto, che non può essere mai dato per scontato, dovendo peraltro essere sempre specificato ed essersi verificato prima della commissione del supposto riciclaggio"[286]. Al riguardo, è stato chiarito come "non è necessari che il delitto presupposto risulti accertato con sentenza passata in giudicato, ma è sufficiente che lo stesso non sia stato giudizialmente escluso, nella sua materialità, in modo definitivo e che il giudice procedente per il reato di cui all'art. 648 bis c.p. ne abbia incidentalmente ritenuto la sussistenza"[287].

Quanto all'elemento soggettivo, si tratta di reato a dolo generico, che ricomprende la volontà di compiere attività volte ad ostacolare l'identificazione della provenienza delittuosa dei proventi[288].

2.5.4.1.1 *Riciclaggio e criptovalute.*

Così descritto il reato di riciclaggio, deve ritenersi che le condotte come sopra descritte siano sussumibili nella fattispecie incriminatrice dettata dall'art. 648 *bis* c.p. ogniqualvolta il *trasferimento* o *la sostituzione* di o in *criptovalute* siano commesse da soggetto diverso rispetto all'autore del reato presupposto.

In particolare, l'art. 648 *bis* c.p. sarebbe configurabile rispetto a tutti e tre gli schemi di riciclaggio sopra descritti: 1) criptovaluta sporca – denaro pulito; 2) denaro sporco – criptovaluta pulita; 3) criptovaluta sporca – criptovaluta pulita.

Preliminarmente, si rende necessaria una precisazione in punto di *oggetto materiale* della condotta. Ed invero, la condotta di riciclaggio deve necessariamente ricadere su *denaro*, beni *o altre utilità*.

In tal senso, mentre nessun problema pare configurarsi con riguardo allo schema *denaro sporco – criptovaluta pulita*, qualche quesito in più pongono gli altri due schemi in cui il provento del delitto presupposto è costituito da criptovalute.

Infatti, esclusa la riconducibilità della criptovaluta alle nozioni di *denaro* e di *beni*[289], è necessario interrogarsi sulla sussumibilità del concetto di *valuta virtuale* nell'alveo delle *altre utilità*. D'altra parte, solo ove ciò sia

[285] Cass. pen., Sez. VI, sent. n. 16980/2007.
[286] Cass. pen., Sez. II, sent. n. 1435/2013.
[287] Cass. pen., Sez. II, sent. n. 10746/2014.
[288] Cass. pen., Sez. VI, sent. n. 16980/2007.
[289] Cfr. Capitolo II, §7. *La natura giuridica delle criptovalute: premesse*.

possibile potrà dirsi configurabile il reato di riciclaggio negli schemi *criptovaluta sporca – denaro pulito*, *criptovaluta sporca – criptovaluta pulita.*

In dottrina si discusso sul significato di *altra utilità* nel reato di riciclaggio. Il riferimento, invero, è stato introdotto solo nel 1990, quando l'attuale formulazione ha sostituito l'originale dizione che prevedeva che oggetto materiale della condotta di riciclaggio fossero il *denaro o valori*.

È stato, al riguardo, osservato come la modifica fosse tesa ad includere nell'ambito della fattispecie richiamata ogni *entità suscettibile di valutazione economica*[290]. In tal senso, costituirebbe oggetto materiale della condotta di riciclaggio "qualsiasi entità economica ben definita, che possa assumere la veste di *provento*"[291] dovendosi, pertanto, escludere le *utilità non patrimoniali,* in quanto non suscettibile di valutazione economica[292].

Orbene, alla luce di quanto sin qui detto, non vi è dubbio che possa essere riconosciuto alle criptovalute un valore economico, ancorché caratterizzato da forte volatilità[293].

Ciò detto, occorre ora comprendere che tipo di condotta si realizzi negli schemi richiamati.

Sul punto, pare doversi ammettere una distinzione a seconda dello schema considerato.

---

[290] F. ANTOLISEI, *Diritto penale, parte speciale*, I, Giuffrè, Milano, 2008, p. 465; C. LONGOBARDO, *Delitti di perpetuazione di una situazione antigiuridica*, in S. FIORE (a cura di), *I reaiti contro il patrimonio*, UTET, Torino, 2010, p.847; E. MEZZETTI, *Reati contro il patrimonio*, Giuffrè, Milano, 2013, p. 651; M. ANGELINI, voce *Riciclaggio*, in *Digesto delle Discipline Penalistiche*., UTET, Torino, 2006, p. 1392 ss.

[291] G. J. SICIGNANO, *Bitcoin e riciclaggio*, Giappichelli, Torino, 2019, p. 125; M. ANGELINI, *op.cit*.

[292] In tal senso, l'*utilità* cui si fa riferimento nel *riciclaggio*, differirebbe dall'*altra utilità* propria dei reati di concussione e corruzione per cui, generalmente, si ammette la possibilità di fare rientrare in detta nozione anche ipotesi di *utilità morale*, quindi non patrimoniale. Si rinvia, tra gli altri, a M. ANGELINI, *op.cit*.

[293] A ben vedere, in passato è stata negata la possibilità di riconoscere alle criptovalute un *valore economico*, proprio in ragione della loro connaturata *volatilità*, principalmente dovuta alla decentralizzazione della *blockchain*. Interessante, al riguardo, il decreto n. 7556/2018 con cui l Tribunale di Brescia, Sez. spec. in materia di impresa, ha affermato la legittimità della scelta di un notaio di non trascrivere una delibera di aumento di capitale di una s.r.l. sottoscritto in criptovaluta. Tale scelta sarebbe stata dovuta al fatto che il notaio non considerava possibile una valutazione economica della valuta virtuali. Il Tribunale ha deliberato nello stesso senso, ritenendo che non vi sia conformità tra la criptovaluta e l'art. 2464 c.c. il quale dispone che «*possono essere conferiti tutti gli elementi dell'attivo suscettibili di valutazione economica*». In particolare, nella motivazione si legge che *«non è ad oggi presente in alcuna piattaforma di scambio tra criptovalute ovvero tra criptovalute e monete aventi corso legale, con la conseguente impossibilità di fare affidamento su prezzi attendibili in quanto discendenti da dinamiche di mercato»*.

Ed invero, mentre nelle ipotesi *criptovaluta sporca – denaro pulito* e denaro *sporco – criptovaluta pulita* sembrerebbe configurarsi un'ipotesi di *sostituzione*, nel terzo caso (criptovaluta sporca – criptovaluta pulita) vi sarebbe un'ipotesi di *trasferimento* della criptovaluta da una *blockchain* ad un'altra (ad esempio, da Bitcoin a Monero).

2.5.4.2 *L'art. 648 ter c.p.e criptivalute.*

Il delitto di *Impiego di denaro, beni o utilità di provenienza illecita* punisce chiunque, fuori dai casi di ricettazione e riciclaggio, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

Si tratta di un "reato a forma libera realizzabile attraverso condotte caratterizzate da un tipico effetto dissimulatorio e finalizzate ad ostacolare l'accertamento o l'astratta individuabilità dell'origine delittuosa del denaro, dei beni o delle altre utilità che si intendono occultare"[294].

Detta fattispecie si pone in un rapporto di *species a genus* con l'art. 648 bis c.p., rispetto al quale si caratterizza per le modalità con cui si intende ostacolare l'identificazione delittuosa dei proventi; nella condotta ivi considerata tale scopo è perseguito mediante l'impiego delle risorse in attività economiche o finanziarie. In tal senso, il soggetto che abbia già commesso il reato di *ricettazione* o *riciclaggio* di denaro non potrà essere punito anche per *impiego di denaro, beni o utilità di provenienza illecita*.

Il *discrimen* rispetto all'art. 648 bis c.p, infatti, è rappresentato proprio dalla *attività economica* o *finanziaria* la cui nozione è rinvenibile agli artt. 2082, 2135 e 2195 c.c. Si tratta, dunque, di attività produttiva *in senso stretto*, in quanto diretta a produrre nuovi beni e servizi, ma anche ad ogni altra attività idonea a produrre profitti, quindi connessa agli strumenti finanziari.

Ciò detto, richiamate tutte le considerazioni già svolte rispetto alla fattispecie di *riciclaggio*, deve ritenersi che la fattispecie richiamata possa venire ad esistenza con l'utilizzo di criptovalute.

In particolare, ciò sarebbe sicuramente possibile rispetto allo schema *criptovaluta sporca – denaro pulito*, che venga poi impiegato nelle predette attività.

Inoltre, il crescente utilizzo della criptovaluta anche come mezzo di pagamento scelto dai privati induce a ritenere che la fattispecie considerata possa astrattamente venire in rilievo anche negli altri due schemi considerati.

Rispetto alle *attività economiche* deve osservarsi che, sebbene la giurisprudenza intervenuta in materia abbia negato la possibilità di ammettere conferimenti societari in criptovalute in ragione della loro volatilità, parte della

---

[294] Cass. pen. Sez. II, sent. n. 26796/2021.

dottrina ammette detta possibilità ogniqualvolta la criptovaluta sia suscettibile di valutazione economica, coerentemente al disposto degli artt. 2464, comma 2, c.c. e 2481 bis c.c[295].

Quanto alle *attività finanziarie*, intese come aventi ad oggetto gli strumenti finanziari, deve osservarsi che con D.L. n. 25/2023, convertito con modificazioni dalla L. 52/2023, è stato modificato l'art. 1, comma 2, TUF, così ammettendo la possibilità che gli strumenti finanziari contenuti nell' Allegato I, Sezione C del TUF possano essere emessi da tecnologia a registro distribuito.

In tal senso, la fattispecie incriminatrice richiamata potrebbe venire in rilievo anche nelle ipotesi in cui la criptovaluta provento del delitto sia utilizzata per svolgere le attività considerate.

2.5.4.3 *L'art. 648 ter.1. c.p. e criptovalute.*

L'art. 648 *ter*.1. è stato introdotto dall'art. 3, L.186/2014, recante *Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio*, in attuazione della Convenzione penale di Strasburgo del 1999 sulla *corruzione*, ratificata in Italia con L. 110/2012 e la Convenzione ONU *contro il crimine organizzato transazionale*, adottata dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001, ratificata in Italia con L. 146/2006.

Il legislatore con l'introduzione dell'*autoriciclaggio* ha inteso elidere il *privilegio di non punibilità* riconosciuto all'autore del reato presupposto. Ed invero, prima dell'introduzione della fattispecie in analisi, il soggetto che operava sul bene proveniente dal reato da lui stesso commessoera punito in base all'art. il 12 *quinquies* del D.L. 306/92 *trasferimento fraudolento e possesso ingiustificato di valori*[296]: in tal caso veniva richiesto che il soggetto tenesse il suo comportamento per soddisfare il dolo specifico di «*eludere le disposizioni di legge in materia di prevenzione o di contrabbando*».

La recentissima incriminazione prevede che venga punito chi, avendo commesso un delitto doloso o avendo concorso nella realizzazione dello stesso, *impieghi*, *sostituisca, trasferisca* il denaro, i beni o le altre utilità provenienti dalla commissione di un reato presupposto, in attività economiche,

[295] Si rinvia a S. A. CERRATO, *Conferimento di criptoattività in società*, in S. CAPACCIOLI (a cura di), *Criptoattività*, op. cit, p. 203 ss.
[296] «*salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o la disponibilità del denaro, beni o altre utilità 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* (ora anche il 648 ter) *del codice penale, è punito con la reclusione da due a sei anni*.»

imprenditoriali o speculative, per occultarne concretamente l'origine delittuosa.

Con tale previsione il legislatore ha voluto, da un lato, eliminare o quanto meno limitare la lacuna punitiva dovuta alla *clausola di sussidiarietà* inserita negli artt. 648 *bis,* 648 ter c.p.; dall'altro lato, invece, si è voluto prevedere uno strumento più severo nella lotta all'occultamento dei patrimoni illeciti.

Si tenga presente che a livello sovranazionale le Autorità competenti avevano più volte invitato i singoli Stati a prevedere una norma che incriminasse le condotte di *autoriciclaggio*.

Siffatta volontà è stata, peraltro, ribadita nella Direttiva 2018/1673/UE sulla *lotta al riciclaggio mediante il diritto penale*, nella parte in cui ha disposto che «*Gli Stati membri dovrebbero assicurare che taluni tipi di attività di riciclaggio siano perseguibili anche quando sono commessi dall'autore dell'attività criminosa che ha generato i beni (autoriciclaggio). In tali casi, laddove l'attività di riciclaggio non si limiti alla mera detenzione o utilizzazione di beni, ma ne implichi anche il trasferimento, la conversione, l'occultamento o la dissimulazione, da cui derivi un danno supplementare oltre a quello già causato dall'attività criminosa, ad esempio mettendo in circolazione beni derivanti da un'attività criminosa e, così facendo, occultandone l'origine illecita, tale attività di riciclaggio dovrebbe essere perseguibile*»[297].

Ciò detto, in ragione della sua formulazione sostanzialmente coincidente con gli artt. 648 *bis* c.p. e 648 *ter* c.p. deve ritenersi la configurabilità dell'ipotesi considerata ogniqualvolta il soggetto autore del reato presupposto commetta una delle condotte descritte dalla norma.

In tal senso, per le considerazioni sopra esposte, deve ritenersi che l'autoriciclaggio sia configurabile rispetto a tutti e tre gli schemi richiamati.

A questo proposito il rischio principale deriva proprio dal fatto che il sistema delle criptovalute è finanziabile da soggetti anonimi. Sono molti gli *users* che vendono Bitcoin ed altre *virtual currencies* in via del tutto privata, senza passare per intermediari finanziari o altre Autorità, quindi pubblicando annunci di vendita sia su *blog* che su piattaforme a questo preposte. La vendita di Bitcoin, in questi casi, si conclude con i metodi di pagamento tradizionali quali carte di debito o ricariche postepay, piuttosto che in contanti. Questa è una possibilità accessibile a tutti: l'acquirente deve unicamente dotarsi di un *wallet* su cui poi deterrà i Bitcoin acquistati, contattare il venditore che pagherà in contanti con un incontro *face to face*. Sono moltissime le modalità di acquisto

[297] Direttiva 2018/1673 del Parlamento europeo e del Consiglio del 23 ottobre 2018, "Considerando" n.11.

di Bitcoin e altrettanti sono gli articoli *online* che spiegano come fare, tra queste citiamo l'utilizzo dei *Contract for Difference* e l'acquisto al dettaglio. Non agevole, inoltre, è il fatto che le transazioni possono verificarsi tra individui di uno stesso Stato, ma anche tra residenti in Stati diversi. E non solo: ognuno potrà detenere molteplici *account*, quindi molteplici portafogli elettronici[298]. È chiaro quindi come un soggetto con un'ingente quantità di denaro liquido, frutto di attività illecita, potrebbe agevolmente ripulire tale provento senza lasciare alcuna traccia. Proprio in questo consiste, nell'ordinamento italiano, l'art. 648 *bis* c.p. precedentemente analizzato, quindi le sue derivazioni rinvenibili agli artt. 648 *ter*, 648 *ter.1.* c.p.

Inoltre, il proprietario di un *portafoglio digitale* che contenga proventi di attività illecita potrebbe a reimpiegare le criptovalute, trasferendole in paesi non dotati di una normativa antiriciclaggio e convertirle nuovamente in valuta avente corso legale.

A livello internazionale le Autorità giudiziarie hanno più volte rilevato operazioni come quelle finora descritte, potendo in questo modo analizzare il fenomeno in profondità. Si pensi che già nel 2006 il GAFI-FAFT ha affrontato il problema in un *report* avente ad oggetto i nuovi metodi di pagamento. Vi sono stati poi numerosi aggiornamenti al riguardo. In tutti si è dato riconoscimento alle innovazioni tecnologiche e alla loro applicabilità come mezzi di pagamento. Chiaramente però, l'Autorità di prevenzione e controllo ha sottolineato i rischi da queste tecnologie derivanti e ha proposto agli Stati alcune misure da applicarsi in via preventiva. Come previsto nella IV Direttiva antiriciclaggio, anche il GAFI ha sostenuto che è necessario adottare un "approccio basato sul rischio" che possa permettere la regolamentazione dei nuovi strumenti digitali utilizzati nella commissione, tra gli altri, del reato di riciclaggio. Il GAFI-FAFT proprio in virtù della continua e velocissima evoluzione che sta riguardando negli ultimi anni tali strumenti innovativi, ha scelto di non stilare un elenco esaustivo ma linee guida aventi ad oggetto gli strumenti a rischio[299].

Un'analisi approfondita del fenomeno delle criptovalute è stata effettuata dal GAFI-FAFT in un *report* dedicato nel 2014, poi aggiornato negli anni successivi. In questo contesto, l'Autorità internazionale considera le valute virtuali come una *species* del *genus "Internet- based payment service"*, indicando, oltretutto, anche una classificazione, modificabile, delle stesse sulla

---

[298] L. STURZO, *Bitcoin e riciclaggio 2.0.*, in *Archivio Diritto penale contemporaneo,* 5, 2018, p.23, in www.archiviodpc.dirittopenaleuomo.org. reperibile al seguente link.
[299] L. LA ROCCA, *La prevenzione del riciclaggio e finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali,* in *Analisi Giuridica dell'Economia*, Il Mulino- Rivisteweb, Fascicolo 1/2015, p. 205, in www.rivisteweb.it.

base delle caratteristiche della tecnologia e del suo funzionamento. Vengono, inoltre, individuati i soggetti che agiscono nella rete, quindi nella *blockchain*. Anche qui, come avvenuto nella Direttiva 2015/849 vi è una definizione, volutamente vaga di cosa sia una *virtual currencies*: sono descritte come rappresentazioni digitali di valore che funzionano come mezzo di scambio, unità di conto o strumento di conservazione del valore, ma non viene loro riconosciuto il *corso-legale.* Abbiamo già detto, e ancora affronteremo nel prosieguo, della natura giuridica delle criptovalute. Vengono quindi distinte criptovalute *convertibili e non convertibili*: le prime vengono scambiate su un mercato che permette di trasformare le valute virtuali in valuta avente corso legale. Potranno essere centralizzate o decentralizzate a seconda, come sappiamo, che vi sia o meno un soggetto che le emetta e che controlli tale emissione. Evidentemente non è il caso del Bitcoin. Le seconde, invece, non potranno mai rientrare nell'alveo delle *fiat currency* perché utilizzata in un sistema chiuso, come ad esempio il gioco *online.* Sono valute centralizzate che prevedono l'emissione da parte di un soggetto, definito *administrator*, il quale definisce le regole di utilizzo e annota le transazioni nel *central payment ledger.*

Il GAFI, quindi, si concentra sulla criptovaluta Bitcoin, riconoscendo tutte le caratteristiche fin ora descritte e la possibilità che queste, divenute totalmente anonime, possano permettere ai criminali economici di agire indisturbati nella rete.

Ad oggi, le soluzioni prospettate dall'Unione Europea non risultano idonee a combattere i fenomeni ivi descritti. Nel prossimo capitolo cercheremo di comprendere, grazie a uno studio di circolazione dei modelli giuridici, se vi sia qualche ordinamento che abbia coerentemente e opportunamente disciplinato il fenomeno del riciclaggio per tramite di criptovalute. E, qualora vi sia, come e se questa possa essere applicata nell'ordinamento italiano, ancora oggi privo di una regolamentazione idonea ad evitare il riciclaggio di proventi illecite per il tramite di criptovalute, soprattutto quando questo avvenga senza l'intervento di prestatori di servizi, oggi previsti tra i "soggetti obbligati" dalla V Direttiva antiriciclaggio.

2.5.4.4 *...in modo da ostacolare l'identificazione della provenienza delittuosa.*

Tanto l'art. 648 *bis* c.p. quanto l'art. 648 *ter.*1. c.p. richiedono esplicitamente – ancorché nell'art. 648 ter .1. sia precisato che ciò debba avvenire *concretamente*[300] – che le condotte considerate siano tenute in modo

[300] Si tratta di una distinzione solo testuale: anche rispetto all'art. 648 *bis* c.p., infatti, la giurisprudenza richiede che la condotta di riciclaggio sia *concretamente* idonea ad

da ostacolare l'identificazione della provenienza delittuosa dei proventi derivanti dal reato presupposto.

Orbene, alla luce di quanto sin qui detto, non vi è dubbio che le criptovalute siano, in sé, idonee ad ostacolare l'identificazione della provenienza delittuosa del provento. In tal senso, già solo lo pseudoanonimato – caratteristica propria della maggior parte delle valute virtuali – è idoneo a rendere particolarmente difficoltosa l'identificazione della provenienza delittuosa tanto del denaro *sostituito* in criptovaluta, quanto della criptovaluta *trasferita* su altra *blockchain*. Ciò è ancora più vero quando le operazioni hanno ad oggetto le criptovalute anonime (Monero).

Ma vi è di più.

A ben vedere, nei casi in cui provento del delitto sia la criptovaluta, l'ostacolo all'identificazione della provenienza delittuosa sembrerebbe, configurarsi già con la consumazione del reato presupposto. In tali casi, il provento del delitto nasce come *anonimo* o *pseudoanonimo* ed è, *ex se*, idoneo a *nascondere* la sua provenienza delittuosa.

In tal senso, in questi casi, lo scopo del riciclaggio o dell'autoriciclaggio sarebbe sostanzialmente realizzato già con la condotta presupposta, rappresentando così un'ipotesi eccezionale, che non pare potersi verificare quando il provento del delitto sia il *denaro* o un *bene.*

Ciò detto, tale caratteristica delle criptovaluta di anticipare al reato presupposto la capacità di ostacolare l'identificazione della provenienza del delitto non pare incidere sulla configurabilità delle fattispecie richiamate.

Al riguardo può essere richiamata la giurisprudenza di legittimità che ha, più volte, affermato che affinché vi sia ostacolo all'identificazione non è necessario che le condotte si esplichino sul bene trasformandolo o modificandolo parzialmente, dovendosi ritenere sufficiente le condotte che, senza incidere sulla cosa, siano comunque di ostacolo per la ricerca della provenienza delittuosa[301].

Di talché, pare potersi ritenere che ove il reato presupposto sia stato commesso con criptovalute al fine di ostacolare la ricerca della provenienza delittuosa, ciò sarà sufficiente per integrare le modalità di condotta richieste tanto dall'art. 648 *bis* c.p.

---

ostacolare l'identificazione delittuosa del provento riciclato. Cfr. *ex multis* Cass. pen., Sez. II, sent. n. 15092/2007.

[301]Cass. pen., Sez. II, sent. n. 19480/2019; Cass. pen., Sez. II, sent. n. 39702/2019; Cass. pen., Sez. II, sent. n. 56391/2017; Cass. pen., Sez. II, sent. n. 41740/2015; Cass. pen., Sez. II, sent. N. 25940/2013.

3. *Market Darknet e Fraud Shop*

Le potenzialità criminali delle criptovalute sono state fortemente amplificate con la nascita dei *marknet darknet* e dei *fraud shop*, che hanno reso sostanzialmente accessibile a chiunque la possibilità di commettere *cybercrime*, indipendentemente dal possedimento di specifiche competenze informatiche.

3.1 *Market Darknet.*

Sin dalla loro originaria diffusione le criptovalute sono state utilizzate dai criminali economici quale *mezzo di pagamento* richiesto nell'ambito dell'attività illecita svolta.

In particolare, i fatti di cronaca emersi nell'ultimo decennio dimostrano che le valute virtuali sono state utilizzate anche come mezzo di scambio per acquistare beni o servizi di illecita provenienza (quali, a titolo di esempio, armi, droga, materiale pedopornografico…).

Tra i fenomeni maggiormente sviluppati con l'avvento delle criptovalute troviamo i c.d. "*Mercati Darknet*". Trattasi di piattaforme online presenti nel "dark web" che in cui gli utenti possono acquistare e/o scambiare servizi e merci illegali, quali armi, droghe, materiale pedopornografico, ma utile anche per individuare e assoldare *killer*, favorire il traffico di organi e di esseri umani, commissionare reati informatici.

Sebbene dette piattaforme siano esistite sin dall'avvento di Internet, con l'evolversi delle criptovalute gli "affari" sono divenuti più sicuri e meno tracciabili per i soggetti che operano nel *dark web*.

3.1.1 *Silk Road.*

La prima manifestazione si è avuta agli arbori di Bitcoin con la piattaforma Silk Road che vantava circa 100.000 utenti in tutto il mondo, riuscendo a raggiungere ricavi complessivi del valore di circa 1,2 miliardi di dollari l'anno a cui corrispondevano circa 80 milioni di dollari di ricavi annuali per il sito[302].

Il sito si caratterizzava per permettere, da un lato, lo scambio di beni e servizi illeciti (armi, droga, ma anche dati personali) dietro il pagamento di criptovalute e, dall'altro lato, per fornire un servizio interno di *laundering* tramite l'utilizzo di tecnologie di *mixing*.

Più precisamente, Silk Road svolgeva un servizio di intermediazione tra gli utenti, garantito dal collegamento dei portafogli di Bitcoin degli utenti alla

---

[302] G.P. ACCINNI, *Profili di rilevanza penale delle "criptovalute"*, *op.cit.*, p. 15.

piattaforma. In particolare, la forza di Silk Road consisteva nella sua capacità di trasferire la criptovaluta solo una volta che la merce veniva effettivamente ricevuta dall'acquirente, vanificando, così, il rischio di truffa causato dall'irreversibilità delle transazioni.

Inoltre, per ogni transazione la piattaforma non solo garantiva il trasferimento di criptovaluta tra utenti, ma attraverso proprie tecnologie di *mixing* permetteva di eludere lo pseudoanonimato della *blockchain*, rendendo le operazioni non tracciabili.

Silk Road è stato scoperto dal Dipartimento di Giustizia degli Stati Uniti d'America e successivamente chiuso nel maggio 2013.

3.1.2 *Hydra Market.*

La chiusura di Silk Road, tuttavia, non ha sancito la fine dell'utilizzo delle criptovalute quale mezzo di pagamento nei *market darknet*. Risale, infatti, almeno al 2015 la fondazione del sovietico Hydra Market, chiuso solo nell'aprile 2022 a seguito di un'operazione congiunta tra USA – già l'OFAC era intervenuta con numerose sanzioni[303] – e Germania, che ha permesso la confisca di circa venticinque milioni di dollari in Bitcoin. Dalle stime di Elliptic – società attiva sin dal 2011 nello studio della *blockchain*, delle criptovalute e dei reati correlati con riferimento alla gestione del rischio – emerge che Hydra è stato il *market darknet* più longevo della storia con circa 19.000 account di venditori ed oltre 17.000.000 di utenti[304] con un volume di affari complessivo di oltre 5 miliardi di dollari in transazioni Bitcoin[305].

Dalle stime di Chainalysis emerge come Hydra, solo nel 2022 anno in cui è stato chiuso, ha raggiunto in meno di quattro mesi un volume di affari di quasi 600.000.000 di dollari statunitensi[306]; come evidenziato da Elliptic, nel 2021 il volume di affari è stato di circa 1,6 miliardi di dollari (pari a circa il 93,6% del valore economico complessivo di tutti i *mercati darknet*[307]).

La forza di *Hydra* deve essere ricercata nel suo "servizio clienti": la piattaforma, che permetteva principalmente il traffico di droga (ma anche di documenti contraffatti e servizi digitali) operava come un vero e proprio *e-*

---

2. [303] Si rinvia a *OFAC, Press Releases. Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex,* aprile 2022*,* in www.home.treasury.gov , reperibile al seguente link.

[304] A. GREENBERG, *Il più longevo mercato nero nella storia del* dark web *è stato smantellato*, aprile 2022, in www.wired.it , reperibile al seguente link.

[305] ELLIPTIC, *US sanctions Garantex exchange and Hydra dark web marketplace following seizure of Hydra by German authorities*, aprile 2022, in *www.elliptic.co* , reperibile al seguente link.

[306] CHAINALYSIS, *Il report sui crimini crypto del 2023*, *cit.*, pp. 45 ss.

[307] ELLIPTIC, *op.cit.*; CHAINALYSIS, *Il report sui crimini crypto del 2023*, *cit.*, pp. 48 ss.

commerce, attenzionando i servizi di *customer care,* garantendo la "qualità" degli acquisti e la "sicurezza" degli utenti[308]. Al riguardo, Salih Altuntas, agente federale tedesco che ha svolto le operazioni di chiusura del sito, ha dichiarato che "Hydra offriva un servizio in cui gli utenti potevano inviare droghe per testarne la purezza, disponeva di un bot di Telegram che gli utenti potevano contattare per ottenere istruzioni di primo soccorso in caso di overdose e aiutava inoltre i venditori a ottenere assistenza legale nel caso in cui fossero stati perquisiti dalla polizia"[309].

Inoltre, al pari di quanto già avvenuto per Silk Road, il mercato sovietico offriva ai suoi utenti un servizio di *mixing* che permetteva, da un lato, più difficoltosa la tracciabilità delle operazioni e, dall'altro lato, permetteva di convertire le criptovalute ottenute illegalmente – non solo dagli affari finalizzato sulla piattaforma – in moneta avente corso legale (rubli), favorendo anche operazioni di *money laundering*[310].

3.1.3 *Market Darknet post Hydra.*

Dal report di Chainalysis relativo all'annualità 2022 emerge come a seguito della chiusura di Hydra i ricavi dei mercati *darknet* hanno inizialmente riscontrato un'importante flessione – il ricavo medio giornaliero è, invero, sceso da 4,2 milioni di dollari a 447.000,00 dolari – con conseguente ripresa nel secondo semestre del 2022.

I principali successori di Hydra sono *Mega Darknet Market*, *Blacksprut Market* e *OMG!OMG! Mercato*. Gli studi intervenuti in materia mostrano come queste tre piattaforme abbiano ottenuto la loro quota di affari a seguito della caduta di Hydra e con sforzi coordinati finalizzati ad attirare gli utenti del mercato sovietico, garantendo parte dei servizi da questo già offerti (riciclaggio di criptovalute, *customer care*, servizi di consegna a domicilio).

In tale contesto, nei cinquanta giorni successivi alla chiusura di Hydra, vi è stato un predominio di OMG che ha rappresentato quasi un monopolio del *darknet,* salvo poi dividere il mercato con Mega Darknet Market, Blacksprut Market.

---

[308] CHAINALYSIS TEAM, *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, aprile 2022, in www.chainalysis.com, reperibile al seguente link.

[309] CHAINALYSIS, *Il report sui crimini crypto del 2023*, *cit.*, pp. 46.

[310] Hydra forniva un *mixer* interno (Bitcoin Bank Mixer) che permetteva ai venditori di prelevare Bitcoin dalla piattaforma, così da farli apparire puliti *on chain*.

Il report sull'annualità 2023 mostra come i proventi del *market darknet* abbiano subito una variazione in aumento rispetto all'annualità 2022, con introiti pari a circa 2 miliardi di dollari[311].

È interessante notare come, a seguito della chiusura di Hydra, nessuno dei *competitor* sia riuscito ad eguagliarla monopolizzando il *deep web,* con una conseguente frammentazione dei servizi illeciti tra le varie piattaforme.

3.2 *Fraud Shop.*

Accanto ai *market* negli anni si sono sviluppati anche i c.d. *fraud shop*, che operano tipicamente sul *dark web* e mettono in commercio dati sensibili e dati personali utili a facilitare la commissione di frodi informatiche, truffe ed estorsioni tramite *ransomware*.

Tra questi, operava altresì Genesis Market – *fraud shop* con un giro di affari milionario – chiuso solo nell'aprile 2023 a seguito dell'azione "Operation Cookie Monster" intrapresa nell'ambito di un'azione internazionale a contrasto della criminalità economica ed informatica.

Caratteristiche principale di Genesis Market era l'accessibilità.

Innanzitutto, era possibile collegarsi al *fraud shop* senza accedere al *deep web*, ma semplicemente tramite una ricerca su Google, che rinviava al sito, su cui era possibile operare dopo avere creato un *account*. Tale possibilità ha attirato anche criminali "comuni a cui Genesis forniva una guida su come utilizzare illecitamente le credenziali delle vittime, così ampliando il suo "parco clienti" anche a soggetti privi delle capacità e delle conoscenze sino quel momento possedute solo dai *cybercriminal*.

È interessante notare come la facilità di accesso a Genesis Market – possibile a seguito di una semplice ricerca su Google la cui iscrizione era subordinata unicamente all'inserimento di un codice di invito utile a creare un account, senza necessità di operare nel *dark web* – ha attirato criminali comuni, non associabili ai *cybercriminal*, che hanno sfruttato le informazioni acquistate a loro vantaggio.

Ulteriore punto di forza di Genesis Market è da individuare nei servizi offerti: veniva, infatti, data la possibilità di acquistare specifici date per precise operazioni ovvero accedere a tutti i *cookie del browser* delle vittime, che consentivano ai criminali informatici di eludere l'autenticazione a due fattori (2FA) e di creare scompiglio negli *account* delle vittime.

Detto servizio è stato reso possibile dalle modalità con cui operava Genesis: per ottenere il controllo dei computer, il *fraud shop* si serviva di un

---

[311] CHAINALYSIS, *The 2024 Crypto Crime Report*, cit., pp. 89 ss.

indirizzo *Bitcoin legacy*[312] che permetteva di individuare il server di comando e controllo (C2) utilizzato dall'utente, dal quale i criminali informatici avviavano l'accesso remoto ai dispositivi infetti.

Il pacchetto di *malware* conteneva un *plugin* nascosto per il browser basato su Chromium, un web browser libero creato da Google, fatto apparire come un *plug-in* di Google Drive, che registrava le credenziali memorizzate nei browser delle vittime.

Il *software*, inoltre, era in grado di rilevare le intervenute modifiche delle *password* da parte degli utenti vittime di *malware* e di impossessarsi delle nuove credenziali, così di fatto permettendo a chi acquistasse i dati di agire liberamente per conto della vittima ignara, che si ritrovava i conti bancari e DeFi prosciugati.

Peraltro, nel sottrarre i dati dai computer infettati dal *malware*, Genesis vendeva le c.d. "impronte digitali" [313] delle vittime - che chiamava "bot" - sul suo mercato. Ogni *bot* rappresentava un computer o un dispositivo compromesso e le credenziali associate al suo proprietario. Durante la sua attività, Genesis Market ha venduto 1,6 milioni di bot: sul sito web, i *cybercriminal* potevano passare in rassegna centinaia di migliaia di bot, anche filtrando i risultati in base a criteri come il Paese o la ricerca di credenziali legate a un particolare nome di dominio. L'interfaccia utente mostrava quanti accessi e quali *account* conteneva ogni *bot;* più accessi venivano forniti, più costoso era il bot, soprattutto se includeva credenziali di conti bancari o criptovalute. L'interfaccia utente mostrava anche quando il dispositivo della vittima era stato infettato dal *malware* e quando era stato aggiornato l'ultima volta[314].

4. *Delitti contro lo Stato.*

Gli studi condotti da Chainalysis dimostrano che, sebbene in minima parte, le criptovalute vengono utilizzate, altresì, per finanziare le organizzazioni terroristiche[315]. Ciò nonostante, è emerso come, contrariamente a quanto comunemente ritenuto, le valute virtuali, in ragione della sostanziale trasparenza della *blockchain*, non rappresenterebbero uno strumento efficace

---

[312] Il riferimento è agli indirizzi originali di Bitcoin.

[313] Con il termine "digital footprints", tradotto in italiano con "impronte digitali" si fa comunemente riferimento alle tracce digitali lasciate dagli individui nello svolgimento delle loro attività online. Queste *tracce* comprendono i post sui social media, le transazioni online, la cronologia di navigazione, l'attività sui dispositivi mobili etc. Infatti, ogni interazione e comunicazione lascia una traccia di dati che può essere utilizzata per identificare i soggetti, conoscerne i gusti e le abitudini.

[314] Si rinvia a CHAINALYSIS, *The 2024 Crypto Crime Report, cit.*, pp. 99 ss.

[315] CHAINALYSIS, *The 2024 Crypto Crime Report, op.cit.*

nel finanziamento del terrorismo ma, al contrario, permetterebbero il sostanziale tracciamento dei finanziatori.

Ne è un esempio la decisione presa dalle Brigate Al – Qassam (ala militare di Hamas), che hanno rinunciato alle donazioni ricevute in criptovalute proprio in ragione della tracciabilità dei donari. In particolare, la scelta è stata determinata da una fuga di notizie che correlava l'attacco a Israele del 7 ottobre 2023 e le ingenti somme in criptovalute ricevute in donazione da Al Qassam nei giorni immediatamente precedenti.

4.1 *Finanziamento del terrorismo: rete intermediari e crowdfunding.*

D'altra parte, nel 2023, l'Ufficio Nazionale Israeliano per il Contrasto al Finanziamento del Terrorismo (NBCTF) ha annunciato il sequestro di 1,7 milioni di criptovalute destinate a Hezbollah[316] e alla Forza Quds dell'Iran[317].

L'operazione condotta dal NBTCF ha permesso di svelare una prima modalità di finanziamento del terrorismo, che si basa sulla collaborazione di una rete di intermediari, destinatari di somme in criptovalute oggetto, almeno apparentemente, di transazioni lecite.

Ad esempio, Hezbollah si avvaleva, quali intermediari, di imprese di servizi monetari che, in ragione dell'attività svolta, attiravano meno attenzioni. Nel caso in esame, venivano sfruttati tanto i c.d. "broker over-the- counter" (OTC) – noti per gestire un volume significativo di transazioni – quanto i c.d. "hawala", costituiti da una rete di intermediari, capaci di svolgere operazioni su scala ridotta.

Siffatta modalità di finanziamento è idonea a facilitare le transazioni illecite, limitando i rischi di scoperta. È bene, invero, precisare come non tutte le operazioni svolte da questi intermediari hanno finalità illecite, di talché vi è un preciso mescolamento tra transazioni lecite e transazioni criminali, che aumentano le difficoltà di individuazione e scoperta delle operazioni di finanziamento al terrorismo, talvolta all'insaputa delle piattaforme coinvolte.

Inoltre, dette organizzazioni tendono a servirsi di intermediari che non siano destinatari di sanzioni o che non siano stati segnalati a causa dell'evidente vicinanza con determinati gruppi terroristici, da eludere i controlli cui sono sottoposti i fornitori di servizi *crypto* (c.d. VASPs – *virtual asset service providers*).

In tal senso, storicamente Hezbollah ha potuto contare sull'intermediazione svolta da un tale noto come Tawfiq Muhammad Said Al-

---

[316] Hezbollah, nata nel 1982 come organizzazione paramilitare islamista sciita e ansionista libanese, oggi è un importante partito politico libanese.
[317] Organizzazione militare iraniana.

Law. Costui, servendosi di portafogli digitali a lui intestati, aveva costruito una rete di scambi apparentemente leciti, che ha permesso ad Hezbollah di ricevere donazioni in criptovalute per oltre un miliardo di dollari. Ed invero, Al-Law movimentava i fondi avvalendosi di una rete di *exchange* leciti e di altri fornitori di servizi, che talvolta ignari delle reali finalità delle operazioni compiute, contribuivano a celare la fonte, la destinazione e lo scopo delle transazioni. Si pensi che Chainalysis ha stimato che su 904 trasferimenti totali partiti da portafogli facenti capo a Said Al-Law, almeno 145 operazioni hanno visto coinvolte le borse tradizionali.

Altra modalità di finanziamento del terrorismo tramite criptovalute, favorita da gruppi terroristici come ISIS e Hayat Tahrir Al – Sham, è rappresentata dal *crowdfounding*.

Si tratta di campagne di donazione pubbliche che si celano dietro finalità di beneficienza.

Detta tecnica, ancorché meno sofisticata rispetto alla creazione di una rete di intermediari, ha comunque permesso il trasferimento di fondi a favore delle attività terroristiche svolte da alcuni gruppi.

È quanto avvenuto, ad esempio, nel caso di Farrukh Furkatovitch Fayzimatov, un cittadino tagico, *recruiter* del gruppo terroristico Hay'at Tahrir Al-Sham (HTS), che si serviva dei *social media* per favorire operazioni di finanziamento di HTS, indicando nei post pubblicati l'indirizzo digitale a cui devolvere Bitcoin, riuscendo a raccogliere fondi per oltre 12.000,00 dollari.

4.2 *Finanziamento del terrorismo.*

Occorre, a questo punto, indagare la riconducibilità delle condotte descritte alle fattispecie incriminatrici contenute nel Libro II, Titolo I, del c.p.

In particolare, con riferimento alla condotta di *finanziamento,* è necessario fare riferimento agli artt. 270 *bis* c.p., 270 quinquies.1. c.p, preliminarmente analizzando i rapporti tra le due norme.

L'art. 270 bis c.p., rubricato *associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*, punisce "chiunque promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico*".*

La giurisprudenza di legittimità è unanime nel ritenere che "Il bene giuridico protetto dall'art. 270 bis c.p. (…) è l'ordinamento costituzionale italiano, dovendosi escludere quindi la configurabilità del reato quando la finalità suddetta che connota il programma di atti violenti riguardi uno Stato straniero"[318] .

In tal senso, nel caso in cui il programma dell'associazione riguardi uno Stato straniero, dovrà ritenersi applicabile l'art. 270 *quinquies*.1., rubricato *finanziamento di condotte con finalità di terrorismo*, che punisce "chiunque, al di fuori dei casi di cui agli articoli 270-bis e 270-quater.1, raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'articolo 270-sexies[319] è punito con la reclusione da sette a quindici anni, indipendentemente dall'effettivo utilizzo dei fondi per la commissione delle citate condotte".

4.2.1 *…con l'utilizzo di criptovalute.*

Orbene, ciò detto le condotte di finanziamento sopra descritte paiono sussumibili nelle fattispecie incriminatrici richiamate solo in parte.

Ed invero, mentre l'art. 270 *bis* c.p. è stato costruito dal legislatore prevedendo una condotta di *finanziamento* a forma libera – non specificando in che termini e con quali modalità la stessa si debba realizzare –, nell'ipotesi in cui il finanziamento riguardi uno Stato straniero, per il perfezionamento dell'art. 270 *quinquies*.1. c.p. è stato previsto che l'*erogazione* o la *messa a disposizione* possa avere ad oggetto unicamente *beni* o *denaro*.

Ne consegue che, allo stato, il finanziamento del terrorismo tramite l'utilizzo di criptovalute costituisce reato unicamente nell'ipotesi in cui la predetta erogazione sia diretta nei confronti di associazioni con finalità di terrorismo o di eversione dell'ordine democratico italiano. Ed invero, per le ragioni già analizzate, le criptovalute non paiono qualificabili alla stregua di *beni* o *denaro*[320] con la conseguente inapplicabilità dell'art. 270 *quinquies*.1. c.p. al soggetto che eroghi criptovalute nei confronti associazioni con finalità di terrorismo rivolte *unicamente* a un Paese diverso dall'Italia o ad un'organizzazione internazionale.

---

[318] Cfr., *ex multis*, Cass. pen., Sez. VI, sent. n. 973/1996; Cass. pen., Sez. VI, sent. n. 737/1999.

[319] La norma richiamata qualifica quali *condotte con finalità di terrorismo* "le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia".

[320] Cfr. *supra,* Capitolo II, §7 *La natura giuridica delle criptovalute*.

Dalla clausola di sussidiarietà con cui si apre l'art. 270 *quinquies*.1. c.p. può, infatti, ragionevolmente ritenersi che ove un'associazione abbia finalità terroristiche rivolte tanto all'ordinamento statale italiano quanto a un altro Paese o a un'organizzazione internazionale – ne è un esempio l'ISIS – prevarrà l'applicazione dell'art. 270 *bis* c.p. con la conseguenza che anche le erogazioni in criptovalute potranno essere punite in quanto penalmente rilevanti.

Gli studi condotti in materia, le casistiche riportate suggeriscono, tuttavia, come spesso i finanziamenti più cospicui vengono devoluti ad associazioni terroristiche che hanno specifiche finalità rivolte a Paesi o organizzazioni internazionali diversi dall'Italia. È il caso, ad esempio, dei sopracitati gruppi Hazbolla e Forza Quds dell'Iran.

Appare, pertanto, opportuno un intervento del legislatore italiano in modifica dell'art. 270 *quinquies*.1. c.p., che preveda anche la rilevanza penale di erogazioni in criptovalute, sicché il bene giuridico tutelato dalla norma possa trovare effettiva protezione anche a fronte dell'evolversi della tecnologia e delle modalità di finanziamento.

5. *Le ultime frontiere.*

È necessario, ora, affrontare quelle che sono le *ultime frontiere* dell'utilizzo criminale delle criptovalute. In tal senso, non si farà riferimento unicamente a condotte che sono venute in rilievo nell'ultimo anno, ma si valuterà anche la possibile rilevanza penale di condotte che, ancorché non ancora manifestatisi – in quanto probabilmente rientranti nella c.d. *cifra nera* – potrebbero essere incentivate dall'utilizzo delle criptovalute.

5.1 *Le sanzioni.*

Nelle annualità 2022 e 2023 le criptovalute sono state impiegate quale strumento di elusione delle sanzioni imposte dagli Stati.

Le sanzioni – anche dette *misure restrittive* – sono strumenti di politica estera imposti – in via definitiva o temporanea – da uno Stato al fine di influenzare il comportamento degli attori colpiti. Si tratta, invero, di misure che possono essere rivolte tanto nei confronti governi quanto di individui, entità e gruppi terroristici.

È possibile distinguere le sanzioni *finanziarie* dalle sanzioni *commerciali.*

Mentre le sanzioni finanziarie, tendenzialmente, si rivolgono a persone fisiche o giuridiche che vengono indicate in apposite liste e possono consistere in *asset freeze*[321] o *travel ban*[322]; le *sanzioni commerciali*, colpiscono – di regola – un intero Paese e possono colpire i procedimenti di importazione e di esportazione di beni e servizi.

Deve, al riguardo, precisarsi che – contrariamente a quanto si potrebbe pensare – le misure restrittive previste riguardano solo indirettamente gli Stati o i soggetti sanzionati: tenuti al rispetto delle sanzioni sono i cittadini dello Stato sanzionante, cui direttamente si rivolge la disciplina in materie.

È bene evidenziare come le sanzioni possano essere applicate in presenza di presupposti diversi a seconda dell'autorità competente ad irrogarla. Ad esempio, un'importante differenza – che è utile rimarcare ai fini della trattazione – intercorre nella disciplina delle sanzioni applicate dall'Unione Europea e dagli Stati Uniti d'America.

5.1.1 *Le sanzioni nell'Unione Europea.*

In ambito europeo, la decisione di imporre sanzioni è assunta dal Consiglio, di propria iniziativa, su proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza o degli altri Stati membri. Sono tenuti al rispetto delle sanzioni irrogate sia i cittadini dell'Unione Europea, ovunque essi si trovino, sia le persone giuridiche che agiscano sul territorio dell'Unione. La verifica del rispetto delle misure restrittive disposte a livello unionale da parte dei cittadini, tuttavia, è rimessa agli Stati membri, cui compete la definizione di "violazione della sanzione" e l'individuazione di una efficace risposta sanzionatoria[323].

La mancata armonizzazione a livello europeo della normativa sulle sanzioni, a causa delle forti disomogeneità tra le sanzioni, talvolta penali talaltre solo amministrative, ha acuito i rischi di elusione delle sanzioni imposte e di ineffettività delle stesse.

In ragione di ciò, il 28 novembre 2022, il Consiglio ha adottato la decisione 2332/2022, con la quale ha inserito la violazione delle misure restrittive dell'Unione tra le sfere di criminalità elencate nell'art. 83, par. 1, 2° comma, TFUE, rispetto alle quali l'Unione può "stabilire norme minime relative alla definizione dei reati e delle sanzioni". Per attuare tale previsione il Consiglio non ha modificato il trattato, ma ha utilizzato la c.d. "clausola

---

[321] La misura c.d. di "congelamento dei beni" comporta il blocco dei conti bancari e delle attività finanziarie relative ai soggetti colpiti dalla sanzione. Si tratta, di regola, di una misura mirata applicata nei confronti di soggetti appartenenti o affiliati a governi o Paesi sanzionati.
[322] Sono i c.d. "divieti di viaggio" in ragione dei quali il soggetto sanzionato non può entrare nel Paese che lo ha sottoposto a sanzione.
[323] Si rinvia a www.consiulium.europa.eu.

passerella” contenuta al comma 3 dello stesso paragrafo, che permette al Consiglio di adottare decisioni che individuano “altre sfere di criminalità” rispetto a quelle previste dal 2° comma.

Il 2 dicembre 2022 la Commissione, responsabile ai sensi dell’art. 215 TFUE delle misure restrittive adottate dall’UE, ha presentato una proposta di direttiva in materia, volta a stabilire norme minime relative alla definizione dei reati e delle sanzioni previste per la violazione delle misure restrittive dell'UE.

Successivamente, il 9 giugno 2023, il Consiglio ha concordato la sua posizione per armonizzare, a livello degli Stati membri, i reati e le sanzioni per la violazione delle misure restrittive dell'UE. Il progetto di direttiva definisce quale tipo di comportamento costituisce reato e le sanzioni del caso.

Dalla bozza presentata, si evince che, tra le azioni che l’Unione intende perseguire rientrerebbero a) aiutare soggetti destinatari di misure restrittive dell'UE a eludere un divieto di viaggio; b) commerciare beni oggetto di sanzioni ed effettuare operazioni con Stati o entità oggetto di misure restrittive dell'UE; c) prestare servizi finanziari o effettuare attività finanziarie vietati o limitati a causa delle sanzioni; d) eludere i controlli sulla riconducibilità di fondi o risorse economiche a persone fisiche o giuridiche e a organismi sanzionati dall’UE; e) l'istigazione, il favoreggiamento e il concorso in tali reati.

Più precisamente, gli Stati membri, nel recepire le indicazioni della Direttiva, da un lato, dovranno assicurare che la violazione delle misure restrittive dell'UE sia punibile con sanzioni penali effettive, proporzionate e dissuasive; dall’altro lato, dovranno intensificare le misure idonee a garantire il rispetto delle sanzioni imposte dall’UE, tramite la previsione di precisi termini di prescrizione e dell’effettiva applicazione di misure ablatorie – sub specie di *confisca* – dei proventi derivanti dalla elusione o dalla violazione delle anzidette misure restrittive.

In tal senso, l’Unione ha disposto che la violazione intenzionale delle sanzioni debba prevedere, nei casi più gravi, la pena della reclusione, con una cornice edittale da uno a cinque anni, in ragione della gravità del reato. È ammessa la possibilità che gli Stati Membri prevedano condanne più severe, anche in comminatoria congiunta con la pena pecuniaria.

È stato, peraltro, previsto che possano essere ritenute responsabili dei reati previsti dalla direttiva anche le persone giuridiche che abbiano agito nell’interesse o a vantaggio dell’impresa. Sul fronte italiano, dunque, ci si aspetta una modifica al d.lgs. 231/2001, che dovrà prevedere nel catalogo dei reati presupposti, anche le condotte considerate dalla direttiva[324].

[324] Cfr.*infra,* Capitolo III, §7. *La responsabilità dell’ente e l’utilizzo di criptovalute.*

Da ultimo, in data 12 marzo 2014 il Parlamento Europeo ha approvato la Direttiva, che deve essere ancora formalmente approvata dal Consiglio, prima che possa diventare legge. Entrerà in vigore venti giorni dopo la sua pubblicazione nella Gazzetta ufficiale dell'UE, dopodiché che gli Stati membri avranno un anno per recepirla nella legislazione nazionale.

5.1.2 *USA.*

Le sanzioni USA – irrogate dall'OFAC – è subordinata alla a presenza di un qualsiasi *US nexus*, ivi incluso l'utilizzo del dollaro[325]. Ed invero, sono tenuti al rispetto delle sanzioni applicate dagli USA tutti i cittadini statunitensi, ovunque si trovino; gli stranieri permanenti negli USA, ovunque si trovino; le persone giuridiche costituite secondo la legge americana; tutte le organizzazioni e le persone giuridiche con sede negli USA; tutte le società e gli enti di proprietà o controllati da cittadini statunitensi.

Particolarità tutta statunitense deve essere ricercata nelle c.d. *sanzioni secondarie*, che colpiscono gli attori di Paesi terzi che – ancorché non sottoposti direttamente a sanzione (c.d. sanzioni primarie) – intrattengono rapporti economici con regimi, persone e organizzazioni sottoposte a sanzioni primarie.

È bene evidenziare come le *sanzioni americane*, in ragione dell'ampiezza dei c.d. *Us nexus* sono particolarmente afflittive. Ed invero, il dollaro americano svolge un vero e proprio ruolo di moneta internazionale nel mercato economico mondiale. È stato, in tal senso, osservato come "il dollaro assume, in via prevalente a livello globale, tutte e tre le funzioni monetarie: è la principale unità di conto per la denominazione dei debiti transfrontalieri, nonché dei prezzi di materie prime, beni e servizi scambiati sui mercati internazionali; è il più diffuso mezzo di pagamento per il regolamento delle transazioni reali e finanziarie; ed è lo strumento di riserva privilegiato tanto dalle banche centrali quanto dagli operatori finanziari privati. Ciò ne fa la moneta egemone nel sistema monetario internazionale"[326].

Si comprenderà, allora, come in presenza di una sanzione prevista dagli USA, stante anche la previsione delle c.d. *sanzioni secondarie,* il soggetto destinatario della misura restrittiva subirà profonde conseguenze economiche e finanziarie, destinate ad acuirsi quando ad essere sanzionato è un intero Paese.

A fronte di ciò, tanto i soggetti sanzionati quanto coloro che subiscono la misura restrittiva imposta dagli USA (ad esempio, le imprese americane)

---

[325]Si rinvia a www.ofaclawyer.net

[326] L. FANTACCI, L. GOBBI, D. LUCIANI, *Bene pubblico globale o arma finanziaria? L'egemonia del dollaro alla prova delle sanzioni*, in *Moneta e Credito*, vol. 75 (298), 2022, pp. 123-147, in www.rosa.uniroma1.it , reperibile al seguente link.

hanno immediatamente compreso le potenzialità delle critptovalute come strumento di vanificazione delle misure restrittive loro imposte.

5.1.3 *Sanzioni e criptovalute.*

Dagli studi condotti da Chainalysis è emerso come, solo nel 2023, gli afflussi di criptovalute verso entità e giurisdizioni sanzionate hanno rappresentato il 61,5% di tutto il volume delle transazioni illecite complessivamente operate, pari a 14,9 miliardi di dollari.

Più precisamente, ì rispetto al 2022, anno in cui l'OFAC ha sanzionato principalmente soggetti prestatori di servizi – quali *market darknet* (Hydra)[327] e *mixer* (Tornado cash)[328] –, nel 2023 le sanzioni hanno riguardato, principalmente persone fisiche, ad eccezione del *fraud shop* Genesis Market[329] e del *mixer* Sinbad.io[330].

5.1.3.1 *Dagli USA all'Europa: le criptovalute quale strumento di elusione delle sanzioni.*

Il fenomeno in analisi si è manifestato per la prima volta negli USA a seguito delle sanzioni imposte all'Iran e alla Corea del Nord che per primi sono riusciti ad eludere le sanzioni loro imposte in via *diretta* e *indiretta*[331].

Più precisamente, si verifica elusione in via *diretta* quando le criptovalute vengono utilizzate sia per evitare l'uso del dollaro sia per garantire lo (pseudo)anonimato tanto ai soggetti cui sarebbe direttamente precluso intrattenere rapporti commerciali con i sanzionati (ad esempio, i cittadini americani) quanto a coloro che, pur non appartenendo a nessuna delle categorie c.d. "nexus", rischierebbero di incorrere nelle c.d. *sanzioni secondarie*.

Ad esempio, l'Iran – sotto embargo USA – ha eluso in via diretta le sanzioni, utilizzando le criptovalute quale metodo di pagamento per l'acquisto o la vendita di beni e/o servizi, altrimenti bloccati a causa dell'utilizzo del dollaro, in criptovalute.

---

[327] Si rinvia *supra,* Capitolo III, § 3.1.2. *Hydra Market.*
[328] Si rinvia *supra*, Capitolo II, §3.2. *I crypto mixer.*
[329] Si rinvia *supra,* Capitolo III, § 3. *Market Darknet e fraud shop.*
[330] Anche Sinbad.io, al pari di TornadoCash, è stato utilizzato da Lazarus Group per riciclare le criptovalute sottratte: gli studi al riguardo hanno dimostrato come Sinbad.io sia stata la piattaforma con cui Lazarus ha riciclato gran parte dei proventi, pari a 665,4 milioni di criptovalute. Cfr. "*The 2024 Crypto crime Report*", *op.cit.*, pp. 71 ss.
[331] W.A.Reinsch, A. L. Palazzi, *Cryptocurrencies and U.S. Sanction Evasion: implications for Russia*, in *Center for Strategic and International Studies*, dicembre 2022, in www.csis.org, reperibile al seguente link.

L’elusione in via indiretta, invece, si verifica quando le valute virtuali vengono utilizzate dai soggetti o dai Paesi inseriti nelle *sanction list* per mitigare il deficit finanziario causato dalla previsione della misura restrittiva.

L’Iran, in tal senso, ha impiegato le risorse di petrolio invendute nell’attività di *mining* di criptovalute, poi convertite in moneta avente corso legale. Non è un caso che l'"Iran continua ad essere uno dei principali utilizzatori di criptovalute, con decine di *exchange* nel Paese da cui passano transazioni del valore di miliardi di dollari.

Diversamente, la Corea del Nord ha assoldato – se non addirittura fondato – il gruppo di hacker “Lazarus Group”, affinché sottraesse con l’utilizzo delle tecniche di *hacking*, *phishing* e *ransomware* ingenti somme in criptovalute, con successivo riciclaggio dei proventi, poi immessi nell’economia di Stato.

5.1.3.2 *Il conflitto Russia-Ucraina: l’Unione Europea.*

La problematica è tornata in auge con l’inizio del conflitto Russia-Ucraina, coinvolgendo più da vicino anche l’Unione Europea che, a seguito dello scoppiare del conflitto, ha inserito la Russia nelle liste dei paesi sanzionati.

Gli interrogativi, invero, hanno riguardato sia l’utilizzo delle criptovalute come strumento elusivo delle sanzioni sia il loro impiego come strumento per alimentare il conflitto.

A ben vedere, parte della dottrina intervenuta in materia ha categoricamente negato la possibilità che la Russia possa mitigare gli effetti delle sanzioni internazionali ricorrendo alle criptovalute. Chi ha sostenuto ciò ha addotto quattro diverse ragioni:

1) L’industria delle criptovalute sarebbe troppo piccola per soddisfare le esigenze di una nazione sovrana come la Russia. Sarebbero necessari centinaia di miliardi di dollari per mitigare gli effetti delle sanzioni, mentre l'intero mercato delle criptovalute ammonta a circa 2.000 miliardi di dollari;

2) Il sistema SWIFT BIC, che consente di effettuare transazioni estere in modo rapido e sicuro, elabora ogni giorno in media 42 milioni di messaggi finanziari. Efficienza che non può essere replicata da una tecnologia finanziaria decentralizzata;

3) l'uso di una tecnologia pubblicamente accessibile – qual è la *blockchain* – sarebbe inefficace per svolgere le attività illecite, in quanto il libro mastro aperto rende i movimenti di denaro più tracciabili rispetto all'uso di altri beni come il contante o l'oro;

4) l'idea che alcune criptovalute possano essere utilizzate per aggirare le sanzioni dipende dal fatto che questo asset venga effettivamente raccolto per un uso diffuso, cosa che al momento non avverrebbe[332].

Ciò nonostante, gli episodi che hanno visto protagoniste Iran e Nord Corea in uno con le ormai note potenzialità criminali delle criptovalute, nonostante la presenza di un registro pubblico delle transazioni, ha indotto le Autorità europee ad interrogarsi in ordine all'efficacia di dette sanzioni nel conflitto Russia-Ucraina.

Per questo motivo, nell'ambito della direttiva UE 1226/2024, pubblicata in Gazzatta Ufficiale dell'Unione Europea in data 24.04.2021,
volta ad introdurre l'elusione delle sanzioni nelle sfere di criminalità, , all'art. 3, rubricato *Violazioni delle misure restrittive dell'Unione,* è previsto che costituisce reato "eludere una misura restrittiva dell'Unione nei seguenti modi:

i) con l'utilizzo, il trasferimento a terzi o la cessione in altro modo di fondi o di risorse economiche direttamente o indirettamente posseduti, detenuti o controllati da una persona, entità od organismo designati, e che sono congelati in virtù di una misura restrittiva dell'Unione, allo scopo di occultare tali fondi o risorse economiche;
ii) con la comunicazione di informazioni false o fuorvianti allo scopo di occultare il fatto che una persona o entità designata o un organismo designato sia il titolare effettivo o il beneficiario finale di fondi o di risorse economiche che dovranno essere congelati in virtù di una misura restrittiva dell'Unione;
iii) con il mancato rispetto, da parte di una persona fisica o di un rappresentante di un'entità od organismo designati, dell'obbligo, che costituisce una misura restrittiva dell'Unione, di segnalare alle autorità amministrative competenti fondi o risorse economiche ad essi appartenenti o da essi posseduti, detenuti o controllati nella giurisdizione di uno Stato membro;
iv) con il mancato rispetto dell'obbligo, che costituisce una misura restrittiva dell'Unione, di fornire alle autorità amministrative competenti informazioni riguardanti fondi o risorse economiche congelati o informazioni detenute su fondi o risorse economiche nel territorio degli Stati membri, appartenenti a persone, entità o organismi designati o da essi posseduti, detenuti o controllati,

[332] *Ibidem*.

e che non sono stati congelati, qualora tali informazioni siano state ottenute nell'esercizio dei doveri d'ufficio;

Le criptovalute, in tal senso, vengono qualificate alla stregua di *fondi* rappresentando – come precisato nel considerando n.11[333] – uno degli strumenti utili ad eludere le criptovalute.

Ne consegue che, una volta adottata la direttiva, gli Stati membri dovranno necessariamente intervenire sulla disciplina vigente, modificandola e prevedendo l'uso delle criptovalute quale mezzo di violazione ed elusione delle sanzioni internazionali nei termini testè descritti.

5.2 *Il Metaverso.*

Con il termine *metaverso* si fa riferimento a una realtà virtuale, alternativa e parallela al mondo reale, in cui le persone, utilizzando Internet, possono vivere delle nuove esperienze immersive, giocando e comunicando tra loro, semplicemente vivendo una vita diversa e parallela rispetto a quella reale.

Sebbene si tratti di un concetto che ha acquisito particolare popolarità negli ultimi anni, è bene evidenziare come, in realtà, la comparsa di un *mondo virtuale* sia stata concepita sin dalla fine degli anni '70, con la comparsa dei *domini o dimensioni multiutente* (Multi-User Domains or Dimensions, c.d. MUD), che assumevano la forma di giochi basati sul testo.

I MUD si sono poi evoluti in MUD Object Oriented (MOO), *social network* virtuali basati sul testo, a cui la grafica è stata introdotta solo a partire dagli anni '80.

Risale, invece, al 1992 la nascita del concetto di *metaverso* come un mondo virtuale in cui le persone, attraverso l'utilizzo di identità virtuali (oggi c.d. *avatar*), possano trascorrere il proprio tempo libero, giocando, comunicando, socializzando tra loro.

Dal punto di vista tecnologico-informatico, vediamo come il passaggio dal Web2 – caratterizzato da un *do ut des* tra le aziende informatiche, che mettono a disposizione le piattaforme, e gli utilizzatori, che offrono in cambio

---

[333] Viene, infatti, previsto che "Union restrictive measures include sectoral economic and financial measures on the provision of financial services or the performance of financial activities. Such financial services and activities include but are not limited to financing and financial assistance, providing investment and investment services, issuing transferable securities and money market instruments, accepting deposits, providing specialised financial messaging services, dealing in banknotes, providing credit rating services, and providing crypto-assets and wallets. The violation of those sectoral economic and financial measures should constitute a criminal offence".

dell'accessibilità alle stesse i propri dati personali – al Web3, basato sui concetti di *decentralizzazione, privacy* e *anonimato* degli *users*, ha inciso anche sulla struttura del *metaverso*.

Ed invero, da un *metaverso centralizzato* (c.d. *Web2 closed corporate metaverse*), di proprietà e sotto il controllo di grandi compagnie tecnologiche, si è passati ad un *metaverso decentralizzato* (c.d. *Web3 open crypto metaverse*), privo di controlli da parte di autorità pubbliche e/o private, in quanto tale accessibile liberamente a tutti gli utilizzatori. Da un punto di vista strutturale, il *metaverso decentralizzato* è, attualmente, sviluppato sulla base del Web3, che sfrutta protocolli *peer-to-peer* (P2P) e la tecnologia *blockchain*. In tal senso, la decentralizzazione e lo (pseudo) anonimato dei soggetti che agiscono nel Metaverso possono comportare – al pari di quanto avviene per le criptovalute basate su tecnologia *blockchain* [334] – gravi implicazioni in punto di tracciabilità di eventuali condotte criminose commesse nel metaverso[335].

5.2.1 *Metaverso e diritto penale.*

Il crescente sviluppo del Metaverso come strumento ormai popolare, in quanto accessibile ai più, impone di riflettere in ordine alla rilevanza giuridica delle operazioni su di esso svolte. Ed invero, l'utilizzo del Metaverso solleva, tra gli altri, una serie di interrogativi che interessano tutte le branche del diritto compreso, ovviamente, il diritto penale.

Si è detto come, storicamente, le nuove tecnologie abbiano rappresentato – e rappresentino tuttora – importanti occasioni di evoluzione delle capacità criminali e delle modalità utilizzate per delinquere.

In tal senso, è stato ha previsto che il Metaverso potrà valere fino a 13 trilioni di dollari entro il 2030 con conseguente aumento delle transazioni illecite[336].

5.2.1.1 *L'offesa nella realtà virtuale.*

In tal senso, appare fondamentale comprendere quali siano le condotte criminose realizzate e realizzabili nel metaverso, gli ostacoli alla loro individuazione e alla successiva identificazione del soggetto agente e quali le possibili soluzioni ai problemi individuati.

---

[334] Cfr. *supra* Capitolo III, §3.1. *La* blockchain.

[335] E. HABER, *The Criminal Metaverse,* in *Indiana Law Journal*, forthcoming 2024, pp. 5-1, reperibile al seguente link; *EUROPOL INNOVATION LAB*, *Policing in the metaverse: what law enforcement needs to know*, 2022, in www.europol.europa.eu, reperibile al seguente link.

[336] CITI, *Life, the Metaverse and Everything*, giugno 2022, in www.citigroup.com, reperibile al seguente link.

È necessario, innanzitutto, delimitare la sfera del penalmente rilevante rispetto alle condotte tenute in questa realtà parallela, interrogandosi circa l'*offensività* di determinate condotte.

Se, invero, non c'è reato senza *offesa* a un bene giuridico, dobbiamo necessariamente comprendere se e quando i beni giuridici tutelati nel mondo virtuale possano considerarsi *offesi* nel mondo reale e se tutte le offese astrattamente manifestatisi possano essere, concretamente, ritenute reato – e, pertanto, punite – nel mondo reale ancorché realizzate nel mondo virtuale.

In materia, Eldar Haber ha proposto di riflettere sulle note teorie dell'*harm principle* – nel prosieguo *teoria del danno patito* – e della *wrongfulness of a conduct*, nel prosieguo *teoria del danno percepito*[337].

La *teoria del danno patito* muove dall'assunto che la punizione sia legittima e necessaria ogniqualvolta la condotta di un soggetto causi un danno ad un altro soggetto.

La *teoria del danno percepito*, al contrario, si fonda sull'immoralità del comportamento per affermarne la rilevanza penale: la condotta è offensiva se viene percepita come tale dal soggetto verso cui è diretta[338].

Prima di rispondere al nostro quesito dobbiamo considerare che le condotte penalmente rilevanti e, quindi, il diritto penale, possono differire da giurisdizione a giurisdizione: è possibile che determinate condotte, lecite in una giurisdizione, siano considerate illecite in un'altra e viceversa.

Parimenti, ulteriori differenze potrebbero sorgere in ordine alle conseguenze derivanti da una stessa condotta, ancorché considerata penalmente rilevante in giurisdizioni differenti: è, invero, possibile che una medesima offesa sia punita diversamente (più o meno severamente) in una o in altra giurisdizione.

Calando detti principi nel caso di specie, secondo i sostenitori della *teoria del danno patito*, la questione posta è puramente ontologica, dovendo l'operatore di diritto interrogarsi circa le conseguenze che la condotta virtuale ha avuto nella vita reale. Se le conseguenze si manifestano unicamente nel

---

[337] E. HABER, *op. cit.*, pp. 15 ss.

[338] È possibile, al riguardo, richiamare la dicotomia tra *concezione realistica* (o *necessariamente lesiva*) e *concezione sostanzialistica* del reato e dell'offesa proposta da Ferrando Mantovani. La *concezione realistica*, in quanto espressione del liberalismo penale, si fonda sulla compenetrazione tra il *principio di offensività* e il *principio di legalità.* In tal senso, costituisce *reato* solo il fatto *necessariamente lesivo* dell'interesse tutelato da una norma prevista dalla legge.
Nella *concezione sostanzialistica*, espressione del socialismo penale, l'illiceità penale della condotta non è dettata dalla legga, ma dai valori della società di riferimento: diviene *tipico* – e quindi previsto dalla legge come reato – il fatto che offende un interesse ritenuto rilevante per la società socialista. Si rinvia a F. MANTOVANI, *Diritto penale*. Parte generale, X Edizione, CEDAM, Padova, 2019, pp. 179 ss.

mondo virtuale, senza interessare il mondo reale, allora l'offesa rimarrà circoscritta al mondo virtuale; il diritto penale non potrà applicarsi alle condotte tenute nel metaverso e, quindi, il soggetto agente non subirà alcuna *pena* nel mondo reale. Al contrario, se l'offesa realizzata nel Metaverso viene percepita anche nel mondo reale, allora, il diritto penale dovrà essere applicato in risposta alla condotta virtuale[339].

La *teoria del danno percepito*, invece, imporrebbe la criminalizzazione di tutte le condotte virtuali percepite come offensive dal soggetto nel mondo reale[340].

Se rispetto a determinati beni giuridici – che coinvolgono, ad esempio, la sfera personale, morale e sessuale degli individui che operano nel metaverso – l'adesione a una o all'altra teoria potrebbe portare a conclusioni diverse circa la criminalizzazione di determinate condotte, detti dubbi non paiono sorgere rispetto a condotte lesive di beni giuridici economici e, quindi, ai c.d. "reati economici".

5.2.1.2 *Metaverso, reati economici e criptovalute.*

Il Metaverso ha un proprio sistema economico, implementato tramite l'utilizzo della *blockchain* e, in particolare, delle criptovalute, degli *smart contract* e dei *digital assets*, ed alimentato da denaro proveniente dal mondo reale.

Ne consegue che tutte le transazioni compiute nel Metaverso influiscono sull'economia reale.

In tale ottica, assumono rilevanza per il diritto penale tutte quelle transazioni *illecite* che, ancorché operate nel Metaverso, producono effetti disfunzionali su beni giuridici economici tutelati nel mondo reale.

In particolare, con riguardo ai reati economici, recenti studi condotti in materia mostrano come il Metaverso rappresenti, al contempo, luogo e strumento di commissione dei reati di truffa, "code-exploit", riciclaggio di denaro[341], finanziamento del terrorismo ed elusione delle sanzioni internazionali[342], celati dietro l'acquisto di beni e servizi nella realtà virtuale (terreni, vestiti, case e tutto quanto necessario a "vivere" nel mondo virtuale).

---

[339] E. HABER, *op.cit.*, pp.18 ss.
[340] *Ibidem.*
[341] Si rinvia a A. R. CASTALDO, *Anti-Money Laundering Strategies and The Metaverse: New Dangers and opportunities,*in *Iura&Legal Systems*, IX, 2022, 4, pp. 94-97, reperibile al seguente link.
[342] Si rinvia a E. HABER, *op.cit.*; EUROPOL INNOVATION LAB, *op.cit.*; ELLIPTIC, *The Future of Financial Crime in the Metaverse. Fighting Crypto-crime in Web 3.0*, 2022, in www.elliptic.com, reperibile al seguente link

Si aggiunga, peraltro, come proprio le caratteristiche del Metaverso, in uno con l'utilizzo delle criptovalute, tendono ad amplificare tanto gli effetti criminali delle operazioni compiute quanto le difficoltà nella loro tracciabilità.

Ed invero, come detto, gli utenti operano nel Metaverso servendosi di *avatar* non direttamente collegati o collegabili alla loro identità reale. Ne consegue, in tal senso, che la tracciabilità e l'identificazione delle transazioni compiute sul Metaverso tramite l'utilizzo di criptovalute sono doppiamente ostacolate tanto dall'adozione dell'*avatar* e dallo (pseudo)anonimato delle criptovalute quanto della doppia decentralizzazione della *blockchain* su cui si basa il Metaverso del *web 3* e su cui si basano le criptovalute.

Inoltre, le operazioni immesse nel Metaverso avvengono tendenzialmente tra privati senza che, dunque, vengano coinvolte piattaforme di *exchange* o *intermediari*, sottoposti a specifici obblighi di registrazione degli utenti.

5.2.1.3 *Prospettive di riforma.*

Nonostante molte, se non tutte, azioni virtuali compiute nel Metaverso comportino precise conseguenze nel mondo reale, ad oggi, non è intervenuta – né a livello europeo né a livello nazionale – alcuna normativa idonea a disciplinare le modalità e le conseguenze dell'agire criminale in questa nuova dimensione.

Sebbene non risultino ancora casi di cronaca giudiziaria che si siano occupati del fenomeno in analisi, è di tutta evidenza che il Metaverso sia divenuto un nuovo strumento di elusione della normativa vigente da parte dei criminali economici.

Ciò in ragione sia delle summenzionate caratteristiche, che ne agevolano – se non, addirittura, garantiscono – l'impunità, sia della semplicità con cui gli stessi possono, da un lato, procurarsi proventi e, dall'altro lato, dell'agilità con cui riescono a reimmetterli nel mercato finanziario, traendo ulteriori profitti anch'essi illeciti.

Non vi è dubbio, allora, che il vuoto normativo, che oggi lascia ampio spazio di manovra ai colletti bianchi, debba essere presto riempito prevedendo una specifica legislazione in materia, che introduca obblighi di registrazione univoca alle piattaforme[343] e dichiarazione dei proventi derivanti dall'attività ivi svolta.

---

[343] Negli ultimi tempi, ad esempio, si parla di un'identificazione univoca per potere accedere ai *social network*: una sorta di *spid* per le piattaforme social, che possa permettere l'identificazione di tutti i soggetti che agiscono *online,* sicché i colpevoli di condotte offensive di beni giuridici tutelati possano essere chiamati a rispondere per le azioni virtuali commesse.

Sul fronte strettamente penalistico, coerentemente con il principio di offensività accolto agli artt. 13, 25 comma 2 e 27 commi 1 e 3 Cost., appare necessario sposare la teoria dell'*harm principle*. Sicché, potranno essere qualificate alla stregua di *reato* unicamente quelle condotte che, ancorché commesse nel mondo virtuale vedono esplicare i propri effetti nel mondo reale. Tra questi rientrano, senza ombra di dubbio, i reati economici.

Al contrario, dovrà escludersi la criminalizzazione di condotte che, sebbene astrattamente offensive nel mondo virtuale, non producano alcun effetto nella realtà (ad esempio, condotte di lesioni e omicidio di avatar…).

5.3 *Discipline in via di definizione.*

Occorre, da ultimo, dar conto dell'evoluzione normativa che sta interessando alcuni ambiti della tutela penalistica e che sarà oggetto di definizione nei prossimi mesi.

Il riferimento è, in particolare, alla tutela del *mercato finanziario criptovalutario* e *dell'interesse dell'amministrazione finanziaria*.

5.3.1 *La tutela del mercato finanziario criptovalutario.*

Parte della dottrina ha ammesso la possibilità che le criptovalute, in presenza di determinati presupposti, possano assurgere a *strumento di investimento*, *sub specie* di *valori mobiliari* o di *prodotto finanziario*.

In tal senso, la diffusione dei *cripto-asset* come forma di investimento finanziario ha sollevato il tema della protezione dell'integrità del mercato e la fiducia degli investitori, tenendo conto delle peculiarità dell'ecosistema digitale.

Gli studi intervenuti in materia hanno, anche da ultimo[344], dimostrato come le tecnologie a registro distribuito, qual è la *blockchain*, possano facilitare la consumazione di *abusivismi* quanto su quello *oggettivo*, tanto sul piano *soggettivo*. Possono, infatti, venire in rilievo condotte abusive con riguardo tanto al ruolo svolto dagli attori del mercato criptovalutario, quanto alla natura del comportamento abusivo[345].

Nel mercato tradizionale tali comportamenti possono essere qualificati, rispettivamente, alla stregua di *abusivismo finanziario* e di *market abuse.*

A fronte di ciò, il riconoscimento della natura finanziaria delle criptovalute – ancorché non in termini assoluti –ha spinto gli interpreti ad

---

[344] CHAINALYS, *The 2024 Crypto Crime, op.cit.,* p. 49 ss.

[345] M. MAUGERI, *Cripto-attività e abusi di mercato*, in *Osservatorio del diritto civile e commerciale*, in Fascicolo Speciale, il Mulino, Riviste Web, Bologna, settembre 2022, pp. 414-434, in www.rivisteweb.it.

interrogarsi circa l'applicabilità della disciplina già prevista a tutela del mercato mobiliare, anche sul fronte penalistico.

5.3.1.1 *Abusivismo "criptovalutario" di exchange e wallet provider.*

Sul *piano soggettivo* il nostro ordinamento, al fine di tutelare il sistema bancario e il sistema finanziario, riserva le attività e i servizi di investimento solo a determinati soggetti, sottoposti a preventivo controllo della Consob e di Banca d'Italia, deputati a vagliare l'affidabilità organizzativa e patrimoniale degli intermediari e degli emittenti in ambito finanziario[346].

Al proposito, già nel 2015, la Banca d'Italia, nella comunicazione *Avvertenza sull'utilizzo delle cosiddette 'valute virtuali'*[347], nell'ammettere la liceità dell'utilizzo delle criptovalute – in quanto non vietate dall'ordinamento – rilevava come "le attività di emissione di valuta virtuale, conversione di moneta legale in valute virtuali e viceversa e gestione dei relativi schemi operativi potrebbero invece concretizzare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati (artt. 130, 131 TUB per l'attività bancaria e l'attività di raccolta del risparmio; art. 131 ter TUB per la prestazione di servizi di pagamento; art. 166 TUF, per la prestazione di servizi di investimento)".

Successivamente, con d.lgs. 90/2017 – attuativo della Quarta Direttiva antiriciclaggio – è stato modificato l'art. 17 *bis*, comma 8 *bis*, L.141/2010, che prevede precisi obblighi di registrazione per i soggetti che esercitano professionalmente nei confronti del pubblico l'attività di cambia valute, anche su base stagionale. È stato, inoltre, disposto che agli *exchanger* e ai *wallet*

---

[346] In dottrina si rinvia a A. R. CASTALDO, *Accesso all'attività bancaria e strategie penalistiche di controllo*, in *Riv. It. dir. proc. pen.*, 1996, p. 81 ss.; R. CANTONE *Abusivismo finanziario: esperienze da un'indagine giudiziaria*, in *Cass. Pen.,* 1996, pp. 3122 ss.; L. CONTI, *Profili penalistici del testo unico sull'intermediazione finanziaria*, in *Dir. pen. proc.*, 1998, p. 548 ss.; C. RUGA RIVA., *L'abusivismo finanziario: questioni giurisprudenziali e profili di illegittimità costituzionale*, in *Riv. trim. dir. pen. econ.,* 2001, 3, p. 531 ss.; R. ZANNOTTI, *Il nuovo diritto penale dell'economia*, Milano, 2008, p. 359 ss.; R. ZANNOTTI, *La tutela dell'accesso al mercato nella prospettiva della lotta contro il riciclaggio: il caso dell'abusivismo*, in *Rivista della Guardia di Finanza*, 1, 2004, p. 33, ss.; R. ZANNOTTI, *La tutela penale del mercato finanziario*, Giappichelli, Torino, 1997, p. 209 ss.; E. MONTANI., *La tutela del corretto svolgimento dell'attività di intermediazione e bancaria*, in A. ALESSANDRI (a cura di), *Reati in materia economica*, Giappichelli,Torino, 2017, p. 232 ss.; D. GUIDI, *Una nuova ipotesi di abusivismo finanziario,* in F. GIUNTA., D. MICHELETTI, (a cura di), *La disciplina penale del risparmio*, Milano, 2008, p. 173 ss.; P. SORBELLO, *L'abusivismo finanziario tra atto giuridicamente lecito e fatto penalmente rilevante*, in *Giurisprudenza di merito*, 2009, p. 2499 ss.

[347] BANCA D'ITALIA, *Avvertenza sull'utilizzo delle cosiddette 'valute virtuali',* 30 gennaio 2015, in www.bancaditalia.it.

provider si applichino anche le previsioni sulla riserva di attività: detti soggetti sono oggi tenuti ad iscriversi a una sezione speciale del registro OAM (Organismo degli agenti in attività finanziaria e dei mediatori creditizio), nel rispetto delle modalità e delle tempistiche definite dal MEF con il decreto del 13 gennaio 2022. Si tratta di presupposti che costituiscono condizione essenziale per l'esercizio legale dell'attività dei prestatori di servizi relativo all'utilizzo di valuta virtuale, in mancanza dei quali è prevista la sanzione amministrativa per esercizio abusivo dell'attività di cambia valute virtuali.

Nonostante ciò, in data 28 maggio 2019, l'UIF nella Comunicazione "Utilizzo anomalo di valute virtuali", nell'analizzare i rischi derivanti dall'utilizzo delle criptovalute, ha ribadito che "È inoltre da considerare l'utilizzo di Virtual asset[348] connesso con sospetti di abusivismo e con violazioni della disciplina in materia di: i) offerta al pubblico di prodotti finanziari, qualora siano promessi rendimenti periodici collegati all'operatività in Virtual asset; ii) prestazione di servizi di investimento, laddove agli investitori sia offerta la possibilità di effettuare "operazioni regolate per differenza aventi come sottostante (anche) valute virtuali" [349].

In tale contesto, l'assenza di norme volte ad estendere anche alle criptovalute la disciplina dettata dal TUF e dal TUB ha imposto negli anni un importante sforzo nomofilattico. Ed invero, lo sviluppo di piattaforme di intermediazione professionale operanti nel mercato di criptovalute, il cui ruolo è oggi pacificamente riconosciuto nell'ambito della normativa antiriciclaggio, ha richiesto di indagare l'applicabilità della disciplina vigente anche agli operatori del mercato criptovalutario; ovvero la necessità di un introdurre una normativa idonea a rispondere alle nuove ipotesi di abusivismo finanziario.

Più precisamente, sul fronte penalistico, la dottrina intervenuta in materia si è interrogata in ordine alla possibilità di ricondurre le condotte di abusivismo tenute da *exchanger* e *wallet provider* – come definiti nel d.lgs. 231/2007, a fronte delle modifiche introdotte dai d.lgs. 90/2017 e 125/2019, in attuazione della Quarta e Quinta Direttiva antiriciclaggio – alle fattispecie incriminatrici dettate dal Titolo VIII, Sanzioni, del d.lgs. 385/1993 (artt. 130-133 TUB), nonché al Titolo I, Sanzioni penali, del d.lgs. 58/1998 (art. 166 TUF)[350].

---

[348] Come specificato dall'UIF in nota, il termine *virtyal asset* è stato utilizzato nella Comunicazione quale sinonimo di *criptovaluta. Cfr.* UNITÀ DI INFORMAZIONE FINANZIARIA PER L'ITALIA, *Utilizzo anomalo di valute virtuali*, *op.cit.,* nota 1.

[349] UNITÀ DI INFORMAZIONE FINANZIARIA PER L'ITALIA, *Utilizzo anomalo di valute virtuali*, 28 maggio 2019, in www.bancaditalia.it .

[350] F. DI VIZIO, *Moderni abusivismi e criptovalute. Tra il mito della completa disintermediazione e la realtà di nuovi intermediari,* in *Discrimen,* aprile 2022, in www.discrimen.it, reperibile al seguente link. Le considerazioni *ivi* svolte, che si

Nonostante gli sforzi esegetici e nomofilattici compiuti, il quadro è improvvisamente mutato – portando con sé tutte le considerazioni svolte – con la pubblicazione del Regolamento UE 2023/1114 "Market in Crypto Asset" (c.d. MiCA), che sembra avere escluso la possibilità di richiamare in materia la disciplina degli strumenti finanziari, mirando all'introduzione di una normativa speciale e parallela dell'intero mercato criptovalutario[351].

In tal senso, alla luce della struttura proposta dal MiCA, che mira a costruire un mercato criptovalutario diverso e indipendente, ma parallelo al mercato tradizionale, è auspicabile l'introduzione di disciplina penalistica *ad hoc*, capace di prevenire *abusi* della disciplina sugli intermediari digitali. Pare, pertanto, potersi ammettere la costruzione di un quadro normativo speculare a quello già previsto dal MiFID II, che tenga conto della struttura e delle

---

condividono, potranno essere richiamate rispetto alla cripto-attività cui, sulla base delle indicazioni che fornirà ESMA, dovrà essere applicata la direttiva MIFID II e, quindi, a livello nazionale, le norme del TUF e del TUB. Si riportano, in sintesi, le conclusioni cui è giunto l'autore.

Rispetto al reato di *abusiva attività di raccolta del risparmio*, disciplinato all'art. 130 TUB, pare doversi negare l'applicabilità della fattispecie richiamata al mercato delle valute virtuali per due ordini di ragioni.

In primo luogo, le criptovalute non sono riconducibili alla nozione di *fondi* (banconote e monete, moneta scritturale o moneta elettronica); in secondo luogo, l'attività descritta dall'art. 130 TUB non è tipica né degli *exchange* – che svolgono attività di cambio – né dei *wallet provider* la cui attività, per definizione, consiste in "servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali" e non anche l'attività di acquisizione di fondi con obbligo di rimborso.

Deve, altresì, escludersi l'applicabilità degli artt. 131 e 132 TUB in materia di abusivismi in attività bancaria e in attività finanziaria, posto che né gli *exchanger* né i *wallet provider* erogano i finanziamenti, come descritti all'art. 106 TUB. Deve, tuttavia, darsi atto di come l'Autore abbia aperto alla possibilità che gli *exchanger,* quantomeno astrattamente, possano abusivamente erogare prestiti in criptovalute ovvero concedere crediti, così aprendo all'applicabilità delle disposizioni considerate.

Risulta parimenti preclusa configurabilità delle disposizioni dettate dagli artt. 131 *bis* e 131 *ter* TUB, stante l'assenza di valore legale delle criptovalute.

Più complessa la questione che ha riguardato l'applicabilità dell'art. 166 TUF in materia di abusivismi nei servizi e nelle attività di investimento. Ed invero, se parte della dottrina ha pacificamente ammesso detta possibilità, peraltro confermata dal formante giurisprudenziale, altra parte ha fortemente criticato detta presa di posizione, rilevando una violazione del divieto di *analogia in malam partem*. In materia si rinvia, a F. CONSULICH, *Nella* wunderkammer *del legislatore penale contemporaneo:* monete virtuali *che causano* danni reali, *op.cit.*; *contra* F. DALAITI, *op.cit.*

[351] La normativa riguardante gli strumenti finanziari potrò avere ad oggetto solo le criptovalute che rispondano alle caratteristiche dettate dalla Direttiva MiFID II e che, a fronte del regolamento MiCA, siano qualificate alla stregua di strumenti di investimento dall'ESMA.

caratteristiche delle criptovalute e della *blockchain,* senza, tuttavia, rinunciare alla tutela dei beni giuridici in gioco[352].

5.3.1.2 *Market abuse.*

Guardando, ora, al piano *oggettivo*, è possibile distinguere diversi comportamenti abusivi che, ancorché già noti nel mercato mobiliare, si manifestano in termini differenti quando hanno ad oggetto cripto-attività.

Il mercato criptovalutario, in quanto libero tanto da regolamentazione quanto da controlli di soggetti intermediari, ha a lungo rappresentato – e, in realtà, rappresenta tuttora – luogo di importanti speculazioni, così differenziandosi dal mercato tradizionale, sottoposto – almeno astrattamente – a stringenti controlli delle Autorità, che vigilano sul suo corretto andamento.

Già nel marzo 2021, da uno studio condotto da Deloitte, emergeva come la capitalizzazione di mercato delle criptovalute avesse raggiunto il record di 1 trilione (mille miliardi) di dollari nel 2021 con un aumento di 1000 volte rispetto all'anno 2018, quando era stato pari a 1 miliardo di dollari. In tal senso, si osservava come fino al 90% del volume di *trading* criptovalutario potrebbe essere stato oggetto di manipolazione[353].

Occorre, dunque, capire se le tutele previste per il mercato finanziario debbano essere, altresì, estese al mercato criptovalutario.

I dubbi circa l'applicabilità o meno delle norme sul *market abuse* dettate dal TUF appaiono oggi superati dal Regolamento MiCA, che al Titolo VI, detta le norme di *prevenzione e divieto degli abusi di mercato relativi alle criptoattività*.

5.3.1.2.1 *Insider trading.*

Nel mercato finanziario, il reato di *insider trading*, disciplinato all'art. 184 TUF, punisce lo sfruttamento di informazioni privilegiate[354], ottenute in

---

[352] Il Titolo V del Regolamento MiCA (artt. 59-85) disciplina l'autorizzazione e le condizioni di esercizio dell'attività di prestatori di servizi criptvalutari (*exchanger* e *wallet provider*). All'art. 111, rubricato *sanzioni amministrative e altre misure amministrative*, il regolamento impone di adottare *almeno* sanzioni amministrative adeguate in relazione *almeno* alle violazioni di specifiche norme, tra cui rientrano, altresì, le disposizioni di cui al Titolo V. è rimessa al legislatore la scelta di introdurre norme penali.

[353] DELOITTE, *Market Manipulation in Digital Assets,* marzo 2021, in www.deloitte.com, reperibile al seguente link.

[354] La nozione di *informazione privilegiata* era originariamente prevista all'art. 181 TUF, abrogato dal d.lgs. 107/2018, che ha rinviato all'art. 7, §§ 1-4, Regolamento UE 596/2014 c.d. MAR.

ragione della propria posizione funzionale, al fine di impiegarle in operazioni di borsa ovvero di comunicarle o trasmettere a terzi[355].

Detta norma si applica agli strumenti finanziari in senso stretto, come previsti dall'Allegato 1, Sez. C, TUF, dovendosi, pertanto, escludere l'applicabilità alle criptovalute.

In particolare, è possibile distinguere tre diverse condotte di *abuso di informazioni privilegiate*[356]:

Una prima ipotesi si verifica quando un soggetto in possesso di informazioni privilegiate acquista, vende o compie altre operazioni per conto proprio o di terzi. Vi è uno sfruttamento della conoscenza dell'informazione privilegiata.

C'è poi la condotta c.d. di *tipping,* che consiste nella comunicazione a soggetti terzi dell'informazione privilegiata, al di fuori dell'esercizio della propria professione.

Infine, può configurarsi *tuyautage* ogni qualvolta il soggetto in possesso dell'informazione privilegiata induca terzi al compimento di una determinata operazione finanziaria.

Ciò nonostante, è possibile ammettere che un fenomeno simile possa manifestarsi anche nel mercato criptovalutario[357].

In tal senso, il regolamento MiCA, agli artt. 86-92 ha introdotto una disciplina volta a prevenire gli abusi di mercato delle criptoattività, sostanzialmente richiamando il contenuto del regolamento UE 596/2014, c.d. *Market Abuse Regulation* (MAR).

Più precisamente, gli artt. 86-89 ripropongono le condotte appena descritte in ambito criptovalutario, auspicando la formulazione di una fattispecie di *insider trading criptovalutario*.

L'art. 86 nel definire l'ambito di applicazione delle norme in materia di abusi di mercato si riferisce a tre categorie di azione: 1) atti compiuti da qualsiasi persona in relazione a cripto- attività ammesse alla negoziazione o in relazione alle quali è stata presentata una richiesta di ammissione alla negoziazione; 2) a qualsiasi operazione, ordine o condotta relativi alle cripto-attività di cui al paragrafo 1, indipendentemente dal fatto che tale operazione,

---

[355] S. SEMINARA, *Diritto penale commerciale, Volume III. Il diritto penale del mercato mobiliare*, Giappichelli, Torino, 2018, pp.72-85.
[356] *Ivi, p.* 81.
[357] Si rinvia a A. VERSTEIN, *Crypto Asset and Insider Trading Law's Domain*, in *Iowa Law Review*, 2019, p. 27, in www.iuowa.edu , reperibile al seguente link. L'Autore riporta quale esempio il caso di dipendenti di un *trading venue* che anticipano la decisione di una piattaforma di negoziare una determina attività digitale ovvero forniscono l'informazione a terzi, sicché possano realizzare importanti guadagni una volta che la decisione venga resa pubblica.

ordine o condotta avvenga in una piattaforma di negoziazione; 3) alle azioni e alle omissioni, nell'Unione e nei paesi terzi, riguardanti le cripto-attività di cui al paragrafo 1.

All'art. 87, comma 1, lett. a) viene proposta una autonoma, ma sostanzialmente speculare, definizione di *informazione privilegiata* rispetto a quella dettata dall'art. 7 MAR in riferimento ai mercati tradizionali. In tal senso, nel mercato criptovalutario si fa riferimento a *informazioni di natura precisa, che non sono state rese pubbliche e che riguardano, direttamente o indirettamente, uno o più emittenti di cripto-attività, offerenti o persone che chiedono l'ammissione alla negoziazione o una o più cripto-attività e che, se rese pubbliche, potrebbero avere un effetto significativo sui prezzi di tali cripto-attività o sul prezzo di una cripto-attività collegata*.

Alla lettera b), poi, è prevista una nozione più ampia di informazione privilegiata, cui fare riferimento in caso di persone incaricate dell'esecuzione di ordini di cripto-attività per conto di cliente. In tal senso, costituiscono informazioni privilegiate anche quelle di *natura precisa trasmesse da un cliente e connesse agli ordini pendenti in cripto-attività del cliente, concernenti, direttamente o indirettamente, uno o più emittenti, offerenti o persone che chiedono l'ammissione alla negoziazione o una o più cripto-attività e che, se rese pubbliche, potrebbero avere un effetto significativo sui prezzi di tali cripto-attività o sul prezzo di una cripto-attività collegata.*

È, quindi, possibile affermare che, al pari di quanto avviene nel mercato finanziario tradizionale, l'informazione per essere *privilegiata* deve rispondere a quattro diversi requisiti: 1) precisione, 2) natura non pubblica, 3) riferimento diretto a uno o più emittenti di criptoattività, 4) idoneità ad influire *significativamente* sul prezzo della criptoattività.

L'art. 87, al comma 2, poi, nel tracciare i confini della *precisione* pare richiamare integralmente l'art. 7, comma 2, MAR, considerando *precise* "le informazioni che fanno ferimento a una serie di circostanze esistenti o che si può ragionevolmente ritenere che vengano a prodursi o a un evento che si è verificato o del quale si può ragionevolmente ritenere che si verificherà e se tali informazioni sono sufficientemente specifiche da permettere di trarre conclusioni sul possibile effetto di detta serie di circostanze o di detto evento sui prezzi delle cripto-attività. A tal riguardo, nel caso di un processo prolungato che è inteso a concretizzare, o che determina, una particolare circostanza o un particolare evento, possono essere considerate come informazioni di natura precisa la futura circostanza o il futuro evento, nonché le tappe intermedie di detto processo che sono collegate alla concretizzazione o alla determinazione della futura circostanza o del futuro evento". Viene, quindi, ammesso che anche una *tappa intermedia in un processo prolungato* può essere considerata un'informazione privilegiata se, di per sé, risponde ai criteri fissati al paragrafo 2 riguardo alle informazioni privilegiate.

Quanto, infine, all'*idoneità* dell'informazione ad influire sul prezzo della criptoattività, l'art. 87, comma 2, n. 4, definisce tali le *informazioni che un possessore di cripto-attività ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni d'investimento.*

La sostanziale sovrapponibilità delle condotte di *insider trading* nel mercato tradizionale e nel mercato criptovalutario viene meno rispetto alla *comunicazione al pubblico di informazioni privilegiate*. Ed invero, mentre nel mercato finanziario è tenuto alla comunicazione al pubblico il solo *emittente*, l'informazione privilegiata criptovalutaria – in ragione della natura decentralizzata del registro su cui avvengono le operazioni – deve essere comunicato al pubblico, oltre che dagli *emittenti*, anche dagli *offerenti* e dalle *persone che chiedono l'ammissione alla negoziazione.*

Al riguardo, è stato osservato come siffatta impostazione permetta di ritenere che anche la nozione di *informazione privilegiata*, ancorché formalmente sovrapponibile a quella dettata dal MAR, debba essere sostanzialmente ricostruita guardando alla sfera giuridica di tutti i soggetti tenuti alla comunicazione[358].

5.3.1.2.2 *Manipolazione del mercato.*

Il fenomeno di manipolazione del mercato può, tradizionalmente, manifestarsi o tramite *manipolazione informativa* o con *manipolazione operativa.* Mentre nel primo caso vi sarà una diffusione di notizie false, nel secondo caso l'autore porrà in essere appositi artifizi volti ad alterare l'andamento del mercato.

La *manipolazione informativa* può essere realizzata con qualsiasi modalità, mezzo e forma di divulgazione, rivolta a un pubblico indifferenziato o, comunque, vasta. È bene notare come, in questo caso, la notizia non deve riguardare direttamente le condizioni economico-patrimoniali dell'emittente, ma è sufficiente che la stessa, ancorché falsa, sia concretamente idonea ad alterare il prezzo[359].

La *manipolazione operativa*, invece, è subordinata alla diffusione di notizie false o al compimento di altre operazioni simulate idonee ad alterare il prezzo[360].

---

358 M. MAUGERI, *op.cit.*, p. 433.
359 S. SEMINARA, *op.cit.*p. 92 ss.
360 *Ivi,* p. 90 ss.

Gli studi condotti in materia hanno dimostrato come accanto schemi manipolativi tradizionali, si sono sviluppate nuove ed innovative tecniche di manipolazione del mercato.

La criptoattività può, infatti, essere oggetto di *spoofing*[361], di *wash trading*[362], e *pump and dump*[363].

Le prime due tecniche trovano la loro forza proprio nella *decentralizzazione* della rete: un investitore, infatti, può detenere più conti in diverse piattaforme, senza che gli stessi siano *prima facie* a lui riconducibili. Ciò permette di inserire diversi ordini fittizi – che paiano venire da diversi soggetti ma che, in realtà, sono inseriti sempre dallo stesso utente – capaci a trarre in errore gli utenti della *blockchain* che agiranno comportando un rialzo o un ribasso del valore dell'*asset.*

Anche la tecnica del *pump and dump* (PnD) è fortemente utilizzata nel mercato criptovalutario.

A differenza dei mercati finanziari tradizionali, gli schemi di PnD delle criptovalute sono principalmente realizzati e organizzati tramite cosiddetti gruppi di *pump*, attivi sui principali *social network*. il

I gruppi di "*pump*" sono organizzati con una gerarchia distinta e di solito sono composti da tre attori principali: 1) l'organizzatore del pump, 2) i partecipanti al *pump* e 3) i c.d. *pump target exchanger*[364].

---

361 Tale tecnica consiste nell'inserire ordini che non si intende eseguire al fine di creare una spinta al rialzo o al ribasso sul prezzo dell'attività digitale per poi vendere a prezzi artificialmente più alti o acquistare a prezzi più bassi Tra le tecniche di *spoofing* rientra anche il *quote stuffing*, che comporta l'immissione di un importante volume di ordini, che vengono cancellati subito dopo la loro immissione, per rallentare il sistema e approfittare della lentezza operativa degli altri utenti per eseguire le proprie operazioni. Si rinvia a M. MAUGERI, *op.cit.*, p. 420.

362 Prevede la creazione di c.d. *ghost account* da cui generare un volume artificiale di ordini in cui l'utente è controparte di se stesso, si da fornire una falsa impressione di liquidità della criptovaluta. Si rinvia a M. MAUGERI, *op.cit.*, p. 420.

363 Con tale tecnica un soggetto, nella fase di *pump,* diffondendo informazioni fuorvianti sul potenziale di un *asset*, induce a un acquisto di massa che garantisce un aumento di prezzo e conseguenti guadagni per gli iniziali investitori. Una volta raggiunto il valore desiderato, gli organizzatori dello schema avviano la fase di *dump*: vendono tutte le loro posizioni e inondano il mercato causando un'importante perdita per gli investitori entrati nella fase di *pump*.

364 Il riferimento è all'*exchange* scelto dall'organizzatore del *pump* per svolgere l'operazione. Può succedere che sia direttamente la piattaforma *exchange* ad organizzare le operazioni al fine di ottenere tre diversi benefici: 1) può ottenere profitto dalle criptovalute ottenute prima del *pump;* 2) l'elevato numero di transazioni scatenate dal *pump*, gli permetterà di ottenere importanti profitti in termini di commissioni; 3) possono sfruttare la loro posizione per ottenere *informazioni privilegiate*. Si rinvia a J. XU, B. LIVSHITS, *The Anatomy of a Cryptocurrency Pump-and-Dump Scheme*, 2019, in www.researchgate.net, reperibile al seguente link.

Accanto alla tecnica tradizionale di diretto coinvolgimento di soggetti che, più o meno ignari, partecipano al *pump,* nel mercato cripto-valutario l'organizzatore mira ad attirare nel mercato cripto-valutario soggetti diversi dai tradizionali investitori, i c.d. *outsider,* interessati a beneficiare di facili profitti.

È, poi, interessante notare come accanto a questi schemi di condotta c.d. "classici" sia possibile individuare *nuove* condotte manipolative del mercato[365]. Tra le più note rientrano il *rug pull*, lo *stop hunting* e il *51 percent attack*[366]

Una manovra di *rug pull* consiste nel fatto che gli sviluppatori tendono a chiudere improvvisamente un progetto di *asset digitale* pubblicizzato per appropriarsi delle criptovalute degli investitori.

Il c.d. *stop hunting* coinvolge i c.d. "*crypto-whales*", vale a dire soggetti che detengono una grande quantità di una criptovaluta in particolare. Questi si accordano per operare una vendita di massa, che provoca un ribasso improvviso del valore e, quindi del prezzo, che comportano una vendita a catena di tutti i soggetti che detengono quella criptovaluta. Così, una volta che il prezzo dell'*asset* ha raggiunto i minimi storici i *crypto-whales* possono riacquistare nuovamente la criptovaluta, appropriandosi anche delle quote prima detenute da piccoli investitori, coì rafforzando le proprie posizioni originarie, già di vantaggio[367].

Vi è, infine, la tecnica di *51 percent attack*, che permette di alterando la cronologia delle transazioni a proprio vantaggio sfruttando la potenza di calcolo della *blockchain* nelle attività di *mining.* Tale tecnica viene utilizzata dai *miner*, che sono nella posizione di scegliere quali operazioni convalidare e in quale ordine[368].

Anche in questo caso è interessante notare come il legislatore europeo abbia sostanzialmente richiamato la disciplina del MAR adattandola alla cripto-attività.

Ed invero, all'art. 91 il regolamento MiCA ha dettato tutta una serie di attività che possono comportare fenomeni di *manipolazione del mercato criptovalutario.* Si tratta di condotte sostanzialmente coincidenti con quelle già dettate dall'art. 12 MAR, in linea con la volontà – manifestata dal legislatore europeo nel considerando n. 9 del MiCA – di sottoporre il mercato criptovalutario allo stesso regime sanzionatorio e repressivo adottato nella

[365] M. MAUGERI, *op.cit.*, p. 421.
[366] DELOITTE, *Market Integrity Consideration for Digital Asset*, dicembre 2021, in www.deloitte.com, reperibile al seguente link.
[367] *Ibidem.*
[368] A. VERSTEIN, *op.cit.*, p. 48.

finanza tradizionale, nel rispetto del "principio «stessa attività, stessi rischi, stesse norme» e del principio della neutralità tecnologica"[369] .

5.3.1.2.3 *Prospettive future.*

Gli Stati membri devono ora adeguarsi alla disciplina del Regolamento Mica.

A livello nazionale, con Legge n. 15/2024 del 21.02.204, entrata in vigore in data 10.03.2024, il Parlamento ha conferito delega al governo affinché, entro il 10.9.2024, adotti uno o più decreti legislativi per adeguare la normativa nazionale alle disposizioni del Regolamento MiCA.

Quel che emerge dalla legge delega è un sostanziale ampliamento della disciplina dei mercati finanziari a favore del mercato criptovalutario.

In tal senso, *exchange* e *wallet provider* saranno sottoposti, al pari degli intermediari tradizionali, ai controlli di CONSOB e Banca d'Italia, che pure dovranno collaborare con le Autorità Europee (ESMA e EBA).

Con riferimento ai fenomeni di *abusivismo*, all'art. 19, comma 7, della legge delega, viene prevista l'introduzione di sanzioni penali efficaci, proporzionate e dissuasive nei confronti di chiunque emetta, offra al pubblico o chieda l'ammissione alla negoziazione di criptoattività disciplinate dal regolamento MiCA in mancanza dei requisiti e delle autorizzazioni previste. Si tratta di previsioni in linea con la necessità – manifestata dal parlamento all'art. 18 della legge delega – di modificare il d.lgs. 231/2007, ricomprendendo i prestatori di servizi per le criptoattività – oggi qualificati alla stregua di *operatori non finanziari*[370] – nel novero degli intermediari finanziari, sottoponendoli ai relativi regimi di controllo e sanzionatori.

Nulla viene disposto con riferimento ai fenomeni di *market abuse*.

A fronte di quanto previsto per gli abusivismi che coinvolgono i soggetti che agiscono nel mercato criptovalutario – equiparati in tutto e per tutto agli intermediari tradizionali, come disciplinati nel TUF e nel TUB – pare potersi ritenere che in materia di manipolazione del mercato verranno modificati gli art. 184 e 185, affinché possano trovare applicazione, oltre che agli strumenti finanziari, anche in ipotesi di criptoattività.

---

[369] Cfr. Regolamento MiCA, considerando n. 9).

[370] L'inserimento dei prestatori di servizi criptovalutari nell'ambito degli *operatori non finanziari* aveva indotto parte della dottrina a ritenere che le norme del TUF non fossero ad essi applicabili, soprattutto con riguardo alla disciplina penalistica dettata dall'art. 166 TUF. In materia si rinvia a F. CONSULICH, *op.cit.*; F. DALAITI, *op.cit.*

5.3.2 *La tutela dell'amministrazione finanziaria.*

Le difficoltà qualificatorie delle criptovalute inducono ad interrogarsi anche in ordine al trattamento fiscale delle valute virtuali e, quindi, alla applicabilità della disciplina tributaria penalistica dettata dal d.lgs. 74/2000 e posta dal legislatore a tutela dell'amministrazione finanziaria.

Ed invero, è ragionevole ritenere che le caratteristiche proprie della *blockchain* e, quindi, la decentralizzazione e lo (pseudo) anonimato possano essere sfruttate da criminali economici anche al fine di eludere la disciplina dell'imposte.

Ancora una volta, a destare maggiori problematiche è l'assenza nel nostro ordinamento di una nozione chiara, precisa e definita di *criptovalute*. Si impongono, pertanto, precise riflessioni volte ad indagare – se vi è – qual è la natura delle valute virtuali in ambito tributario, anche tenuto conto che l'ordinamento prevede regole impositive diverse, in ragione delle caratteristiche soggettive del contribuente[371].

La questione sembra porsi con riferimento all'imponibilità delle operazioni in valuta virtuale effettuate tanto da *operatori professionali*, e *società di mining* quanto da *investitori privati.*

5.3.2.1 *Imponibilità delle operazioni in valute virtuali effettuate da operatori professionali.*

A livello eurounitario, in data 28 novembre 2006, il Consiglio ha emanato la Direttiva 2006/112/CE con cui è stata definita la disciplina del sistema comune dell'Imposta sul Valore Aggiunto (c.d. IVA). Ancora oggi, tuttavia, nonostante l'espansione del mercato criptovalutario e la recente introduzione del Regolamento MiCA, il fronte tributario – e con esso quello penaltributario – rimane ancora sprovvisto di una normativa *ad hoc*.

A livello nazionale, l'Italia ha parzialmente colmato il vuoto normativo in materia tributaria, introducendo all'art. 1 commi da 126 a 147, L. 197/2022, una disciplina fiscale delle criptoattività tra cui rientrano anche le criptovalute, in vigore dal 1° gennaio 2023. In particolare, detta disciplina ha inciso sull'art. 67 TUIR, quindi sui *redditi diversi* imponibili ai fini IRES e ai fini IRPEF.

Non è stata, invece, considerata in alcun modo la disciplina ai fini IVA.

5.3.2.1.1 *Imponibilità ai fini IVA.*

Per quanto qui di interesse, occorre comprendere se le *operazioni in valute virtuali effettuate da operatori professionali* (tanto *exchanger* quanto

[371] Il contribuente è il soggetto passivo dell'imposta. Può essere una persona fisica o una persona giuridica.

wallet provider) siano o meno assoggettabili alla disciplina tributaria ai fini IVA nonché ai fini IRES.

In tal senso, in assenza di una specifica disciplina in materia, parte della dottrina aveva proposto di ricondurre le criptovalute all'alveo delle *operazioni finanziarie* di cui all'art. 135, par. I, Direttiva IVA, potendo considerarsi Bitcoin come "quasi-divise" o strumenti finanziari negoziabili ovvero agli strumenti di *pagamento in natura*, *sub specie* di *voucher*, quali beni di secondo grado rappresentativi di beni o servizi digitali[372]. Con tale tentativo si mirava, infatti, ad assimilare il regime fiscale delle criptovalute a quello previsto per le transazioni in valuta legale.

Siffatta impostazione, tuttavia, è stata successivamente negata dalla Corte di Giustizia dell'Unione Europea (CGUE) che, chiamata dall'Amministrazione finanziaria svedese ad esprimersi in materia[373], nell'ambito della causa C-264/14 (decisa il 22 ottobre 2015) ha fornito una definizione ai fini tributari tanto dell'attività fornita dagli *exchanger* quanto della valuta virtuale.

In tal senso, la CGUE ha qualificato l'attività di cambio – tanto da *valuta* a *criptovaluta*, quanto da *criptovaluta* a *valuta* – svolta da operatori professionali, dietro il pagamento di un corrispettivo – costituito dalla differenza tra il prezzo al quale l'operato acquistava le criptovalute e il prezzo al quale veniva rivenduta – quale *prestazione di servizi a titolo oneroso*, ai sensi dell'art. 2, par. I, lett. c) della Direttiva IVA.

Ciò nonostante, ha osservato come, pur dovendosi in astratto ritenere integrato il presupposto applicativo dell'imposta, le operazioni compiute da

---

[372] Si rinvia a A. MAGLIOCCO, *Bitcoin e tassazione,* in *Strumenti finanziari e fiscalità,* 22, 2016, pp. 31-33; G. CORASANITI, *Il trattamento tributario tra obblighi antiriciclaggio e trattamento fiscale,* in *Strumenti finanziari e fiscalità*, Egea, Milano, 2018, pp. 45-61 reperibile al seguente link

[373] La CGUE è stata chiamata ad interpretare gli artt.2, par. I e 135, par. I della Direttiva IVA. Più precisamente, la questione è stata sollevata dall'Amministrazione finanziaria svedese nell'ambito di una controversia con un contribuente che intendeva fornire per il tramite della propria società attività di *exchange*, ritenendo che la stessa non fosse soggetta ad IVA. La questione, posta alla Commissione tributaria svedese, era stata risolta nel senso che, effettivamente, l'attività di cambio di criptovalute dovesse andare esente da IVA, coerentemente al disposto dell'art. 135, par. I, lett. e) della Direttiva IVA. Ed invero, come dato atto nella sentenza, la Commissione aveva qualificato la valuta virtuale alla stregua di *mezzo di pagamento* utilizzato in maniera corrispondente a mezzi legali di pagamento. Peraltro, l'espressione mezzi di pagamento con «valore liberatorio» di cui all'articolo 135, paragrafo 1, lettera e), della direttiva IVA sarebbe utilizzata per circoscrivere l'ambito dell'esenzione relativa alle banconote e alle monete. Di talché, la disposizione dovrebbe essere letta nel senso che è riferita solo alle banconote e alle monete, ma non alla valuta. Tale interpretazione sarebbe altresì coerente con lo scopo dell'esenzione di cui all'articolo 135, paragrafo 1, lettere da b) a g), della direttiva IVA, qual è quello di evitare le difficoltà che deriverebbero dall'assoggettamento dei servizi finanziari all'IVA.

exchanger avrebbero dovuto essere considerate esenti ai sensi dell'art. 135, par. I, lett. e). Ed invero, non avendo Bitcoin "altra finalità oltre a quella di un mezzo di pagamento ed essendo questa moneta accettata a tal fine da alcuni operatori", l'esenzione rispondeva pienamente alla *ratio* dell'istituto, potendo la criptovalute ricondursi alla categoria esente di *moneta con valore liberatorio*, purché convenzionalmente accettate.[374].

A livello nazionale, la questione è stata successivamente affrontata dall'Agenzia delle Entrate (AE) con Risoluzione 72/E del 2 settembre 2016. Si tratta del primo documento con cui l'Agenzia ha reso noto il proprio orientamento in materia, affermando l'esenzione dell'attività svolta dagli operatori *exchange*.

Siffatta conclusione, ancorché esplicitamente ancorata dall'Agenzia dell'Entrate alla pronuncia della CGUE, è giunta in realtà solo alle medesime conclusioni, ma ha percorso una strada differente.

Ha, invero, richiamato l'art. 10, comma 1, n. 3 del d.P.R. n. 633/1972, equiparando le *criptovalute* alle *valute estere*.

Detta impostazione è stata successivamente recepita dal Consiglio Nazionale del Notariato[375].

---

[374] CGUE, sentenza Skattevrket vs Hedqvist, causa C-264/2015, 22 ottobre 2015. In dottrina si rinvia a D. MAJORANA, *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in *Corriere Tributario*, 2018, 8, p. 630 ss.; S. CAPACCIOLI, *Regime impositivo delle monete virtuali: poche luci e molte ombre*, in *Il Fisco*, 2016, 37, p. 3538 ss; F. DI VIZIO, *Le cinte daziarie del diritto penale, op. cit.,* p. 128; A. MAGLIOCCO, *Bitcoin e tassazione*, in *Strumenti finanziari e fiscalità*, 2016, 1, p. 34 ss.; G. PALUMBO, *Il trattamento tributario dei bitcoin*, in *Diritto e Pratica Tributaria*, 2016, 1, pp. 2079 ss.; S. MAZZOCCHI, *Esenti da IVA le operazioni di cambio nella valuta virtuale "bitcoin"*, in www.*iltributario.it*, 22 dicembre 2015; P. CLAPS – M. PIGNATELLI, *L'acquisto e la vendita per conto terzi di "bitcoin" non sconta l'IVA ma rileva ai fini IRES ed IRAP*, in *Corriere Tributario*, 40, 2016, pp. 3073 ss., IPSOA; R. LUCEV, F. BONCOMPAGNI, *Criptovalute e profili di rischio penale nelle attività degli exchanger*, in *Giurisprudenza Penale Web*, 2018, 3, in www.giurisprudenzapenale.com. reperibile al seguente link ; F. FASSÒ, *Il regime fiscale dei* bitcoins *secondo una recente (e unica) prassi amministrativa. Un passo avanti e un'occasione mancata* in *Strumenti finanziari e fiscalità*, 28, 2017, pp. 105-114; G. CORASANITI, *l trattamento tributario dei bitcoin tra obblighi antiriciclaggio e monitoraggio fiscale,* in *Strumenti finanziari e fiscalità*, 36, 2018, pp. 52-54; M. PIERRO, *La qualificazione giuridica e il trattamento fiscale delle criptovalute*, in *Rivista di Diritto Tributario*, 2, 2020, pp. 116-120; R. SCALIA, *op.cit.*, pp. 12-13.

[375] U. BECHINI, M.C. CIGNARELLA, *Consiglio Nazionale del Notariato, Quesito Antiriciclaggio – Compravendita di Immobile – Pagamento del prezzo in Bitcoin*, vertente sulla richiesta in ordine alla legittimità del pagamento del prezzo della vendita di un bene immobile in criptovaluta.

Al contrario, tanto la qualificazione della CGUE quanto quella dell'AE non sono state accolte con favore da parte della dottrina, che ha suggerito di ricondurre le criptovalute, ai soli fini tributari, alla categoria di beni[376].

Tuttavia, siffatte obiezioni non sono state, al momento, accolto né da dall'AE né dal legislatore.

5.3.2.1.2 *Note critiche.*

La pronuncia della CGUE impone precise riflessioni in ordine all'effettiva portata della decisione richiamata.

Ed invero – sebbene svolto con specifico riguardo alle ipotesi di esenzioni dettate, in via tassativa, dall'art. 135 Direttiva IVA – la qualificazione delle *criptovalute* come *mezzo di pagamento*, merita una precisa delimitazione, che tenga conto della *ratio* dell'Imposta sul Valore Aggiunto.

L'IVA, infatti, oggetto di disciplina armonizzata dettata proprio dalla Direttiva 2006/112/CE, è un'imposta generale sui consumi che sorge in capo ai *consumatori finali,* vale a dire sui soggetti che acquistino beni e servizi sottratti alla filiera produttiva o distributiva.

In tal senso, presupposto oggettivo dell'IVA è la costituzione o il trasferimento di diritti reali di godimento sui beni (art. 2) e lo svolgimento di prestazioni di servizio dietro pagamento di un corrispettivo di cui beneficia il consumatore (art. 3 Direttiva IVA).

Quanto ai soggetti obbligati al versamento del tributo, l'IVA è dovuta da coloro che esercitano un'attività oggettivamente considerata commerciale o agricola, indipendentemente dal fatto che sia organizzata in forma di impresa; da un'attività che presenta i caratteri tipici dell'attività commerciale, in quanto organizzata in forma di impresa; una professione abituale.

Pare, allora, doversi precisare che, indipendentemente dalla qualificazione alla stregua di *mezzo di pagamento* delle criptovalute, la disciplina sull'esenzione IVA opererà unicamente rispetto alle ipotesi espressamente previste dall'art. 135 Direttiva IVA e non in tutte le ipotesi, generalmente intese, in cui le criptovalute siano convenzionalmente utilizzate quale mezzo di pagamento.

Di talché, ogniqualvolta, non si versi nelle eccezionali ipotesi di cui all'art. 135, ove la criptovaluta sia utilizzata come mezzo di pagamento convenzionalmente scelto tra le parti di un negozio avente ad oggetto il trasferimento di diritti reali di godimento su beni ovvero prestazioni di servizi

[376] In particolare, si rinvia a M. PIERRO, *Contributo all'individuazione della nozione di* crypto asset *e suoi riflessi nell'ordinamento tributario nazionale*, *op.cit.,* pp. 574-611; M. PIERRO, *La qualificazione giuridica e il trattamento fiscale delle criptovalute*, *op.cit,* pp. 589-611; R. SCALIA, *op.cit*., pp. 13-40.

subordinate a un corrispettivo, destinate a un consumatore finale dovrà ritenersi applicabile la disciplina IVA.

5.3.2.1.3 *Imponibilità ai fini IRES e IRAP.*

Altro quesito affrontato dall'Agenzia delle Entrate con Risoluzione 72/E, di cui non si era mai occupata la giurisprudenza della CGUE, ha riguardato la rilevanza delle operazioni di *exchange* ai fini dell'applicazione delle imposte dirette IRES e IRAP.

In particolare, ricorrendo alla equiparazione delle criptovalute alle *valute estere*, l'AE ha affermato che i componenti positivi di reddito derivanti dall'attività di *exchange* per conto degli utenti devono essere assoggettati a tassazione al netto dei relativi costi inerenti a detta attività[377]. Come ben osservato da Aquaro "in altri termini, il guadagno (o la perdita) di competenza dell'*exchanger* che deve scontare imposizione fiscale sarebbe rappresentato dalla differenza tra quanto anticipato dal cliente e quanto speso per l'acquisto (o tra quanto incassato per la vendita e quanto riservato al cliente). Tale elemento di reddito deve, dunque, essere ascritto ai ricavi (o ai costi) caratteristici di esercizio dell'attività di intermediazione esercitata e contribuire quale elemento positivo (o negativo) alla formazione della materia imponibile soggetta ad ordinaria tassazione ai fini delle imposte sul reddito (Ires) o dell'imposta regionale sull'attività produttiva"[378].

Ove, a fine esercizio, l'*exchanger* detenga proprie criptovalute nel portafoglio, la loro valutazione dovrà essere effettuata secondo il cambio in vigore alla data di chiusa dell'esercizio e, comunque, in applicazione dell'art. 9 TUIR, che disciplina la determinazione dei redditi e delle perdite derivanti dalla detenzione di valute estere.

5.3.2.1.4 *Imponibilità dei proventi di mining.*

È necessario indagare i profili fiscali dell'attività di *mining* svolta nella *blockchain*.

In particolare, si è detto, i minatori svolgono una duplice attività di validazione delle transazioni e *mining* di criptovalute, retribuita dalla *blockchain* con nuove valute virtuali e, in quanto tale, produttiva di reddito.

---

[377] L. AQUARO, *Tassazione in Italia delle operazioni in valuta virtuale*, in M. LORENZINI, M. ZULBERTI, C. IMBROSCIANO (a cura di), *op.cit.,* pp. 211-241.

[378] L. AQUARO, *op.cit.*, p. 225.

Occorre, dunque, comprendere quale sia, ai fini tributari, la *qualificazione* della attività considerata sì da comprenderne l'eventuale rilevanza fiscale e da individuare la disciplina applicabile [379].

La dottrina intervenuta in materia ha ritenuto di potere ricondurre il *mining* alla categoria civilistica delle "prestazioni di fare" ove il *facere* consisterebbe "nel garantire la sicurezza della rete registrando su *blockchain* solo le transazioni che soddisfano i requisiti di validità prescritti"[380].

Dovrebbe, poi, distinguersi tra attività di *mining* svolta dal singolo e attività svolta in *mining pool*.

A livello prettamente civilistico, si tratterebbe di un contratto ex art. 1333 c.c. in cui l'accordo tra gli i *miner* e la *blockchain* passerebbe dall'accettazione delle condizioni dettate dal *software* utile allo svolgimento dell'attività di *mining*. Si tratterebbe di fatti concludenti, corrispondenti allo scaricamento del *software* e all'abilitazione della funzione per il *mining*[381].

È stato sostenuto che nel caso di *mining pool*, bisognerà distinguere a seconda dell'attività svolta e delle modalità di svolgimento.

Ed invero, se i *miner* operano tutti sullo stesso piano potrebbe ipotizzarsi un'*associazione temporanea di impresa* o una *società di fatto*.

Avremo un'*associazione temporanea di impresa* nel caso in cui i partecipanti collaborino all'esecuzione di un'opera complessa, alla prestazione di particolari servizi ovvero alla conclusione di un singolo affare. Vi sarà, invece, una *società di fatto* quando i *miner* svolgono la predetta attività economica al solo fine di dividerne gli utili.

Non è esclusa la possibilità che il *mining pool* sia composto da singoli utenti che lavorano per una vera e propria impresa organizzatasi al fine di prestare detto servizio.

L'individuazione disciplina da applicare in materia è, ad oggi, lasciata all'interprete: la L. 197/2022 non ha preso in alcun modo in considerazione la posizione dei *miner.* Diversamente, l'Agenzia delle Entrate ha affrontato il tema nell'ambito della risposta a interpello n. 508/2022, tanto con riguardo alle imposizioni indirette (IVA) quanto -ancorché in via incidentale – alle imposizioni dirette (IRES, IRPEF).

---

[379] F. TUMBIOLO, *Profili fiscali della formazione del consenso all'interno della* blockchain, in M. LORENZINI, M. ZULBERTI, C. IMBROSCIANO (a cura di), *op.cit.* pp. 243-263.

[380] *Ivi*, p. 250. Nello stesso senso, VALUE ADDED TAX COMMITEE, *Working paper no. 892, Issues arising from recent judjments of the court of Justice of the European Union*, febbraio 2016, p. 13, inwww.circabc.europa.eu, reperibile al seguente link.

[381] F. TUMBIOLO, *op.cit.*, p. 251.

5.3.2.1.5 *Imponibilità ai fini IVA.*

La dottrina intervenuta in materia, qualificando il *mining* a una prestazione di *fare*, ai fini fiscali, ha ammesso la possibilità di ricondurlo alla categoria della *prestazione* o della *produzione di servizi*[382].

Si tratta di categorie indefinite a livello legislativo che, tuttavia, hanno trovato una netta differenziazione nell'elaborazione dottrinale[383].

In particolare, *la produzione* consisterebbe in una attività idonea a generare reddito di impresa ai sensi dell'art. 2195 c.c. In tal senso, si caratterizzerebbe per la contemporanea presenza di *capitale* e di *lavoro*.

Se definita partendo dal combinato disposto degli artt. 54 (determinazione dei redditi da lavoro autonomo) e 55 TUIR (redditi di impresa), *la prestazione* può essere qualificata alla stregua di lavoro autonomo, esercitato senza un'organizzazione in forma di impresa. Di talché, sarebbero centrali le *energie lavorative e personali*[384]. Ciò non esclude, tuttavia, la possibilità che la stessa venga in rilievo nell'ambito dell'impresa, ogniqualvolta l'esecuzione dell'attività lavorativa preveda un'organizzazione in tale forma[385].

Alla luce di quanto osservato pare potersi concordare con la parte di dottrina che ha qualificato il *mining* alla stregua di *produzione*, dovendosi escludere che il *mining* comporti l'impiego di *energie lavorative e personali.* Non vi è bisogno, infatti, di alcun apporto personale da parte del *miner*, posto che la risoluzione degli algoritmi necessaria al *mining* non richiede alcun contributo del minatore ma, piuttosto, l'installazione di specifici e potenti *hardware* e *software*.

A medesime conclusioni pare essere giunta anche l'AE che, in occasione della risposta all'interpello 508/2022, sulla base delle medesime considerazioni, ha osservato come: "tenuto conto delle modalità con le quali il *miner* viene ricompensato, e cioè in modo automatico dal sistema/*network*/rete, si ritiene che la remunerazione pagata dal network non sia corrisposta nell'ambito di un rapporto di scambio di servizi".

Proprio sulla base di detta caratteristica, l'AE è giunta a ritenere l'esenzione del *mining* ai fini IVA. È stato, invero, osservato come "L'assenza di un servizio direttamente prestato dal *miner* a favore di un committente,

---

[382] P.L. BURLONE, R. DE CARIA, *Bitcoin e le altre criptomonete. Inquadramento giuridico e fiscale*, in *IBL Focus,* aprile 2014, p. 9 ss., in www.brunoleoni.it, reperibile al seguente link

[383] Tra tutti, si rinvia a A. FANTOZZI, voce *Imprenditore e impresa nelle imposte sui redditi e nell'IVA,* in *Enc. Giur.,* vol. XVI, Roma, 1989, p. 4.

[384] A. FANTOZZI, *Imprenditore e imprese nelle imposte sui redditi e nell'IVA*, Giuffrè, Milano, 1982, p. 51.

[385] *Ivi,* p. 122.

determinato o determinabile, consente di ritenere il *mining* non rilevante ai fini IVA in quanto caratterizzato dall'assenza di un legame sinallagmatico con conseguente preclusione del diritto a detrazione".

In tal senso, anche la dottrina ha ritenuto i profitti del *mining* esenti ai fini IVA, facendo leva sull'art. 135, par. 1, lett. e) e d), per le attività relative a valute o a pagamenti[386].

5.3.2.1.6 *Imposte dirette.*

Ne consegue che le criptovalute rilasciate da *blockchain* all'esito dell'attività di *mining* rilevano, ai fini tributari, come *reddito di impresa* (art. 55 TUIR) o *reddito diverso* (art. 67 TUIR), a seconda che siano connotate o meno da abitualità. Le criptovalute, in tal senso, rileveranno come *ricavi* quando si tratti di corrispettivo del *mining* per l'attività di impresa svolta.

A conferma di ciò, l'AE nell'ambito di risposta ad interpello n. 508/2022 – seppur affrontando principalmente la materia dell'imposizione IVA dei *miner* – ha osservato come "1ualora l'attività del "miner" non risulti retribuita, poiché come evidenziato il "blocco" è stato risolto da un attore differente, in considerazione della circostanza per cui il servizio è stato prestato, si realizza una perdita su crediti la cui deducibilità sarà consentita sussistendone gli elementi certi e precisi di cui all'articolo 101, comma 5 del TUIR"[387].

Quanto ai *mining pool*, la dottrina intervenuta in materia ha osservato come nel caso di *associazioni temporanee di imprese* e nelle *società di fatto* il reddito sarebbe imputabile direttamente al singolo *miner*, ancorché per motivi diversi.

Nel primo caso, saremmo in presenza di un soggetto autonomo e l'imputazione avverrebbe a titolo di *reddito di impresa.*

Nel secondo caso, la disciplina applicabile sarebbe quella della *società di persone* con la conseguente inapplicabilità tanto dell'IRES quanto dell'IRPEF[388].

5.3.2.2 *Tassazione per gli investitori privati.*

L'ambito considerato è, a livello nazionale, oggi regolato dalla normativa introdotta con L. 197/2022.

Ed invero, a fronte delle incertezze iniziali che avvolgevano la disciplina delle criptovalute, il legislatore nell'ambito della Legge di Bilancio 2023 ha inteso regolamentare, almeno in via temporanea, il fenomeno. È stato,

---

[386] F. TUMBIOLO, *op.cit.*, p. 256.
[387] AGENZIA DELLE ENTRATE, risposta a interpello 508/2022, p. 9.
[388] F. TUMBIOLO, *op.cit.*, pp. 253-255.

in tal senso, introdotto al comma 1 dell'art. 67 TUIR, la nuova lett. c-*sexies*, che ha introdotto una nuova categoria di *redditi diversi di natura finanziaria.* Vi rientrano, in particolare, le plusvalenze e gli altri proventi realizzati mediante rimborso o cessione a titolo oneroso, permuta[389] o detenzione di criptoattività – comprese, quindi, le criptovalute – comunque denominate, archiviate o negoziate elettronicamente su tecnologia DLT o tecnologie equivalenti.

È, inoltre, prevista una soglia di esclusione della tassazione pari a euro 2.000,00 per periodo di imposta. Non si tratta, tuttavia, di una esenzione o franchigia: rileva solo ai fini dei redditi imponibili.

Ai sensi del nuovo comma 9 bis dell'art. 68 TUIR, poi, vengono definite le *plusvalenze derivanti da criptoattività* come la differenza tra corrispettivo percepito ovvero il valore normale della criptoattività permutate e il costo o il valore acquisito. Le plusvalenze possono essere portate in compensazione con le minusvalenze.

I proventi derivanti dalla detenzione di criptovaluta, percepiti nel periodo d'imposta, sono assoggettati a tassazione senza alcuna deduzione.

Con specifico riguardo alle sole criptovalute, la Legge di Bilancio 2023 ha modificato la disciplina degli artt. 5,6,7 del d.lgs. 461/1997, introducendo specifiche modalità di tassazione.

In particolare, con riferimento alla nuova lett. c- sexies dell'art. 67, comma 1, TUIR, l'imposta sostitutiva sulle plusvalenze e sugli altri redditi è stata fissata al 26%, con possibilità di esercitare l'opzione del *regime amministrato* e del *risparmio gestito* anche presso gli intermediari di portafogli digitali, ancorché previsti dal d.lgs. 231/2007 tra gli operatori non finanziari[390].

5.3.2.2.1 *La disciplina transitoria.*

Ha sollevato perplessità la disciplina transitoria introdotta dalla L. 197/2022 in materia di criptovalute. All'art. 127 è stato, infatti, previsto che le plusvalenze realizzate con criptovalute prima del 1° gennaio 2023, siano considerate realizzate ai sensi dell'art. 67 TUIR con applicazione dell'art. 68 TUIR. Le plusvalenze dovrebbero, pertanto, essere costituite dalla "differenza tra il corrispettivo percepito ovvero la somma od il valore normale dei beni rimborsati ed il costo od il valore di acquisto assoggettato a tassazione,

---

[389] La norma precisa come la permuta tra criptoattività, qual è lo scambio cripto-cripto, non costituisce fattispecie fiscalmente rilevante se avente ad oggetto criptovalute con stesse caratteristiche e funzioni.

[390] Si tratta, in realtà, di eccezione destinata a venire meno, stante la previsione della L.Delega 15/2024 che, nell'attuare le norme del Regolamento MiCA, dovrebbe inserire i prestatori di servizi criptovalutari tra gli *intermediari finanziari*..

aumentato di ogni onere inerente alla loro produzione, compresa l'imposta di successione e donazione, con esclusione degli interessi passivi", ammessa la possibilità di portare in deduzione le minusvalenze.

Si tratta di norma particolarmente discussa, in quanto contrastante con l'art. 3, comma 1, dello Stato dei diritti del contribuente (L. 212/2012), che prevede espressamente il divieto di retroattività delle norme tributarie.

5.3.2.3 *Monitoraggio fiscale.*

Ulteriore aspetto da considerare, utile ai nostri fini, riguarda la disciplina del monitoraggio fiscale introdotta dall'art. 129 L. 197/2022 anche rispetto alla criptoattività e ai prestatori di servizi di portafoglio digitale. Vige, quindi, l'obbligo per le persone fisiche residenti nel territorio dello Stato, detentori di criptovalute, la compilazione del Quadro RW del modello redditi – Persone fisiche.

5.3.3 *Reati tributari e criptovalute.*

Così sintetizzata la disciplina fiscale delle criptovalute, occorre comprendere se e quali fattispecie incriminatrici possano venire in rilievo ai sensi della disciplina dettata dal d.lgs. 74/2000.

5.3.3.1 *IVA.*

Esclusa l'assoggettabilità a IVA tanto dei *prestatori di servizi criptovalutari* quanto dei *miner*, si ritiene di dovere escludere in capo a essi la configurabilità dei delitti previsti e puniti dagli artt. 2 (Dichiarazione fraudolenta mediante uso o fatture o altri documenti inesistenti), 3 (Dichiarazione fraudolenta mediante altri artifici), art. 4 (Dichiarazione infedele), 5 (Omessa dichiarazione), 10 (occultamento o distruzione di documenti contabili), 10 *ter* (Omesso versamento IVA) e 11 (sottrazione fraudolenta al pagamento di imposte).

Al contrario, le fattispecie incriminatrici richiamate potranno venire in rilievo ogni qualvolta le condotte descritte siano tenute da soggetto tenuto al versamento dell'IVA.

In tal caso, la circostanza che i fatti compiuti dal contribuente ricadano su criptovalute ovvero vengano commessi previo loro utilizzo, non ne esclude la punibilità.

La formulazione delle norme richiamate, invero, appare assolutamente idonea a ricomprendere condotte criminose che sfruttino la decentralizzazione e lo pseudoanonimato della *blockchain*.

5.3.3.2 *Imposte dirette.*

Diverso, invece, è il caso delle imposte dirette, che sembra aprire alla configurabilità di tutte le fattispecie incriminatrice del d.lgs. 74/2000, la cui formulazione non preclude le condotte violative degli interessi dell'amministrazione finanziaria tenute con criptovalute.

Come noto, la disciplina dettata dal d.lgs. 74/2000 è una disciplina di ampio respiro, che guarda alle "imposte sui redditi" *lato sensu* intese, a prescindere dalle modalità con cui il reddito è stato prodotto. Ne consegue, al riguardo, l'applicabilità a tutte le imposte sui redditi cui sono obbligate tanto le persone fisiche quanto le persone giuridiche.

Si tratta, tuttavia, di disciplina che prevede specifiche soglie di punibilità, che variano a seconda della fattispecie considerata.

Di talché, anche rispetto ai redditi derivanti da attività criptovalutaria, sarà necessario valutare, di volta in volta, la sussistenza della soglia di punibilità, in mancanza della quale il soggetto potrà, eventualmente, essere chiamato a rispondere solo sul fronte amministrativo.

L'introduzione della disciplina sul *monitoraggio fiscale delle criptoattività* induce ad interrogarsi in ordine alla configurabilità, nel caso di mancata compilazione del Quadro RW, del reato di Dichiarazione infedele, disciplinato all'art. 4, d.lgs. 74/2000.

In materia si è, anche da ultimo, pronunciata la giurisprudenza di legittimità che con sentenza 19849/2021 – in materia di monitoraggio fiscale di valute estere – ha affermato come il mancato rispetto della disciplina in commento non integra reato di dichiarazione infedele.

Tali considerazioni risultano senz'altro applicabili anche alla disciplina fiscale delle criptoattività.

5.3.3.2.1 *La sottrazione fraudolenta al pagamento di imposte.*

Ciò detto, è bene osservare come, in via generale, le caratteristiche proprie delle criptovalute potrebbe favorire, tra le altre, la commissione del reato previsto dall'art. 11 d.lgs. 74/2000, rubricato *sottrazione fraudolenta al pagamento di imposte*.

La disposizione punisce "chiunque, 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.

Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni".

In particolare, le caratteristiche di decentralizzazione e pseudoanonimato potrebbero indurre il contribuente a convertire i beni nel corrispondente valore in criptovalute, sì da eludere la disciplina fiscale, profittando dello (pseudo)anonimato delle transazioni. In tal caso, si potrebbe configurare un'ipotesi di *compimento di atti fraudolenti*. Ciò sarebbe sufficiente a integrare gli estremi della condotta.

Ed invero, l'astratta tracciabilità delle operazioni compiute sulla *blockchain*, quale registro pubblico e consultabile da chiunque, non escluderebbe l'applicabilità della norma richiamata.

Al riguardo, anche da ultimo, la giurisprudenza di legittimità ha, infatti, affermato che "Ai sensi dell'art. 11 d.lgs. n. 74/2000, gli atti dispositivi compiuti dall'obbligato, oggettivamente idonei ad eludere l'esecuzione esattoriale, anche se leciti e tracciabili, hanno natura fraudolenta quando, all'esito di una valutazione complessiva delle singole condotte nel loro collegamento finalistico e nella loro sequenza funzionale, risultino connotati da elementi di artificio, inganno o menzogna tali da rappresentare ai terzi una riduzione del patrimonio non corrispondente al vero, così mettendo a repentaglio o, comunque, rendendo più difficoltosa la procedura di riscossione coattiva"[391].

6. *I reati fallimentari.*

Alla luce dei recenti avvenimenti che hanno coinvolto società di *exchange*, occorre dare conto della concreta possibilità che nell'immediato futuro possano venire in rilievo reati fallimentari che coinvolgano prestatori di servizi criptovalutari.

In tale direzione pare avere rivolto lo sguardo anche il legislatore italiano che nell'ambito della legge n. 15/2024, entrata in vigore il 10 marzo 2024 all'art. 19, lett. m), ha conferito delega al Governo affinché entro sei mesi preveda "una disciplina della gestione delle crisi per gli emittenti di token collegati ad attività e per i prestatori di servizi per le cripto-attività di cui al regolamento (UE) 2023/1114, apportando alla normativa nazionale in materia di gestione delle crisi ogni altra modifica necessaria o opportuna per chiarire la disciplina applicabile, per tenere in considerazione le specificità connesse con le attività disciplinate dal citato regolamento (UE) 2023/1114 e per assicurare efficacia ed efficienza alla gestione delle crisi dei soggetti che esercitano attività disciplinate dal medesimo regolamento (UE), anche tenendo conto delle esigenze di proporzionalità della disciplina e di celerità delle procedure".

[391] Cass. pen., Sez. III, sent. N. 16686/2021.

6.1 *Il caso BitGrail.*

Tra i casi più noti di fallimento che hanno coinvolte le piattaforme *exchange* troviamo anche la vicenda che ha riguardato la piattaforma italiana *BitGrail*.

Si trattava di uno dei principali *exchanger* attivi *online*, che permetteva di cambiare le valute virtuali con la nuova cripto Nano, considerata particolarmente allettante dagli investitori.

La vicenda si è originata nell'autunno 2017, quando la piattaforma, ha iniziato a manifestare malfunzionamenti che causavano ritardi sia nelle operazioni di prelievo che di accredito delle somme.

Nel gennaio 2018, quando Nano ha raggiunto il suo valore massimo (pari a circa 30 euro per ogni criptovaluta), i disservizi sono aumentati, financo a comportare un'errata contabilizzazione – ovviamente al ribasso – dei fondi presenti sul conto.

In data 12 gennaio 2018, pertanto, il gestore della piattaforma decideva di bloccare tutte le operazioni in usciti, trincerandosi dietro gli obblighi antiriciclaggio nel frattempo introdotti dal d.lgs. 90/2017.

Quasi un mese dopo, in data 9 febbraio 2018, il gestore della piattaforma lamentava di avere subito un importante attacco *hacker,* cui era conseguita la sottrazione dai *wallet* degli utenti di 17 milioni di Nano (pari a circa l'80% di tutta la criptovaluta detenuta dall'*exchange*), il cui valore, all'epoca, si aggirava attorno a circa 120 milioni di euro.

La versione dei fatti fornita dall'operatore suscitava precisi dubbi negli utenti che continuavano a chiedere informazioni su quanto accaduto, senza, tuttavia ricevere risposta.

Successivamente, il gestore aveva iniziato a proporre accordi transattivi particolarmente sconvenienti per gli investitori, cui veniva richiesto di rinunciare alla maggiore parte dei crediti a fronte della conversione del residuo in una nuova e diversa criptovaluta.

Proprio l'istanza presentata da alcuni investitori ha portato alla dichiarazione di fallimento di *Bitgrail*, pronunciata dal Tribunale di Firenze, sezione fallimentare con sentenza n. 18 del 21 gennaio 2019.

In detta sede è stata rilevata la totale assenza di misure di sicurezza adeguate accompagnata da un comportamento fortemente scorretto tenuto da Bitgrail che era a conoscenza del malfunzionamento almeno dal luglio 2017 e che, pur astenendosi dal tutelare i conti degli utenti, aveva provveduto a trasferire parte dei propri fondi personali su piattaforme terze.

6.2 *L'ampliamento della disciplina dei reati fallimentari.*

Il caso di BitGrail non ha rappresentato, purtroppo, un *unicum* nel panorama criptovalutario.

Il riferimento, tra gli altri, è al caso MtGox, exchanger che ha gestito il 70% di tutte le transazioni di criptovalute fino al 2014, quando ha improvvisamente chiuso i battenti, annunciando la perdita di 744.408 Bitcoin (il cui valore, all'epoca, era pari a circa 450.000.00 di dollari). Successivamente, si scoprì che, in realtà, erano scomparsi 850.000 Bitcoin (è stato uno dei periodi di maggiore calo del valore del Bitcoin, che calo drasticamente del 36%). Riuscirono a recuperarne solo 200.000. Anche in questo caso, la causa della sottrazione fu imputata a malfunzionamenti cui erano seguiti prelievi fraudolenti. Poco dopo il Tribunale di Tokyo, ove aveva sede la società, ne ha dichiarato il fallimento Tuttavia, la procedura di rimborso dei creditori, prevista per settembre 2023, non è ancora iniziata.

In tal senso, pare ragionevole la scelta del legislatore di sottoporre gli emittenti di token e, per quel che qui interessa, i prestatori di servizi per le cripto-attività alla disciplina della gestione delle crisi. Si tratta di un importante passo avanti, che permetterà di rendere ancora più sicuro il mercato criptovalutario.

In quest'ottica appare opportuno iniziare a immaginare una disciplina penalistica che possa tutelare i beni giuridici in rilievo che, in ragioni della sempre più considerevole attività riconosciuta dalla legge ai prestatori di servizi criptovalutari, paiono meritevoli di una tutela crescente.

7. *La responsabilità dell'ente e l'utilizzo di criptovalute.*

Alla luce delle condotte sin qui analizzate occorre interrogarsi circa il rapporto tra responsabilità dell'ente e criptovalute.

La responsabilità delle persone giuridiche è disciplinata dal d.lgs. 231/2001, che detta la normativa in materia, individuando i soggetti destinatari, i presupposti della responsabilità per gli illeciti amministrativi dipendenti da reato, i meccanismi di imputazione dell'illecito e le conseguenze da esso derivanti.

Sia concessa una sintetica panoramica del d.lgs. 231/2001[392].

[392] Si rinvia a A.ALESSANDRI, S. SEMINARA, *Diritto penale commerciale*. *Volume I. I principi generali*, Giappichelli,Torino, 2018, pp. 88-128.

7.1 *I soggetti.*

All'art.1 d.lgs. 231/2001 il legislatore ha previsto che la normativa sulla responsabilità amministrativa dell'ente si applichi *agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica*, che operino in Italia, a prescindere dal fatto che la sede sia all'estero.

Sono esclusi lo Stato, gli enti pubblici territoriali, gli altri enti pubblici non economici[393] e gli enti che svolgono funzioni di rilievo costituzionale.

7.2 *I presupposti della responsabilità.*

Il legislatore ha subordinato la sussistenza della responsabilità della persona giuridica alla presenza di tre diversi presupposti.

Ed invero, l'ente è chiamato a rispondere solo della commissione di determinati reati, previsti dall'art. 24 all'art. 25 octiesdecies, commessi da soggetti apicali o sottoposti alla vigilanza di questi, che abbiano agito nell'interesse o a vantaggio dell'ente. Di talché, l'ente non risponderà se questi abbiano agito per soddisfare un interesse esclusivo proprio o di terzi.

7.2.1 *Interesse e vantaggio.*

L'*interesse*, che deve essere valutato *ex ante,* viene inteso come "direzione finalistica del fatto illecito (…) esternamente riconoscibile, favorevole all'ente". Ha natura oggettiva, che prescinde dalle *intenzioni* dell'agente.

Il *vantaggio*, invece, fa riferimento alle *utilità* percepite dall'ente all'esito del reato commesso e, pertanto, deve essere valutato *ex post.*

La dottrina e la giurisprudenza maggioritaria hanno chiarito come detti presupposti siano tra loro alternativi, non dovendo, pertanto, sussistere entrambi affinché possa essere affermata la responsabilità dell'ente[394].

È interessante notare come la profondità dell'interesse perseguito e il vantaggio ottenuto possono rilevare ai fini della riduzione della sanzione pecuniaria, conformemente al disposto dell'art.12.

7.2.2 *I meccanismi di imputazione dell'illecito amministrativo.*

La sussistenza della responsabilità amministrativa della persona giuridica è, altresì, subordinata alla commissione di un reato causata da un difetto di organizzazione, direzione o vigilanza. In tal senso, le modalità di configurazione del reato variano a seconda che sia stato commesso da un

---

[393] Sono, quindi, esclusi gli enti pubblici associativi, erogatori di pubblici servizi senza scopo di lucro (ad esempio, le università statali) e gli enti che curano i fini e gli interessi dello Stato (ad esempio, il CNR e l'Inps).

[394] Si rinvia a Cass. pen., Sez. V, sent. n. 10265/2014.

soggetto in posizione apicale ovvero da un *soggetto sottoposto all'altrui direzione o vigilanza.*

Nel caso in cui il reato sia commesso da un soggetto in posizione di vertice, l'art. 6 prevede che l'ente non risponde se prova che:

"a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)".

Vi è, in tal senso, un'inversione dell'onere della prova che incombe sull'ente anziché sull'accusa, che dovrà limitarsi a dimostrare l'effettiva commissione dell'illecito commesso dalla persona fisica e la sussistenza dell'interesse o del vantaggio.

Ove, invece, il reato sia stato commesso da un *sottoposto* l'art.7 prevede che "l'ente é responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza". L'inosservanza è, tuttavia esclusa, "se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi".

Viene, quindi, precisato che il modello deve essere *idoneo* ed *adeguato*, da un lato, a garantire lo svolgimento dell'attività in relazione alla natura, alla dimensione dell'organizzazione e alla tipologia di attività svolta; dall'altro lato a "scoprire ed eliminare tempestivamente situazioni di rischio".

Un modello efficacemente attuato prevede e richiede sia la verifica periodica e l'eventuale modifica dello stesso in caso di scoperta di significative violazioni delle prescrizioni nonché di mutamenti nell'organizzazione o nell'attività; sia un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

È importante sottolineare l'autonomia sussistente tra la responsabilità penale della persona fisica che ha commesso il reato e la responsabilità amministrativa dell'ente che non ha adottato – o non ha dimostrato di avere adottato – modelli idonei a prevenirne la commissione.

L'autonomia della responsabilità dell'ente, d'altra parte, è espressamente sancita all'art. 8, che prevede la *punibilità* dell'ente anche quando l'autore del reato non sia stato identificato, non sia imputabile ovvero il reato si sia estinto per causa diversa dall'amnistia.

7.2.3 *Il criterio di imputazione: la colpa di organizzazione.*

Come detto, la responsabilità dell'ente è esclusa nel caso in cui l'ente dimostri che il reato contestato è stato commesso nonostante l'adozione e l'attuazione di un modello idoneo e adeguato.

In tal senso, ove il reato sia stato commesso da *soggetto apicale*, l'adozione del modello costituirà una *causa di esclusione della punibilità* dell'ente, laddove questo dimostri di avere adottato e attuato misure preventive idonee a prevenire il reato verificatosi. Dovrà, quindi, essere dimostrato che la condotta criminosa sia stata tenuta con una fraudolenta elusione del modello organizzativo.

Nel caso in cui, autore del reato sia un sottoposto, la mancata adozione del modello assurgerà a *elemento costitutivo del reato*. In questo incomberà sull'accusa l'onere della prova circa il nesso di causalità tra l'inosservanza degli obblighi di direzione e vigilanza ovvero l'inidoneità del modello (ove adottato) e la commissione del reato da parte del soggetto sottoposto.

Si può, pertanto, affermare che il criterio di imputazione soggettiva nella responsabilità dell'ente è, dunque, sempre costituito dalla *colpa di organizzazione* che, tuttavia, differirà a seconda delle qualità del soggetto agente.

7.3 *Le sanzioni.*

L'art. 9 prevede che all'ente possano essere inflitte sanzioni pecuniarie, sanzioni interdittive, sanzioni ablatorie (confisca) e stigmatizzanti (pubblicazione della sentenza).

Il nucleo centrale dell'assetto sanzionatorio in materia di responsabilità dell'ente è rappresentato dalle sanzioni pecuniarie – che sono applicabili per tutti gli illeciti amministrativi commessi dall'ente – e dalle sanzioni interdittive, che possono essere applicate solo ove espressamente previste.

In caso di condanna deve, poi, sempre essere applicata la confisca, mentre la pubblicazione della sentenza è disposta, discrezionalmente, solo nei casi di inflizione di una sanzione interdittiva.

7.3.1 *Le sanzioni pecuniarie.*

Il d.lgs. 231/2001 prevede un sistema sanzionatorio per quote. In particolare, la sanzione va da un minimo di cento quote a un massimo di mille quote, il cui importo va da 258 a 1549 euro.

L’art. 11 detta espressamente i criteri di commisurazione della sanzione pecuniaria, intesa come determinazione del numero di quote, che deve essere determinata dal giudice tenendo conto della *gravità del fatto*, del *grado della responsabilità dell’ente*, dell’*attività susseguente al reato* in termini sia di eliminazione e attenuazione delle conseguenze sia di prevenzione di ulteriori illeciti.

Il valore di ciascuna quota, invece, non deve essere commisurato al fatto, ma fissata in base alle condizioni economiche e patrimoniali dell’ente, affinché la sanzione possa essere *efficacemente* applicata.

Il processo di commisurazione è, dunque, bifasico.

4.1.1. *Le sanzioni interdittive*.

Disciplinate all’art. 13 e ss., le sanzioni interdittive hanno una funzione tanto general quanto special preventiva. Possono essere applicate solo in relazione ai reati per i quali sono espressamente previste e possono durare, di regola, da tre mesi a due anni.

Tuttavia, l’art. 16 prevede che, eccezionalmente, le sanzioni interdittive possano essere applicate in via definitiva, quando:

1) L’ente ha tratto dal reato un profitto di rilevante entità ed è già stato condannato, almeno tre volte negli ultimi sette anni, alla interdizione temporanea dall'esercizio dell'attività;
2) L’ente sia già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni. In tal caso il giudice potrà disporre il divieto di contrattare con la pubblica amministrazione ovvero del divieto di pubblicizzare beni o servizi;
3) L’ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità. In detta ipotesi è sempre disposta l’interdizione definitiva dall'esercizio dell'attività, senza che possa essere riconosciuta rilevanza alle ipotesi di riparazione delle conseguenze del reato, dettate all’art. 17.

L’art. 17, infatti, dispone che “ferma l'applicazione delle sanzioni pecuniarie, le sanzioni interdittive non si applicano quando, prima della dichiarazione di apertura del dibattimento di primo grado, concorrono le seguenti condizioni:

a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;

b) l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi;

c) l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

1-bis. In ogni caso, le sanzioni interdittive non possono essere applicate quando pregiudicano la continuità dell'attività svolta in stabilimenti industriali o parti di essi dichiarati di interesse strategico nazionale ai sensi dell'articolo 1 del decreto-legge 3 dicembre 2012, n. 207, convertito, con modificazioni, dalla legge 24 dicembre 2012, n. 231, se l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi. Il modello organizzativo si considera sempre idoneo a prevenire reati della specie di quello verificatosi quando nell'ambito della procedura di riconoscimento dell'interesse strategico nazionale sono stati adottati provvedimenti diretti a realizzare, anche attraverso l'adozione di modelli organizzativi, il necessario bilanciamento tra le esigenze di continuità dell'attività produttiva e di salvaguardia dell'occupazione e la tutela della sicurezza sul luogo di lavoro, della salute, dell'ambiente e degli altri eventuali beni giuridici lesi dagli illeciti commessi".

7.3.2 *La pubblicazione della sentenza.*

L'art. 18 del d.lgs. 231/2001 disciplina la sanzione c.d. *stigmatizzante* della pubblicazione della sentenza. Questa, come detto, può essere disposta solo ove sia stata applicata una sanzione interdittiva e deve essere *irrogata* in conformità all'art. 36 c.p., in materia di *pubblicazione della sentenza penale di condanna* della persona fisica. Inoltre, la sentenza riguardante l'ente deve essere affisa nel comune ove l'ente ha la sede principale.

7.3.3 *La confisca.*

L'art. 19 dispone che la confisca del prezzo o del profitto del reato sia obbligatoriamente disposta con la sentenza di condanna.

Si tratta di un'ipotesi speciale di confisca, che esula dal disposto dell'art. 240 c.p. in materia di misure di sicurezza.

Essa è sempre disposta, salvo che per la parte che può essere restituita al danneggiato ovvero su cui gravino diritti di terzi acquisiti in buona fede. Ove non sia possibile confiscare il *prezzo* o il *profitto* del reato, si potrà procedere per equivalente di denaro, beni o altre utilità.

Ha natura obbligatoria e deve essere applicata anche quando, in caso di commissione del reato da parte del soggetto apicale, operi la causa di non punibilità dell'ente che dimostri la fraudolenta elusi ne dei modelli idoneamente attuati. La *ratio*, in tal senso, deve essere ricercata nella necessità di impedire che il profitto di attività illecita rimanga nella disponibilità dell'ente, costituendone patrimonio.

In tal senso, la giurisprudenza ha chiarito che il "la nozione di profitto confiscabile richiamata negli artt. 240 c.p. e 19 d. Igs. n. 231/2001 debba ritenersi riferita al vantaggio di natura economica che si risolve per colui che ne beneficia in un effettivo incremento patrimoniale

e che possa ritenersi di diretta ed immediata derivazione causale dal reato"[395]. Ciò nonostante, non sono mancate pronunce che hanno ammesso l'estensibilità della confisca anche ai vantaggi indiretti derivanti dalla commissione del reato[396].

7.4 *Reati presupposto e criptovalute.*

Così ricostruita la disciplina della responsabilità amministrativa dell'ente, guardando al catalogo dei reati previsti agli artt. 24 -25 *octiesdecies*, non può escludersi la possibilità che l'ente possa rendersi responsabili di determinati reati commessi con l'utilizzo di criptovalute.

In particolare, il riferimento è alle fattispecie incriminatrici previste all'art. 24 *bis* (Delitti informatici e trattamento illecito di dati), art. 25 *quater* (Delitti con finalità di terrorismo o eversione dell'ordine democratico), art. 25 *sexies* (abusi di mercato), art. 25 *quinquies* (Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio), art. 25 *quinquiesdecies* (reati tributari).

8. *Criptovalute e misure ablatorie.*

Le caratteristiche tanto oggettive quanto soggettive delle condotte commesse dai criminali economici hanno indotto il legislatore a prevedere un sistema sanzionatorio complesso in cui convivono la pena, le sanzioni amministrative e le misure di sicurezza patrimoniali.

E così, per gran parte delle fattispecie incriminatrici analizzate, il legislatore ha previsto l'applicazione della misura ablatoria della confisca, volta a sottrarre alla disponibilità del condannato tanto il profitto quanto il prezzo del reato.

---

[395] Cass. pen., Sez. V, sent. n. 10265/2014.

[396] Per le modalità di confisca, v. *infra* § 8. *Criptovalute e misure ablatorie.*

Si tratta di una misura proteiforme, che assume una certa centralità tanto come strumento di *dissuasione* dall'agire criminale quanto come risposta alla *commissione* di un fatto di reato che abbia comportato un *profitto* o un *prezzo*.

Tale sistema, tuttavia, viene progressivamente chiamato a fare i conti con l'innovazione tecnologica, che ne mina l'*operatività*, privandola della sua effettività, così rischiando di *incentivare* – nella valutazione del *rapporto costi-benefici* – l'agire del colletto bianco.

Questo è tanto più vero se si ha riguardo al *locus commissi delicti* per eccellenza del XXI secolo: la rete.

In tale contesto, occorre, dunque, interrogarsi sull'applicabilità della confisca ai reati in cui le criptovalute costituiscono il *profitto* o il *prezzo* ovvero *servirono o furono destinate a commettere il reato.*

Si tratta, invero, di *strumenti* caratterizzati da *volatilità,* non materialmente detenuti, difficilmente rintracciabili e, quindi, confiscabili.

8.1 *La confisca.*

L'art. 240 c.p. qualifica 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 di 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 possibile eseguire la confisca del profitto o del prodotto diretti"[397].

---

[397] In materia di confisca si rinvia, senza pretese di esaustività, a L. ORNARI., *Criminalità del profitto e tecniche sanzionatorie. Confisca e sanzioni pecuniarie nel diritto penale "moderno*", Cedam, Padova, 1997; A.M. MAUGERI, *Le moderne sanzioni patrimoniali tra funzionalità e garantismo*, Giuffrè, Milano, 2001, p. 127; A. ALESSANDRI A., *La confisca*, in AA.VV., A. ALESSANDRI (a cura di), *Il nuovo diritto penale delle società*, Ipsoa, Milano, 2002; A. ALESSANDRI., *Criminalità economica e confisca del profitto*, in E. DOLCINI E., C.E. PALIERO, *Studi in onore di Giorgio Marinucci*, Giuffrè, Milano, 2006, p. 2107; D. FONDAROLI., *Le ipotesi speciali di confisca nel sistema penale. Ablazione patrimoniale, criminalità economica, responsabilità delle persone fisiche e giuridiche*, Bononia University Press, Bologna, 2007; D. FONDAROLI, *Splendori e miserie della confisca obbligatoria del profitto*, in D. FONDAROLI (a cura di), *Principi costituzionali in materia penale e fonti sovranazionali*, CEDAM, Padova, 2008, p. 117 ss.; F. VERGINE, *Confisca e sequestro per equivalente,* Ipsoa, Milano, 2009; G. GRASSO, *sub* Art. 240, in M. ROMANO M., G. GRASSO., T. PADOVANI (a cura di), *Commentario sistematico del codice penale*, Giuffrè, Milano, 2011, p. 606 ss.; T.E., EPIDENDIO, *La confisca nel diritto penale e nel sistema delle responsabilità degli enti,* Cedam, Padova, 2011; E. NICOSIA, *La confisca, le confische. Funzioni politico-criminali, natura giuridica e problemi ricostruttivo-applicativi*, Giappichelli, Torino, 2012; F. MENDITTO, *Le confische di prevenzione e*

L'ordinamento, poi, prevede ulteriori ipotesi di confisca in relazione a specifici reati previsti dalla legge. È il caso dei reati di riciclaggio *lato sensu* intesi nonché dei reati tributari.

Vi sono poi ipotesi speciali di confisca, tra cui rientra la sanzione prevista ex art. 19, d.lgs. 231/2001[398].

8.1.1 *La confisca di criptovalute.*

Le caratteristiche delle criptovalute impongono di ripensare completamente il sistema delle misure ablatorie non tanto con riguardo ai suoi contenuti quanto, piuttosto, alle modalità di esecuzione.

Si tratta, infatti, di valori difficilmente tracciabili, immateriali e soggetti a volatilità.

Appare, quindi, necessario superare le procedure tradizionali e prevedere una disciplina normativa apposita che possa regolarne sia la tracciabilità sia la quantificazione.

8.1.1.1 *Il procedimento di confisca.*

Le caratteristiche della *blockchain* richiedono, in primo luogo, un avanzamento della *digital forensics*, che permetta di individuare più agevolmente i *wallet* del condannato.

In tal senso, si rende necessaria la messa a punto di precise tecniche di tracciamento, che possano prevedere, accanto a strumenti investigativi innovativi, incentivi premiali capaci di influenzare positivamente l'agire del *white collar* e di soddisfare le esigenze di tutela dell'ordinamento, sicché sia egli stesso a rendersi collaborativo e a consegnare, sua sponte, le chiavi private, che permettono di accedere al suo (o ai suoi) portafogli. Ed invero, la natura decentralizzate delle criptovalute, la loro struttura crittografica e il funzionamento delle chiavi digitali rendono particolarmente difficile immaginare uno "spossessamento coatto" da parte delle autorità statali.

Al riguardo, è necessario distingue due diverse ipotesi,

Il primo caso, più semplice, è quello in cui il soggetto detenga i propri fondi presso un *wallet provider*: la problematica potrebbe essere risolta introducendo una disciplina che obblighi il prestatore di servizi a consegnare alle autorità le chiavi digitali, sì da potere accedere al portafoglio e, quindi, alla criptovaluta provento o prezzo del delitto commesso.

---

*penali,*Giuffrè Milano, 2015; F. MAZZACUVA, *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico*, Giappichelli, Torino, 2017, p.95 ss.;

[398] *Cfr. supra*, § 7. *La responsabilità dell'ente e l'utilizzo di criptovalute* e, in particolare, § 7.3.4. *La confisca.*

Il secondo caso, invece, riguarda l'ipotesi in cui l'*user* detenga autonomamente le proprie criptovalute, senza appoggiarsi a soggetti terzi. In tale situazione, invero, non sembra potersi prescindere dalla collaborazione dell'indagato o imputato e, poi, del condannato, che deve permettere alle forze dell'ordine di accedere ai suoi *wallet* per eseguire il sequestro o la confisca. Se nella fase delle indagini e del processo una collaborazione dell'imputato pare auspicabile e, comunque, più facilmente ottenibile; diverso è il caso dell'imputato ormai condannato, nei cui confronti sia stata disposta la confisca.

In tal caso, ove la confisca criptovalutaria risultasse particolarmente complessa, potrebbe applicarsi una confisca per equivalente, in ragione del valore del prezzo o del profitto del reato accertati nel corso del procedimento.

8.1.1.2 *La volatilità.*

Una volta ottenuto l'accesso al *wallet* potrebbe porsi il problema della *quantificazione.*

La decentralizzazione delle criptovalute, infatti, rende fortemente imprevedibile l'andamento del mercato criptovalutario e, conseguentemente, incide fortemente sul valore delle valute virtuali ancorate al principio della domanda e offerta che, tuttavia, non necessariamente è influenzato dall'andamento della borsa.

In tal senso, si pone un problema di *quantificazione* che riguarda tanto il momento di applicazione della misura ablatoria quanto quello dell'esecuzione. È, infatti, altamente probabile che nelle more il valore della criptovaluta subisca un innalzamento del prezzo o una sua diminuzione rispetto alla fase di applicazione.

Quanto alla quantificazione del prezzo o del profitto, pare potersi fare riferimento al valore della criptovaluta al momento del *tempus commissi delicti*: si tratta di un dato facilmente ricavabile e che permette una corretta valutazione in ordine al valore da confiscare. Rispetto al momento dell'esecuzione, ove lo strumento abbia subito una *deminutio* rilevante pare potersi ammettere, oltre all'ablazione delle criptovalute, anche la confisca per equivalente del residuo, calcolato sul valore del prezzo o del profitto al momento della commissione del fatto di reato.

8.1.1.3 *Il trasferimento dei fondi.*

Una volta ottenuto l'accesso al *wallet* e confiscati i fondi, la fase più semplice sembra essere quella del *trasferimento.*

Sarebbe, infatti, possibile istituire uno o più *wallet* di Stato, ove possano essere depositate tutte le criptovalute confiscate.

8.1.2 *Brevi considerazioni conclusive.*

Alla luce di quanto osservato appare necessario, al fine di assicurare l'efficacia e l'efficienza delle misure ablatorie già in termini general preventivi, che il legislatore introduca una nuova disciplina procedimentale, che possa dettare nuove regole in materia di confisca sulla *blockchain*.

In tal senso, dovranno essere definiti meccanismi premiali per il reo, che possano, almeno astrattamente, facilitare l'accesso ai portafogli di criptovalute. Al proposito, potrebbe ricorrersi a una riduzione del valore confiscabile o al riconoscimento, in fase di commisurazione della pena, di una circostanza attenuante appositamente introdotta in materia.

Infine, sarà necessario individuare precise regole che possano fare fronte alla necessità di quantificare il valore delle criptovalute, in quanto uno strumento altamente volatile.

IV CAPITOLO

LA DISCIPLINA DELLE CRIPTOVALUTE NEL CONTESTO INTERNAZIONALE

1. *Premessa.*

L'espansione del fenomeno criptovalutario ha, di gran lunga, anticipato – com'è, d'altra parte, prassi, nei reati economici – lo sviluppo legislativo in materia.

In tal senso, nonostante la portata globale del fenomeno criptovalutario, ancora oggi risulta mancante una disciplina internazionale, capace di rispondere in maniera *efficace*, *efficiente* ed *unitaria* alla commissione di reati economici con l'utilizzo delle valute virtuali.

Lungi dall'essere una pretesa accessoria, un intervento normativo in materia pare porsi come assoluta priorità, sì da evitare, ancor prima che fenomeni di impunità, conseguenze difficilmente rimediabili sul fronte economico-finanziario.

Ed invero, sebbene nel 2023, gli Stati si siano mossi esattamente in questa direzione – con un notevole aumento dei Paesi che hanno introdotto un preciso quadro normativo, volto a disciplinare le valute virtuali – il panorama globale appare ancora non uniforme e non armonizzato.

Al riguardo, lo studio condotto da *PwC*, pubblicato nel dicembre 2023, mostra come, a livello mondiale, quasi tutte le giurisdizioni siano dotate di un Quadro normativo che prevede precisi obblighi di registrazione per i prestatori di servizi digitali, una disciplina AML dotata di *travel rule*, nonché di specifiche norme sulle *stablecoin*.[399] In tal senso, un ruolo antesignano deve essere riconosciuto all'Unione Europea che, per prima, ha introdotto un regolamento "inter-giurisdizionale".

Diversamente, nonostante l'impegno attivo a livello legislativo e regolamentare, non risultano ancora dotati di un quadro normativo generale gli Stati Uniti d'America, il Regno Unito, l'Australia, il Canada, l'India, la Norvegia, il Qatar, il Sudafrica e Taiwan.

---

[399] PwC, *Navigating the global crypto landscape*, dicembre 2023, in www.pwc.it, reperibile al seguente link.

Il processo legislativo non risulta, invece, ancora avviato in Brasile, in Turchia e in Uganda, completamente privi di normativa anche in punto di obblighi di registrazione e di *travel rule*.

2. *Quesito e obiettivo.*

Ebbene, quest'ultima parte della ricerca mira a fornire un sintetico quadro della situazione giuridica mondiale, prendendo in considerazione le due soluzioni estreme che si sono prospettate: da un lato, i Paesi che hanno vietato categoricamente l'utilizzo delle criptovalute; dall'altro lato, gli Stati che non solo ne hanno liceizzato la detenzione, l'acquisto e la vendita, ma hanno anche riconosciuto corso legale alle valute virtuali, equiparandole in tutto e per tutto alla moneta ufficiale.

In particolare, la delineazione nei soli tratti essenziali delle decisioni assunte dagli Stati in materia, lungi dal fornire una rappresentazione completa di tutti gli atti normativi intervenuti in ciascun Paese, mira a comprendere le motivazioni poste alla base di una o dell'altra scelta.

In tal senso, si intende riflettere in ordine alle ragioni che hanno sorretto, rispettivamente, la scelta di *criminalizzazione* ovvero di completa *liceizzazione* delle criptovalute. L'obiettivo è, quindi, comprendere se il legislatore europeo e, quindi, quello nazionale avrebbero potuto optare per politiche diverse, anziché tentare di (ri) disciplinare – con non poche difficoltà e, comunque, con persistenti lacune – l'intero sistema normativo.

3. *Divieto di utilizzo delle criptovalute.*

Sono diversi i governi che hanno vietato l'utilizzo, *lato sensu* inteso, della criptovaluta nell'ambito della propria giurisdizione.

In particolare, i motivi di tali scelte – che muovono, principalmente, da preoccupazioni economiche, normative e di sicurezza – paiono potersi compendiare come segue.

Innanzitutto, vi è un forte timore di *stabilità finanziaria*. Gli Stati proibizionisti temono, infatti il potenziale impatto delle criptovalute sui loro sistemi finanziari nazionali. Più precisamente, il timore è che la natura decentralizzata e, spesso, volatile delle criptovalute possa comportare seri rischi per gli investitori, che potrebbero essere travolti dall'andamento imprevedibile del mercato criptovalutario, con conseguenze anche sulle istituzioni finanziarie.

In tal senso, si teme che la mancanza di meccanismi di protezione degli investitori nei mercati delle criptovalute possa rendere i consumatori più vulnerabili, in quanto più facilmente soggetti a frodi, truffe e fenomeni di abusivismo.

Ed invero, le caratteristiche proprie delle criptovalute – quali, *in primis*, l'anonimato e la decentralizzazione – semplificherebbero la commissione di reati economici, idonei ad incidere negativamente anche sull'andamento del mercato interno. Si ritiene, infatti, che liceizzare l'utilizzo delle criptovalute possa attirare capitali illeciti, poi riversati nel mercato interno.

La decentralizzazione, in particolare, solleva perplessità in ordine, da un lato, alle capacità dello Stato di prevenire e controllare la commissione di crimini economici; dall'altro lato, di garantire sistemi tributari idonei ad evitare che le imprese, in particolare, possano utilizzare le criptovalute per eludere il fisco, sottraendo introiti allo Stato.

È bene notare come in diversi paesi in cui le risorse digitali sono ufficialmente vietate, gli individui continuano a commerciare attivamente o a detenerle come riserva di valore o come modo per generare reddito. Anche in questo caso, lo (pseudo) anonimato e la decentralizzazione vengono sfruttate per eludere i divieti imposti a livello statale.

3.1 *Asia.*

Sebbene la Cina, quantomeno sino al 2018, sia stato il più grande *hub* di *mining* di criptovaluta Bitcoin in tutto il mondo, ad oggi è uno dei Paesi che ha previsto maggiori limitazioni avverso l'utilizzo e la detenzione delle valute virtuali.

Ed invero, la Repubblica Popolare Cinese ha posto delle severe restrizioni rispetto all'uso dei Bitcoin. Tale *input* è sorto a seguito del report emanato dalla Banca Popolare della Cina nel dicembre 2013, in cui annunciava di vietare le transazioni che avessero ad oggetto Bitcoin a tutte le istituzioni finanziarie nazionale. Il divieto non si è esteso automaticamente ai privati, che hanno continuato a fare un grande uso della criptovaluta: l'agenzia Goldman Sachs ha rilevato come nei primi sei mesi del 2015, oltre l'80% delle transazioni di cambio di Bitcoin è avvenuto in Yuan Cinesi[400].

A inizio 2019, inoltre, il *Comitato nazionale cinese per lo sviluppo e le riforme* (NDRC), ha sollevato il problema circa l'elevato dispendio di energia causato dall'attività di *mining*, complice anche un costo molto basso dell'elettricità in Cina. L' NDRC ha infatti considerato tali attività dannose per l'ambiente. Sono state, quindi, chiuse le piattaforme di *trading* e, dal 2021, e gran parte delle attività di *mining*.

[400] A. CAPOGNA, et altri, *op.cit.*, p. 52.

Alla base di tali scelte ci sono state, da un lato, le preoccupazioni sulla stabilità finanziaria strettamente legate alla decentralizzazione della moneta e, dall'altro lato, il percepito aumento dei rischi di commissione di operazioni di riciclaggio.

Tuttavia, per cercare di garantire i vantaggi di una risorsa digitale, ma non decentralizzata, la Cina ha incoraggiato l'adozione del e-yuan, quale criptovaluta di Stato.

È bene evidenziare come Hong Kong SAR non sia sottoposta a questi divieti. Ed invero, Hong Kong gode SAR è una regione amministrativa speciale con una disciplina autonoma rispetto alla Cina, anche rispetto alle criptovalute.

Ed infatti, contrariamente a quanto permesso in Cina, Hong Kong mira a diventare un hub globale per gli Asset Virtuali attraverso l'implementazione di un quadro normativo armonizzato che copra l'intero ecosistema.

In particolare, secondo la legge di Hong Kong, le criptovalute non hanno corso legale regolato dalla HKMA e non si qualificano come denaro.

È dotata di un'apposita disciplina antiriciclaggio pubblicata nell'ottobre 2023 unitariamente all'Autorità Monetaria Locale.

Il Nepal ha vietato le transazioni di criptovaluta dal 2017, quando la banca centrale del paese ha emesso una direttiva che afferma che qualsiasi transazione che coinvolge criptovaluta sarebbe considerata illegale. Si pensi che all'inizio di ottobre 2017, una squadra di polizia del Central Investigation Bureau (CIB) della polizia del Nepal "per la prima volta ha arrestato sette persone per aver presumibilmente gestito attività di scambio di bitcoin da varie parti del paese

Nel 2020, l'Autorità di Regolamentazione del Centro Finanziario del Qatar (QFCRA) ha vietato l'utilizzo di tutti gli *asset virtuali*, comprese le criptovalute ad eccezione dei servizi relativi ai titoli token. Tuttavia, è attualmente in corso la procedura legislativa volta regolamentare il mercato finanziario degli Asset Digitali.

3.2 *Africa.*

Diverse nazioni africane hanno imposto divieti a titolo definitivo sulle criptovalute. In particolare, risulta vietato l'utilizzo e la detenzione di criptovaluta in Algeria, Ghana, Lesotho e Sierra Leone, Egitto, Libia e Marocco.

In Algeria, ad esempio, il governo ha emesso una legge nel 2018 che criminalizza l'uso, l'acquisto, la vendita e la detenzione di criptovalute, citando preoccupazioni sul loro potenziale uso in attività illegali.

In Marocco, l'Ufficio per i cambi e la banca centrale hanno emesso un avvertimento congiunto nel 2017, sottolineando che le transazioni che coinvolgono criptovalute sarebbero soggette a sanzioni.

Particolare è la situazione in Egitto. Ed invero, le autorità egiziane sono state a lungo critiche nei confronti delle valute digitali.

Nel 2018, i leader religiosi hanno rilasciato una dichiarazione secondo cui le valute virtuali sono vietate dalla legge islamica.

Nel 2020, la Banca centrale d'Egitto ha pubblicato regole di licenza per l'emissione, la negoziazione o la promozione di criptovalute, lasciando intravedere un'apertura alla liceizzazione delle valute virtuali.

Tuttavia, nel 2023, la Banca Centrale egiziana ha pubblicato una nuova comunicazione in materia, ribadendo che "*its previous warnings against dealing with all types of cryptocurrencies; whether through individuals, companies, applications, or digital platforms. Thereby, the Central Bank of Egypt emphasizes that no license has ever been issued or granted to engage in such trading activities in the Egyptian market due to the high risks they comprise, including but not limited to, fluctuations and significant price volatility; as well as their use in financial crimes, and electronic piracy.*

Additionally, cryptocurrencies are not issued by any central bank or any official centralized issuing authority, that can be held accountable, and is consequently lacking any issuing cover that would guarantee the stability of such currency and protect the rights of its users"[401]. Ha, quindi, chiuso definitivamente alla possibilità di liceizzare le criptovalute.

Completamente opposti gli avvenimenti che hanno riguardato l'Etopia. Ed invero, sebbene nel giugno 2022 la banca centrale avesse ribadito l'illegalità delle criptovalute, meno di tre mesi dopo, ad agosto, ha ammesso la possibilità di utilizzare le criptovalute, affermato che gli operatori di criptovaluta erano tenuti a registrarsi presso l'Information Network Security Administration (INSA), l'agenzia di sicurezza informatica del governo, entro 10 giorni. L'INSA ha affermato di essere interessata a legalizzare i servizi di *mining* e di trasferimento di criptovalute[402].

3.3 *America Latina.*

L'Autorità di vigilanza del sistema finanziario della Bolivia ha emesso una risoluzione nel 2014 che vieta l'uso di Bitcoin e altre valute digitali, facendo leva sulla mancanza di protezione dei consumatori e il potenziale di riciclaggio di denaro. In tal senso, nel 2022, la Banca Centrale Boliviana ha vietato al

[401] Si rinvia al sito della Banca Centrale egiziana www.cbe.org.eg.
[402] Si rinvia a www.ethiopiamonitor.com.

settore bancario di utilizzare, commercializzare o transare attività di criptovaluta per proteggere il pubblico da "rischi, frodi e truffe" e "il rischio di creare perdite economiche".

Proprio come accaduto in Cina, l'Ecuador, nel vietare l'uso di criptovalute decentralizzate, è stato uno dei primi paesi a introdurre il la criptovaluta centralizzata il *Sistema de Dinero Electrónico*.

3.4 *India.*

Anche in india si sono registrati divieti avverso l'attività in criptovaluta. Ad esempio, il Bangladesh nel 2017 ha vietato l'utilizzo delle valute virtuali, financo a prevedere la pena della reclusione per coloro che le usano.

In questo caso il divieto è stato fondato, principalmente, sui rischi di riciclaggio di denaro e finanziamento del terrorismo.

Ciò nonostante, nel 2020 il governo ha pubblicato il *National Blockchain Strategy*, in cui ha riconosciuto la necessità di esplorare le potenzialità della tecnologia *blockchain* al fine di far progredire la sua capacità tecnica, aumentare l'efficienza nelle *e-governances* e promuovere le innovazioni. Così, almeno in apparenza, aprendo all'utilizzo della tecnologia DLT[403].

Probabilmente detto cambio di rotta è stato dovuto al contenuto della Suprema Corte dell'India, che ha dichiarato l'incostituzionalità del divieto.

Nel 2022, tuttavia, la Bangladesh Bank ha emesso un avviso con cui ha vietato qualsivoglia attività che abbia ad oggetto le valute virtuali. Da ultimo, nel settembre 2023, in occasione del Vertice del G20, l'India si è unita ai Paesi membri del G20 per adottare all'unanimità la Dichiarazione dei Leader del G20 di Nuova Delhi. La Dichiarazione ha approvato le raccomandazioni di alto livello del Consiglio per la Stabilità Finanziaria (FSB) per la regolamentazione, la supervisione e la sorveglianza delle attività e dei mercati di cripto-asset, nonché gli accordi globali di stablecoin.

4. *Criptovaluta avente corso legale.*

Accanto a Paesi che hanno completamente negato la liceità delle criptovalute vi sono El Salvador e la Repubblica Centrafricana che, al contrario, non solo hanno ammesso la liceità delle valute virtuali, ma hanno anche dichiarata il corso legale del Bitcoin, equiparato in tutto e per tutto alla moneta avete corso legale.

---

[403] Il documento è consultabile al sito www.pib.gov.it.

4.1 *El Salvador.*

È stato il primo Paese in assoluto, nel settembre 2021, a introdurre il Bitcoin come valuta a corso legale accanto al dollaro USA.

In tal senso, è stata altresì lanciata Chivo Wallet, un'*app* statale che permette di effettuare transazioni da Bitcon a USD e viceversa senza pagare le commissioni sulle transazioni.

Tuttavia, dallo studio pubblicato su Science dall' *American Association for the Advancement of Science* nel dicembre 2023, emerge chiaramente come i cittadini di El Salvador continuino a preferire l'utilizzo del dollaro USA. Paradossalmente è emerso come i cittadini siano intimoriti dalla possibilità di utilizzare una moneta decentralizzata e anonima[404].

Ciò nonostante, in data 15 marzo 2024 il Presidente Nayib Bukele ha dichiarato di avere accumulato, a livello statale, 400 milioni di dollari, conservati su un *cold wallet*, vale a dire un *portafoglio offline*, utile a prevenire attacchi *hacker.*

4.2 *Repubblica Centrafricana.*

La Repubblica Centrafricana è stata, nell'aprile 2022, il secondo paese al mondo dopo El Salvador a dare corso legale alle criptovalute accanto al Franco CFA, moneta ufficiale della Repubblica.

Nonostante le perplessità iniziali delle Autorità mondiali, nel maggio 2023 il Fondo Monetario Internazionale ha pubblicato un rapporto in cui ha evidenziato come la RCA stia sfruttando al meglio il potenziale del Bitcoin per rilanciare l'economia del proprio paese. In tal senso, si indicava una crescita del PIL reale del 2,2% in un solo anno, con importanti riflessi anche sul tasso di inflazione medio[405].

5. *La regolamentazione delle criptovalute come strumento di gestione del rischio.*

È sostanzialmente possibile individuare una e una sola ragione che ha indotto i diversi Stati richiamati a vietare l'utilizzo delle criptovaluta: il rischio della decentralizzazione e dell'anonimato.

---

[404] F. ALVAREZ, D. ARGENTE, D. VAN PATTEN, *Are cryptocurrencies currencies? Bitcoin as legal tender in El Salvador*, in *Science*, 2023, Vol. 382, in www.science.org, reperibile al seguente link..

[405] FONDO MONETARIO INTERNAZIONALE, *Central African Republic: 2023 Article IV Consultation and request for a 38-month arrangement under the Extended Credit Facility-Press Release; Staff Report; and Statement by the Executive Director for the Central African Republic,* Maggio 2023, in www.imf.org, , reperibile al seguente link.

I Governi, invero, temono che le caratteristiche delle criptovalute possano rappresentare, *ex se*, un rischio per il sistema economico-finanziario, che non può essere controllato da nessuna Autorità statale. Non considerano, tuttavia, che vietare *sic et sempliciter* l'utilizzo di uno strumento non comporta, automaticamente, l'eliminazione del rischio. E ciò pare tanto più vero se si ha riguardo alle criptovalute che, proprio in ragione della decentralizzazione e dello pseudoanonimato di cui sono "affette", più che essere vietate, dovrebbero essere *gestite.*

In tal senso, la completa criminalizzazione delle criptovalute non può che rappresentare un mero palliativo ai timori delle Autorità statali.

Vietare piattaforme di *trading*, società di servizi di intermediazione criptovalutaria non elimina il problema avvertito dagli Stati. E anzi, proprio le caratteristiche della *blockchain*, ove non sottoposte a normativa alcuna al di fuori del divieto imposto, costituiscono lo strumento che permetterà all'utente di eludere l'ostacolo. D'altra parte, il Governo così come non riuscirà a controllarne l'utilizzo lecito, non potrà controllarne l'utilizzo illecito, in quanto conseguente all'introduzione di un divieto.

Tutt'altre riflessioni, di stampo più che altro economico richiede la scelta dei Paesi di equiparare il la criptovaluta – nel caso di specie – il Bitcoin alla moneta avente corso legale.

Deve, al riguardo, citarsi lo studio condotto da Tobias Adrian e Rhoda Weeks Brown, analisti del Fondo Monetario Internazionale, pubblicato nel luglio 2021 proprio sul *blog* del Fondo[406]. In tale occasione, infatti, è stato dato conto dei rischi che potrebbero derivare dall'equiparazione della criptovaluta alla moneta avente corso legale.

Se è vero che l'adozione del Bitcoin come valuta garantisce maggiore velocità nelle transazioni e minori costi delle stesse, a fronte di operazioni *internazionali*, è altresì vero che la connaturata volatilità e la mancanza di un ente centrale di garanzia, rappresentano rischi che un Paese non dovrebbe assumersi. Vi sarebbero, invero, importanti ed evidenti problemi per la stabilità economica interna e per la coesione sociale a livello internazionale. Sarebbe, in tal senso, difficoltoso in ambito di politica monetaria globale stabilire i tassi di cambio su una moneta straniera.

Pare, dunque, potersi affermare che l'unica arma nelle mani del legislatore a fronte di strumenti criptovalutari caratterizzati da decentralizzazione e pseudoanonimato, rimanga quella della *regolamentazione* che, più che prevenire il rischio – talvolta imprevedibile – possa mirare a gestirlo.

---

[406] T. ADRIAN, R, D. HE, A. NAIRAIN, *Global crypto regulation should be comprehensive, consistent and coordinated*, in www.blogs.imf.org, reperibile al seguente link.

CONCLUSIONI

Le risultanze emerse nel corso della ricerca inducono a ritenere che il *cybercriminal* è un criminale economico che, forte delle proprie competenze informatiche, riesce a individuare le lacune del sistema e a sfruttare i vuoti normativi al fine di trarne profitto.

È stato, al riguardo dimostrato come la tecnologia *blockchain*, seppur nata come strumento positivo, funzionale alla pubblicità e alla trasparenza delle transazioni, è stata sin da subito sfruttata dai *cybercriminal* con effetti disfunzionali su beni giuridici primari e per l'economia.

Le caratteristiche proprie della tecnologia quali la decentralizzazione, l'irreversibilità delle transazioni e lo pseudoanonimato degli utenti, pensate dagli sviluppatori per tutelare la *privacy* e l'indipendenza dalle autorità statali, sono state, infatti, ben presto sfruttate nel loro funzionamento per fini criminali, consistenti nella commissione di condotte lesive di beni giuridici primari e per l'economia. Non manca, tuttavia, l'utilizzo di strumenti idonei ad alterarne, ulteriormente, le funzionalità. È questo il caso dei *software* di *mixing*, che potenziano lo pseudoanonimato proprio della *blockchain*, rendendo le transazioni del tutto anonime.

Ciò detto, è stato dimostrato come le criptovalute si prestino alla commissione di tutti i reati di natura economica potendo, in ragione di detta versatilità, essere utilizzate nella commissione di delitti contro il patrimonio, certo, ma anche contro lo Stato, l'amministrazione finanziaria e l'interesse dell'Unione.

Non vi è dubbio, tuttavia, che il terreno di elezione resti, ancora oggi, quello delle frodi informatiche e del riciclaggio che rappresentano l'ambito criminale in cui le criptovalute assumono maggiore rilevanza.

È bene evidenziare, tuttavia, come nonostante l'innovazione apportata dalle criptovalute alle modalità di condotta, il sistema normativo si sia dimostrato sufficientemente idoneo a rispondere a condotte sostanzialmente lesive dei beni giuridici, di volta in volta tutelati.

Ed invero, l'analisi esegetica e nomofilattica condotta ha permesso di ricondurre i *crimini* manifestatisi a fattispecie incriminatrici già previste dall'ordinamento, rivelatisi idonee ad accogliere, nel pieno rispetto del principio di legalità penale – *sub specie* di tassatività – le condotte tenute dai criminali economici con l'utilizzo di criptovalute.

È stata, al riguardo, rilevata una sola carenza in materia di delitti contro lo Stato, che rende opportuno un intervento del legislatore italiano in modifica dell'art. 270 *quinquies*.1. c.p., che preveda la rilevanza penale di erogazioni in criptovalute, sicché il bene giuridico tutelato dalla norma possa trovare effettiva protezione anche a fronte dell'evolversi della tecnologia e delle modalità di finanziamento.

L'ulteriore disciplina tanto nazionale quanto sovranazionale appare solo parzialmente idonea a rispondere al fenomeno criminale, nel rispetto dei principi di offensività, legalità penale e colpevolezza.

Gli esiti della ricerca hanno, infatti, permesso di accertare come la disciplina della Quarta e Quinta Direttiva Antiriciclaggio si sia rivelata sostanzialmente inefficace. Ed invero, sebbene potrebbe pensarsi che, a fronte della disciplina e degli obblighi cui sono sottoposti gli intermediari (*exchange* e *wallet provide*), la maggiore parte delle condotte criminose passi dal rapporto *utente-utente*, in realtà, gli studi condotti in materia dal dott. Nazzari hanno portato ad esiti diversi. È, al riguardo, emerso come il 52% delle transazioni illecite passa da soggetti intermediari.

Risulta, invece, limitato l'utilizzo di *mixing* service, pari all'8% delle transazioni.

In parte, la problematica potrebbe risultare risolta dall'introduzione della *travel rule*, che obbligherà gli intermediari a fornire tutte le informazioni relative alla transazione.

Tuttavia, come detto, la disciplina del Reg. 1113/2023, non riguarderà le transazioni tra privati che, ancorché costituenti la manifestazione minore del fenomeno criminale, rappresentano un'ipotesi ancora irrisolta per il legislatore tanto europeo quanto nazionale.

Deve, peraltro, precisarsi come il minore utilizzo dei *mixing* non possa, di per sé, giustificare il mancato intervento normativo in materia. Ancora oggi, infatti, questi *software* sono astrattamente leciti nonostante gli scopi principalmente criminosi perseguiti.

Ulteriore carenza normativa riguarda le misure ablatorie che paiono, oggi, sostanzialmente inapplicabili agli autori di reati commessi con le criptovalute, in ragione, ancora una volta, delle caratteristiche della tecnologia, che non permettono un'agevole ablazione delle criptovalute che costituirono lo strumento, il provento o il profitto nella commissione del reato.

Alla luce di quanto sin qui osservato, deve ritenersi che la disciplina normativa sin qui elaborata – ancorché strutturalmente e astrattamente idonea, in un'ottica di general prevenzione, alla tutela dei beni giuridici coinvolti – necessiti di appositi interventi legislativi che la rendano maggiormente efficace, efficiente ed effettiva.

In tal senso, correttivi in materia dovranno essere previsti con riguardo all'utilizzo dei *mixing* – che potranno essere vietati o sottoposti agli obblighi antiriciclaggio al pari degli intermediari –e rispetto alle misure ablatorie, che come sopra suggerito, dovranno prevedere precisi meccanismi di collaborazione del reo che, in uno schema *carrot-stick approach*, permettano la confiscabilità del bene a fronte di una riduzione del *quantum* oggetto di ablazione.

Può quindi concludersi affermando il *paradosso della decentralizzazione*: l'utilizzo delle criptovalute, nate come strumenti volti a garantire la *privacy*, l'anonimato e l'indipendenza degli utenti dalle autorità statali, non possono prescindere da una *centralizzazione* delle valute virtuali.

La *decentralizzazione* della *blockchain* deve, essere, infatti compensata con la *centralizzazione* dei controlli. Di talché, stante la particolarità della materia trattata, anche e soprattutto in considerazione delle caratteristiche della tecnologia in parola, appare opportuno immaginare la costituzione di una nuova e apposita divisione all'interno delle Autorità già operative in ambito bancario-finanziario ovvero di ente autonomo, tanto a livello sovranazionale quanto nazionale, preposto ai controlli. Ed invero, solo un gruppo eterogeneo di professionisti della materia – composto, tra gli altri, da informatici, giuristi, statistici, economisti e criminologi – potrebbe, in astratto, permette l'elaborazione di soluzioni idonee ad arginare il fenomeno in parola.

In tal senso, se – come visto – oggi gli obblighi di registrazione degli utenti – con conseguente possibilità di associarvi le chiavi private – sorgono solo in capo ad *exchanger* e *wallet provider*, appare quantomai necessaria una disciplina idonea ad indurre tutti gli utilizzatori, anche privati, a dichiarare allo Stato la detenzione di criptovalute con conseguente onere di registrazione delle chiavi private.

L'immissione dei dati relativi alle chiavi private detenute dagli utenti nel circuito statale permetterebbe, infatti, la generale possibilità di ricondurre un'operazione sospetta a un determinato utente, sì da assicurare un efficiente controllo da parte delle autorità a ciò preposte.

Assumerà, pertanto, rilievo la *collaborazione* con lo Stato del consociato tanto in fase preventiva quanto riparativa.

Al riguardo, da un punto di vista prettamente criminologico e giuridico, sul fronte della *general- prevenzione* appare interessante ipotizzare come gli incentivi alla registrazione potrebbero passare da una disciplina di maggiore favore in ambito tributario, sicché i soggetti registrati beneficino delle plusvalenze prodotte, senza rinunciare al guadagno, ma garantendo un maggiore controllo da parte dello Stato.

Nello stesso senso, all'esito della commissione di un reato tramite l'utilizzo di criptovalute, potrebbe valorizzarsi punto di *commisurazione* della pena il comportamento susseguente adottato dal reo in– per esempio, prevedendo la concessione di una specifica circostanza attenuante – nonché nella fase di applicazione delle misure ablatorie previste dalla legge.

BIBLIOGRAFIA

ACCINNI G.P., *Profili di rilevanza delle «criptovalute» (nella riforma della disciplina antiriciclaggio del 2017),* in *Archivio Penale*, 2018, in www.archiviopenale.it.

ACCINNI G.P., Cybersecurity *e criptovalute. Profili di rilevanza penale dopo Quinta Direttiva*, in *Sistema Penale,* 5, 2020, in www.sistemapenale.it.

ADRIAN T., HE D., NAIRAIN A., *Global crypto regulation should be comprehensive, consistent and coordinated*, 2021, in www.imf.org.

ALESSANDRI A., *La confisca*, in AA.VV., A. ALESSANDRI (a cura di), *Il nuovo diritto penale delle società*, Ipsoa, Milano, 2002.

ALESSANDRI A., *Criminalità economica e confisca del profitto*, in E. DOLCINI E., C.E. PALIERO, *Studi in onore di Giorgio Marinucci*, Giuffrè, Milano, 2006.

ALESSANDRI A., SEMINARA S., *Diritto penale commerciale*. *Volume I. I principi generali*, Giappichelli, Torino, 2018.

ALVAREZ F., ARGENTE D, VAN PATTEN D., *Are cryptocurrencies currencies? Bitcoin as legal tender in El Salvador*, in *Science*, 2023, in www.science.org.

AMASE W., *Household Electricity Costs to Mine 1 Bitcoin at Home, Around the World*, 2023, in www.coingecko.com.

AMATO M., FANTACCI L., *Per un pugno di Bitcoin- Rischi e opportunità delle monete virtuali*, Università Bocconi Editore, Milano, 2016.

AMIR U, *Fake Bittrex cryptocurrency site stealing user funds*, 2017, in www.hackread.com.

ANTONELLI L.N., *Moneta, valuta e aggregati monetari* in *Guida al Forex,* in www.wallstreetitalia.com.

ANDRIGHETTO G., VILLATORO D., *Beyond the Carrot and Stick Approach to Enforcement: An Agent-Based Model*, *in European Perspective on Cognitive Science*, New Bulgarian University Press, 2011.

ANGELINI M., voce *Riciclaggio*, in *Digesto delle Discipline Penalistiche*, UTET, Torino, 2006.

ANNUNZIATA F., *Commento sub art. 94*, in *Commentario Marchetti-Bianchi,* Giuffrè, Milano, 1989.

ANTOLISEI F., *Diritto penale, parte speciale*, I, Giuffrè, Milano, 2008.

AA.VV., CAPACCIOLI S., (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021.

AQUARO L., *Tassazione in Italia delle operazioni in valuta virtuale*, AA.VV., *Criptovalute. Profili storico-economici e giuridici*, a cura di M. LORENZINI, M. ZULBERTI, C. IMBROSCIANO, Giappichelli, Torino, 2023.

ASCARELLI T., *Ordinamento giuridico e processo economico*, in *Studi in onore di Lorenzo Mossa,* CEDAM, Padova, 1961.

ASHMORE D., *Stablecoin: cosa sono e come funzionano*, in *Forbes Advisor*, 2023, in www.forbes.com.

AA.VV., *Digesto delle Discipline Penalistiche*, Utet, Torino.

BANCA D'ITALIA, UNIVERSITÀ CATTOLICA DEL SACRO CUORE, UNIVERSITÀ ROMA TRE, *Caratteristiche degli Smart Contract. Draft v.1.0.*, 2023, in www.bancaditalia.it.

BANDINI T. ET AL., *Criminologia. Il contributo della ricerca alla conoscenza del crimine e alla reazione sociale, Vol. I*, Giuffrè, Milano, 2003.

BARBERA M., Il *nudge e le condizioni per la sua applicazione nello Stato liberale*, in AA.VV. (a cura di), *Dalle regole ai comportamenti. Conversazioini in tema di amministrazione e persuasione*, Mimesis, 2022.

BARTOLI R., *Colpevolezza: tra personalismo e prevenzione,* Giappichelli, Torino, 2005.

BBC, *Exmo Bitcoin exchange manager kidnapped in Kiev*, 2017, in www.bbc.com.

BECCARIA C., *Dei Delitti e delle Pene,* a cura di R.FABIETTI, Mursia, Milano, 1973.

BECKER G.S., *L'approccio economico al comportamento umano,* Il Mulino, Bologna, 1998.

BENTHAM J., E. LECALDANO (a cura di), *Introduzione ai princìpi della morale e della legislazione*, Utet, Torino, 1998.

BERTOLINO M., Corporate, *criminalità*, compliance *d'impresa e personalità del* white collar offender, in *Archivio penale,* 3, 2019, in www.archiviopenale.it.

BIONDI B., *I beni*, in F. VASSALLI (diretto da) *Trattato di Diritto Civile*, Utet, Torino, 1956.

BITCOIN.ORG, *Running a full node. Support the Bitcoin network by running your own full node*, in ww.bitcoin.org.

BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche,* in *Diritto dell'Informazione e dell'Informatica*, Giuffrè, Milano, 2017.

BONGER W.A., *Criminality and economic conditions*, Little Brown, Michigan,1916.

BORSARI R. SAMMICHELI L. (a cura di) Homo oeconomicus*: neuroscienze, razionalità decisionale ed elemento soggettivo nei reati economici,* Padova, Padova University Press, 2015.

BOUCHER P., NASCIMENTO S., KRITIKOS M., *Come La Tecnologia Blockchain Può Cambiarci La Vita, Analisi Approfondita*, in https://op.europa.eu.

BURLONE P.L., DE CARIA R., *Bitcoin e le altre criptomonete. Inquadramento giuridico e fiscale*, in *IBL Focus*, in www.brunoleoni.it.

CALZOLAIO E., *Il Bitcoin come oggetto di* property. *Note a margine di una recente sentenza della* High Court, in *Foro Italiano*, Il Foro Italiano Editore, 2020.

CALZOLAIO E., *La qualificazione del* bitcoin: *appunti di comparazione giuridica*, in *Danno e responsabilità*, Ipsoa, Milano, 2021.

CAMPOBASSO G.F., *Bancogiro e moneta scritturale,* Cacucci Editore, Bari, 1979.

CANTIMORI D., voce *"Utilitarismo"*, in *Enciclopedia Italiana*, Istituto della Enciclopedia Italiana Treccani, 1937, in www.treccani.it.

CANTONE R. *Abusivismo finanziario: esperienze da un'indagine giudiziaria*, in *Cassazione Penale,* Giuffrè, Milano, 1996.

CAPACCIOLI S., *Criptovalute e Bitcoin: un'analisi giuridica,* Giuffrè, Milano, 2015.

CAPOGNA A., ET AL., *Bitcoin: profili giuridici e comparatistici. Analisi e sviluppi futuri di un fenomeno in evoluzione.,* in *Diritto mercato tecnologia,* 2015, in www.dimit.it,

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, Fascicolo I, Sezione I, pp.134-135, in www.dirittobancario.it.

CASSESE S, *Exploring the legitimacy of Nudging,* in AA.VV. (a cura di), *Choice Architecture in Democracies – Exploring the legitimacy of Nudging*, Nomos, Baden- Baden, 2016

CASTALDO A.R., *Accesso all'attività bancaria e strategie penalistiche di controllo,* in Rivista Italiana di Diritto e Procedura Penale, Giuffrè, Milano, 1996.

CASTALDO A.R., *Anti-Money Laundering Strategies and The Metaverse: New Dangers and opportunities,* in *Iura&Legal Systems*, IX, 2022.

CHAINALYSIS TEAM, *Crypto Mixers and AML Compliance*, 2022, in www.chainalysis.com.

CHAINALYSIS TEAM, *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, aprile 2022, in www.chainalysis.com.

CHAINALYSIS TEAM, *U.S. Sanctions crypto mixer Sinbad.io for Role in North Korean Laundering Activities,* 2023, in www.chainalysis.com.

CHAINALYSIS TEAM, *Russian and North Korean Cyberattack Infrastructure Converge: New Hacking Data Raises National Security Concerns*, 2023, in www.chainalysis.com.

CHAUM C., ET. AL., *Advances in Cryptology Proceedings of Crypto 82,* Springer US, University of California, Santa Barbara, 1983.

CHIERICHIELLO G., *Il "criminale razionale", ovvero la teoria microeconomica del crimine. Un saggio introduttivo*, in *Archivio penale,* 2018, in www.archiviopenale.it.

CICLOSI F., GASPARI P., *Bitcoin. Genesi e funzionamento di una criptovaluta*, Edizioni Simple, Macerata, 2017.

CITI, *Life, the Metaverse and Everything*, 2022, in www.citigroup.com

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*, Milano, Ipsoa, 2016.

CONSULICH F., *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali, in Diritto Penale e Processo,* Milano, Ipsoa, 2022.

CONTI L., *Profili penalistici del testo unico sull'intermediazione finanziaria*, *in Diritto Penale e Processo,* Ipsoa, 1998.

CORASANITI G., *Il trattamento tributario tra obblighi antiriciclaggio e trattamento fiscale,* in *Strumenti finanziari e fiscalità*, Egea, Milano, 2018.

COSTI R. D'AGOSTINO P., *Trattato di diritto penale dell'impresa. Volume III, I Reati bancari*, Cedam, Padova, 1992.

CROALL H., *Understanding white collar crime,* Open University Press, Buckingham-Philadelphia, 2001.

DALAITI F., *Cripto-valute e abusivismo finanziario: cripto analogia o interpretazione estensiva?*, in *Sistema Penale,* 2021*,* in www.sistemapenale.it.

D'AURIA S., *Riciclaggio e terrorismo*, in *GNOSIS - Rivista italiana di Intelligence*, 2013, in www.gnosis.aisi.gov.it.

DELOITTE, *Market Manipulation in Digital Assets,* 2021, in www.deloitte.com.

DELOITTE, *Market Integrity Consideration for Digital Asset*, 2021, in www.deloitte.com.

DE LUCA R.S., MACRÌ B., ZOLI B., *Anatomia del Crimine in Italia*, Giuffrè, Milano, 2013.

DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti. Lo statuto delle valute virtuali: le discipline e i controlli*, in *Archivio Diritto penale contemporaneo*, 2018 in https://archiviodpc.dirittopenaleuomo.org.

DI VIZIO F., *Moderni abusivismi e criptovalute. Tra il mito della completa disintermediazione e la realtà di nuovi intermediari,* in *Discrimen,* 2022, in www.discrimen.it.

DOLCINI E., MARINUCCI G., GATTA G.L., *Art. 648 bis*, Riciclaggio, in *Codice Penale Commentato,* Wolters Kluwer, 2015.

ELLIPTIC, *US sanctions Garantex exchange and Hydra dark web marketplace following seizure of Hydra by German authorities*, 2022, in www.elliptic.co.

ELLIPTIC, *The Future of Financial Crime in the Metaverse. Fighting Crypto-crime in Web 3.0*, 2022, in www.elliptic.com.

EPIDENDIO T.E., *La confisca nel diritto penale e nel sistema delle responsabilità degli enti,* Cedam, Padova, 2011.

EUROPOL INNOVATION LAB, *Policing in the metaverse: what law enforcement needs to know*, 2022, in www.europol.europa.eu.

FANTACCI L., GOBBI L., LUCIANI D., *Bene pubblico globale o arma finanziaria? L'egemonia del dollaro alla prova delle sanzioni*, in *Moneta e Credito*, 2022, in www.rivistaweb.it.

FANTOZZI A., *Imprenditore e imprese nelle imposte sui redditi e nell'IVA*, Giuffrè, Milano, 1982.

FANTOZZI A., voce *Imprenditore e impresa nelle imposte sui redditi e nell'IVA,* in *Enc. Giur.,* vol. XVI, Roma, 1989.

FASSÒ F., *IL regime fiscale dei* bitcoins *secondo una recente (e unica) prassi amministrativa. Un passo avanti e un'occasione mancata* in *Strumenti finanziari e fiscalità*, Egea, Milano, 2017.

FONDAROLI D., *Le ipotesi speciali di confisca nel sistema penale. Ablazione patrimoniale, criminalità economica, responsabilità delle persone fisiche e giuridiche*, Bononia University Press, Bologna, 2007.

FONDAROLI D., *Splendori e miserie della confisca obbligatoria del profitto*, in D. FONDAROLI (a cura di), *Principi costituzionali in materia penale e fonti sovranazionali*, Cedam, Padova, 2008.

FONDAROLI D., Homo oeconomicus. *La responsabilità in attività d'impresa tra condizionamenti comportamentali e "spinta gentile"*, in C. PIERGALLINI, G.

MANNOZZI, C. SOTIS, C. PERINI, M. SCOLETTA, F. CONSULICH (a cura di), *Studi in onore di Carlo Enrico Paliero,* Milano, 2022.

FONDAROLI D., *Metafore:* l'homo oeconomicus *e la "spinta gentile" nella prospettiva del sistema punitivo*, in *Criminalia. Annuario di scienze penalistiche*, 2022, in www.discrimen.it.

FORTI G., *L'immane concretezza. Metamorfosi del crimine e controllo penale*, Raffaele Cortina Editore, 2000.

FOTI L., *Capire Blockchain*.

FUMO M. *La condotta nei reati informatici,* in *Archivio penale*, 3, 2013, in www.archiviopenale.it.

GALMARINI S., SABA C., *IV Direttiva Antiriciclaggio e approccio basato sul rischio,* 2018, in www.dirittobancario.it.

GARAVAGLIA R., *Tutto su Blockchain. Capire la tecnologia e le nuove opportunità*, Hoepli, Milano, 2018.

GARGIUOLI F., *Cybercrime*, Aracne Editrice, Roma, 2017.

GASPARRI G., *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema*, in *Diritto dell'Informazione e dell'informatica*, Giuffré, Milano, 3, 2015.

GENTILE M., SCALESE F., CAIVANO V., DI ROCCO S., *Principali tendenze in tema di investimenti sostenibili e criptoattività,* in www.consob.it.

GIRINO E., *Criptovalute: un problema di legalità funzionale*, in *Rivista di Diritto Bancario*, 2018, in www.dirittobancario.it.

GIUNTA F., MICHELETTI D. (a cura di), *La disciplina penale del risparmio*, Giuffrè, Milano, 2008.

GRAGNANI A., Nudging *e libertà costituzionale,* 2021, in www.dirittifondamentali.it.

GRASSO G., *sub* Art. 240, in M. ROMANO M., G. GRASSO., T. PADOVANI (a cura di), *Commentario sistematico del codice penale*, Giuffrè, Milano, 2011.

GRAZIANI F., *Bitcoin, tutti i numeri dell'ascesa*, 2018, in www.masterx.iulm.it.

GREEN SP., *Lying, Cheating and Stealing. A moral theory of White-Collar Crime*, Oxford, Oxford University Press, 2006.

GREENNBERG A., *Il più longevo mercato nero nella storia del* dark web *è stato smantellato*, 2023, in ww.wired.it.

HABER E., *The Criminal Metaverse,* in *Indiana Law Journal*, forthcoming 2024, inn www.papers.ssrnn.com.

HUGES E., *A Cypherpunk's Manifesto,* 1993, in www.activism.net.

IANSITI M., LAKHANI K.R., *The Truth About Blockchain*, in *Harvard Business Review,* 2017, in www.hbr.org.

INZITARI B., *Le obbligazioni nel diritto civile degli affari*, Cedam, Padova, 2006.

KAPLANOV N.V., *Nerd Money: Bitcoin, The Private Digital Currency, And The Case Against Its Regulation,* Loyola Consumer Law Review, vol. 25, 2012.

KESSLER S., BETZ B., *Crypto Bridge Nomad Drained of Early $200M in exploit*, 2022, in www.coindesk.com.

KNAPP G.F. in *Staatliche Theorie des Geldes*, Leipzig, Duncker & Humblot, University of California, 1905.

LA ROCCA L., *La prevenzione del riciclaggio e finanziamento del terrorismo nelle nuove forme di pagamento. Focus sulle valute virtuali,* in *Analisi Giuridica dell'Economia*, Il Mulino- Riviste*web*, 2015, in www.rivisteweb.it.

LECIS N., *La teoria austriaca del ciclo economico*, 2018, in www.financecue.it.

LEDGER ACADEMY, *Light Node Meaning*, in www.ledger.com.

LEMME G., *Moneta scritturale e moneta elettronica*, Giappichelli, Torino 2003.

LUCEV R, BONCOMPAGNI F., *Criptovalute e profili di rischio penale nelle attività degli exchanger*, in *Giurisprudenza Penale Web*, 2018, in www.giurisprudenzapenale.it.

LONGOBARDO C., *Delitti di perpetuazione di una situazione antigiuridica*, in S. FIORE (a cura di), *I reati contro il patrimonio*, UTET, Torino, 2010.

MAGLIOCCO A., *Bitcoin e tassazione,* in *Strumenti finanziari e fiscalità,* Egea, Milano, 2016.

MAJORANA D., *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in *Corriere Tributario*, Ipsoa, Milano, 2018.

MANCINI N., *Bitcoin: rischi e difficoltà normative*, in *Banca Impresa Società*, Il Mulino – Riviste *Web*, 2016, in www.rivisteweb.it.

MANNOZZI G., *Il crimine dei colletti bianchi: profili definitori e strategie di contrasto attraverso i metodi della giustizia riparativa* in AA.VV., *Europe in crisis: crime, criminal justice, and the way forward. Essays in honour of Nestor Courakis*, C.D. SPINELLIS, N. THEODORAKIS, E. BILLIS, G. PAPADIMITRAKOPOULOS, 2017, pp. 1365-1394, in www.crime-in-crisis.com.

MANTOVANI F., *Diritto penale*. Parte generale, X Edizione, Cedam, 2019.

MARTUCCI P., *La criminalità economica. Una guida per capire*, Laterza, Bari, 2006.

MAUGERI A.M., *Le moderne sanzioni patrimoniali tra funzionalità e garantismo*, Giuffrè, Milano, 2001.

MAUGERI M., *Cripto-attività e abusi di mercato*, in *Osservatorio del diritto civile e commerciale*, Il Mulino – Riviste *Web*, 2022, www.rivisteweb.it.

MAZZACUVA F., *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico*, Giappichelli, Torino, 2017.

MAZZOCCHI S., *Esenti da IVA le operazioni di cambio nella valuta virtuale "bitcoin"*, 2015, in www.iltributario.it.

MENDITTO F., *Le confische di prevenzione e penali,* Giuffrè, Milano, 2015.

MEZZETTI E., *Reati contro il patrimonio*, Giuffrè, Milano, 2013.

MONTANI E., *Economic Crimes. Diritto penale ed economia: prove di dialogo*, in *Rivista Trimestrale di Diritto Penale dell'Economia*, 2005.

MONTANI E., *La Babele dell'EAL e il diritto penale*, in *Rivista Trimestrale di Diritto Penale dell'Economia*, 2007.

MONTANI E., *La tutela del corretto svolgimento dell'attività di intermediazione e bancaria*, in A. ALESSANDRI (a cura di), *Reati in materia economica*, Giappichelli, Torino, 2017.

MONTESQUIEU C., *De l'Esprit des lois*, trad. it., *Lo spirito delle leggi*, edizione a cura di R. Derathé e B. Boffito Serra, 2004.

NADDEO M., *Criptovalute e diritto penale*, in AA.VV., *Criptovalute. Profili storico-economici e giuridici*, a cura di M. LORENZINI, M. ZULBERTI, C. IMBROSCIANO, Giappichelli, Torino, 2023.

NAKAMOTO S., *Bitcoin: A Peer-to- Peer Electronic Cash System*, in www.bitcoin.org.

NAZZARI M., *From payday to payoff: Exploring the money laundering strategies of cybercriminals, Trends in Organized Crime,* in *Trends in Organized Crime,* Springer, 2023, in www.link.springer.com.

NICOSIA E., *La confisca, le confische. Funzioni politico-criminali, natura giuridica e problemi ricostruttivo-applicativi*, Giappichelli, Torino, 2012.

OFAC, *Press Releases. Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex*, 2022, in www.home.treasury.gov.

ORNARI L., *Criminalità del profitto e tecniche sanzionatorie. Confisca e sanzioni pecuniarie nel diritto penale "moderno*", Cedam, Padova, 1997.

PAGLIARI E., 4 *agenzie investigano sull'*exchange QuadrigaCX, in *The Cryptonomist*, 2019, in www.cryptonomist.ch.

PALIERO C.E., *Minima non curat praetor. Ipertrofia del diritto penale e decriminalizzazione dei reati bagatellari*, Cedam, Padova, 1985.

PALIERO C.E., *L'economia della pena (un work in progress),* in *Rivista italiana di diritto e procedura penale*, 2005.

PALIERO C.E., *Principio di colpevolezza e reati economici*, in R. BORSARI, L. SAMMICHELI, C. SARRA (a cura di) Homo oeconomicus*: neuroscienze, razionalità decisionale ed elemento soggettivo nei reati economici,* Padova, Padova University Press, 2015.

PALUMBO G., *Il trattamento tributario dei bitcoin*, in *Diritto e Pratica Tributaria*, Cedam, Padova, *Il trattamento tributario dei bitcoin*, in *Diritto e Pratica Tributaria*, 2016.

PICOTTI L., *Diritto penale, tecnologie informatiche ed intelligenza artificiale, una visione di insieme*, in AA.VV. (a cura di) *Cybercrime,* II Edizione, Utet, Torino, 2023.

PIERRO M., *La qualificazione giuridica e il trattamento fiscale delle criptovalute*, in *Rivista di Diritto Tributario*, Pacini Giuridica, Pisa, 2020.

PIERRO M., *Contributo all'individuazione della nozione di* crypto asset *e suoi riflessi nell'ordinamento tributario nazionale,* in *Rassegna Tributaria,* 2022, in www. rassegnatributaria.ilsole24ore.com.

PLANTE. E., *$30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit*, in www.chainalysis.com.

PORTA M., *ATM Bitcoin e negozi affiliati: dove sono e come funzionano,* giugno 2019, in www.cryptonomist.ch.

PwC, *Navigating the global crypto landscape*, 2023, in www.pwc.it.

PUGLIATTI S., voce *Cosa in senso giuridico* (teoria generale), in AA.VV., *Enc. dir.,* Milano, Giuffrè, vol. XII, 1962.

REDDY E, MINNAR A., *Cryptocurrency: a tool and target for cybercrime*, in *Acta criminologica: Southern African journal of criminology*, in Sabinet African Journal of Criminology, 2018, in www.journals.co.za.

REINSCH W.A., PALAZZI A.L., *Cryptocurrencies and U.S. Sanction Evasion: implications for Russia*, in *Center for Strategic and International Studies*, 2022, in www.csis.org.

RESCIGNO P. (diretto da), *Trattato di diritto privato,* Utet Giuridica, Torino, 1999.

RIVERDITI M., COSSAVELLA G., *Criprovalute e NFT. Gli aspetti penali*, in *Diritto ed economia dell'impresa*, Giappichelli, 2022, in www.dirittoeconomiaimpresa.it.

ROSATO A., *Profili penali delle criptovalute*, Pacini Giuridica, Pisa, 2021.

ROTONDO G., CORAGGIO E., *Monete virtuali: tassonomia e inquadramento giuridico*, in *Innovazione Diritto*, 2022, in www.innovazionediritto.it.

RUGA RIVA C., *L'abusivismo finanziario: questioni giurisprudenziali e profili di illegittimità costituzionale*, in *Rivista trimestrale di Diritto penale dell'economia,* Cedam, Padova, 2001.

SABBATINI G., *I Cypherpunks da David Chaum a Satoshi Nakamoto*, 2017, in www.nextgenerationcurrency.com.

STURZO L., *Bitcoin e riciclaggio 2.0.*, in *Archivio Diritto penale contemporaneo,* 2018, in www.archiviodpc.dirittopenaleuomo.org.

SZABO N., *Money, blockchains, and social scalability*, in https://unenumerated.blogspot.com.

SALVINI O., *Il contrasto all'abuso del sistema finanziario per scopi di riciclaggio e finanziamento del terrorismo: la IV Direttiva (EU) 2015/849, tra coordinamento e cooperazione*, in *Rivista Italiana di Diritto Pubblico Comunitario*, Giuffrè, Milano, 2016.

SANDEI C., *Le* Initial Coin Offering *nel prisma dell'ordinamento finanziario*, in *Rivista di Diritto Civile,* Cedam, Padova, 2020.

SAVONA E.U., *Economia e criminalità*" in *Enciclopedia delle Scienze Sociali, Istituto della Enciclopedia Italiana Treccani,* Roma*,* 2001.

SCALCIONE, R., *Gli interventi delle autorità di vigilanza in materia di schemi di valute virtuali,* in *Analisi Giuridica dell'Economia*, Il Mulino, 1, 2015, in www.rivisteweb.it.

SCALIA R., *Riflessioni su alcuni temi controversi sulla disciplina IVA delle c.d. criptovalute*, in *Giurisprudenza delle imposte*, 2020, in www.assonime.it.

SEMINARA S., *Diritto penale commerciale, Volume III. Il diritto penale del mercato mobiliare*, Giappichelli, Torino, 2018.

SHAPIRO S.P., *Collaring the Crime, not the Criminal: Reconsidering the Concept of White-Collar Crime*, in *American Sociological Review,* Vol. 55, n. 3, 1990, in www.jstor.org.

SICIGNANO G.J., *Bitcoin e riciclaggio*, Giappichelli, Torino, 2019.

SORBELLO P., *L'abusivismo finanziario tra atto giuridicamente lecito e fatto penalmente rilevante*, in *Giurisprudenza di merito*, Pacini Giuridica, Pisa, 2009.

SUTHERLAND E.H., *Principles of Criminology*, Philadelphia, 1947.

THALER R., SUSTEIN C., *Libertarian paternalism is not an oxymoron*, in *The University of Chicago Review,* vol. 70, n. 4, 2003.

THALER R., SUSTEIN C., Nudge. *La spinta gentile. La nuova strategia per migliorare le nostre decisioni sul lavoro, salute, felicità*, trad. it., Milano, 2009.

TRAUTMAN L.J., *Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?*, in *Richmond Journal of Law and Technology,* 2014, revised 2017, in www.jolt.richmond.edu.

TUMBIOLO F., *Profili fiscali della formazione del consenso all'interno della* blockchain, in AA.VV., *Criptovalute. Profili storico-economiici e giuridici*, a cura di M. LORENZINI, M. ZULBERTI, C. IMBROSCIANO, Giappichelli, Torino, 2023.

TUZET G., Nudge: *la struttura normativa*, in *Gior.it. psicologia,* 2, 2020.

UK JURISDICTION TASKFORCE, *Legal statement on criptoasset and smart contracts*, novembre 2019, in www.blockchain4europe.eu.

VARDI N., *Criptovalute e dintorni: alcune considerazioni sulla natura giuridica del Bitcoin*, in *Diritto dell'Informazione e dell'Informatica,* in *Diritto dell'Informazione e dell'informatica*, Giuffré, Milano, 3, 2015.

VERGINE F., *Confisca e sequestro per equivalente,* Ipsoa, Milano, 2009.

VERSTEIN A., *Crypto Asset and Insider Trading Law's Domain*, in *Iowa Law Review*, 2019, in www.iuowa.edu.

VIGORITA R. – ILACQUA F., "*Profili giuridici del Bitcoin: la moneta diventa digitale*", in www.iurisprudentes.it.

WEBER M., *Economia e Società*, Edizione di Comunità, 1968.

XU J., LIVSHITS G., *The Anatomy of a Cryptocurrency Pump-and-Dump Schem*, 2019, in in www.researchgate.net.

ZANNOTTI R., *La tutela penale del mercato finanziario*, Giappichelli, Torino, 1997.

ZANNOTTI R., *La tutela dell'accesso al mercato nella prospettiva della lotta contro il riciclaggio: il caso dell'abusivismo,* in *Rivista della Guardia di Finanza*, 1, 2004,

ZANNOTTI R., *Il nuovo diritto penale dell'economia*, Giuffrè, Milano, 2008.

ZENO-ZENCOVICH, voce "Cosa" in *Dig. Disc. Priv. Sez. Civ.*, UTET, Torino, 1989.

GIURISPRUDENZA CONSULTATA

CGUE, sentenza Skattevrket vs Hedqvist, causa C-264/2015, 22 ottobre 2015.

Corte cost., sentenza n. 332 del 24 luglio 2007.

Cass. pen., Sez, VI, sent. n. 973/1996.

Cass. pen., Sez. VI, sent. n. 737/1999.

Cass. pen., Sez. IV, sent. n. 6350/2007.

Cass. pen., Sez. II, sent. n. 15092/2007.

Cass. pen., Sez. VI, sent. n. 16980/2007.

Cass. pen., Sez. II, sent. n. 47394/2008.

Cass. pen., Sez. VI, sent. n. 8755/2009.

Cass. pen., Sez. II, sent. n. 9891/2011.

Cass. pen., Sez. V., sent. n. 9848/2013.

Cass. pen., Sez. II, sent. n. 1435/2013.

Cass. pen., Sez. II, sent. N. 25940/2013.

Cass. pen., Sez. V, sent. n. 10265/2014.

Cass. pen., Sez. II, sent. n. 10746/2014.

Cass. pen., Sez. II, sent. n. 41740/2015.

Cass. pen., Sez. II, sent. n. 11453/2016.

Cass. pen., Sez. II, sent. n. 56391/2017.

Cass. pen., Sez. II, sent. n. 19480/2019.

Cass. pen., Sez. II, sent. n. 17322/2019.

Cass. pen., Sez. II, sent. n. 39702/2019

Cass. pen., Sez. II, sent. n. 11959/2020.

Cass. pen., Sez. V, sent. n. 17360/2020

Cass. pen., Sez. II, sent. n. 32894/2020.

Cass. pen., Sez. V, sent. n. 36864/2020.

Cass. pen., Sez. III, sent. n. 16686/2021.

Cass. pen. Sez. II, sent. n. 26796/2021.

Cass. pen., Sez. II, sent. n. 46209/2023.

Trib. Brescia, Sez. Spec. in materia di impresa, decreto n. 7556/2018.

Trib. Firenze, Sez. Fallimentare, sent.18/2019.

AVVISI, PARERI E RACCOMANDAZIONI AUTORITÀ NAZIONALI ED EUROPEE IN MATERIA DI CRIPTOVALUTE

AGENZIA DELLE ENTRATE, risposta a interpello 508/2022, in www.agenziaentrate.it.

BANCA D' ITALIA, *Comunicazione del 30 gennaio 2015 - Valute Virtuali,* 2015, in www.bancaditalia.it.

BANCA D'ITALIA, *Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*, giugno 2022, in www.bancaditalia.it.

BCE, *Virtual Currency Schemes*, Ottobre 2012, p. 5, www.ecb.europa.eu.

BCE, Parere del 12 ottobre 2016 (C-459/3), in www.eur-lex.europa.eu.

BECHINI U. CIGNARELLA M.C., *Consiglio Nazionale del Notariato, Quesito Antiriciclaggio – Compravendita di Immobile – Pagamento del prezzo in Bitcoin*, vertente sulla richiesta in ordine alla legittimità del pagamento del prezzo della vendita di un bene immobile in criptovaluta

EBA, *Avvertenze per i consumatori sulle monete virtuali,* ABE/WRG/2013/01, 12 dicembre 2013, in www.eba.europa.eu.

CNEL, *Moneta Elettronica. Osservazioni e Proposte,* 2014, in www.camera.it.

CONSOB, *Le offerte iniziali e gli scambi di cripto-attività*, 19 marzo 2019, in www.consob.it.

CONSOB, *Le offerte iniziali e gli scambi di cripto-attività. Rapporto finale*, 2 gennaio 2020, in www.consob.it.

EBA, *Avvertenza per i consumatori sulle monete virtuali*, 12 dicembre 2013, in www.eba.europa.eu.

EBA, *EBA Opinion on virtual currencies*, ABE/OP/2014/08, 4 luglio 2014, in www.eba.europa.eu.

EBA, *Report with advice for the European Commission,* 9 Gennaio 2019, in www.eba.europa.eu.

ESMA, *Advice to ESMA – Own Initiative Report on Initial Coin Offerings and Crypto-Assets (ESMA22-106-1338)* in www.esma.europa.eu.

FATF, *Recommandations update 2012-2023* (update November 2023), in www.fatf-gafi.org.
VALUE ADDED TAX COMMITEE, *Working paper n. 892, Issues arising from recent judjments of the court of Justice of the European Union*, 2016, inwww.circabc.europa.eu

REPORT

CHAINALYSIS, *The 2023 Crypto crime Report,* in www.chainalysis.com.
CHAINALYSIS, *The 2024 Crypto crime Report,* in www.chainalysis.com.