CRIPTOVALUTE: PROFILI DI RILEVANZA PENALE

Marco Naddeo

Sommario: 1. Il diritto penale nell'era degli 'invisibili': *Blockchain* e *cryptocurrencies*. 2. Criptovalute e dogmatica delle categorie nel diritto penale del sospetto. – 3. Utilizzo illecito delle criptovalute. – 4. Prevenzione e repressione del riciclaggio mediante criptovalute. – 4.1. Criptoattività e autoriciclaggio: il *cyber self-laundering*. – 5. '231' e criptovalute: la responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali.

1. *Il diritto penale nell'era degli 'invisibili': Blockchain e cryptocurrencies.*

La proporzione diretta tra sviluppo tecnologico e *crimine economico* riflette un'ulteriore, significativa

relazione tra grandezze che assumono valori il cui rapporto è costante: «*più complessa diventa la società nelle sue articolazioni, più complessa tende a diventare la criminalità che ne riproduce le patologie*»[1]. Si tratta di un legame in grado di spiegare la professionalizzazione e organizzazione della criminalità economica attuale, impegnata nella massimizzazione delle opportunità (profitto), minimizzando i rischi da *law enforcement* (identificazione, arresto, confisca)[2].

Dal punto di vista penalistico è quindi utile accennare a due fenomeni la cui interpolazione genera effetti di rilevanza significativa. Ci si riferisce alla tecnofinanza o *Fintech* – vale a dire al profondo connubio tra tecnologie e nuovi modelli di *business*, che caratterizza l'innovazione finanziaria a disposizione dei nuovi operatori del mercato – e alla finanziarizzazione della ricchezza, che ha profondamente segnato il mondo bancario e l'economia in genere, aprendo nuovi orizzonti anche all'investimento delle famiglie e dei risparmiatori non professionali. Un binomio in grado di generare la "ipertrofia delle opportunità"[3] abilmente sfruttata da organizzazioni criminali proteiformi che orientano i loro comportamenti in base a *scelte razionali*, perseguendo con chiarezza e coerenza l'obiettivo del massimo profitto[4].

In tale contesto «*il mercato finanziario, altamente sensibile allo sviluppo tecnologico e all'informatizzazione, diviene il palcoscenico virtuale (dematerializzazione) calcato da nuovi attori-protagonisti (disintermediazione bancaria)*»[5], che possono contare sulla fluidità della globalizzazione e sulle infinite potenzialità dei sistemi informatici e telematici. È questo l'*humus* che favorisce lo sviluppo della *Blockchain* quale tecnologia alla base del funzionamento delle criptovalute (*Bitcoin, Monero, Ethereum, Stellar, Ripple* e *altcoins* in genere). Lo strumento crittografico della "catena di blocchi" garantisce l'autenticità e l'integrità della transazione, preservando l'identità del mittente che nella visione criminale può avvantaggiarsi di uno pseudo-anonimato[6] in grado di condurre alla spersonalizzazione del binomio operazione finanziaria-soggetto economico. Piegata a fini illeciti, infatti, la crittografia asimmetrica attraverso la quale scorrono i flussi di criptovaluta porta alle estreme conseguenze la de-individualizzazione della criminalità economica, sfocando la linearità dell'*iter criminis* (informazione, ideazione, esecuzione e perfezionamento) già difficilmente decodificabile per la complessità delle moderne operazioni di ingegneria finanziaria. È la nota questione della scarsa percezione sociale dei *white collar crimes* che si oggettivizza.

I nodi della *Blockchain* compromettono la struttura classica dell'azione penalisticamente intesa, costringendo il diritto criminale a fare i conti con gli "invisibili", perché a questo punto, «non solo gli oggetti del reato, ma anche i soggetti del reato sono divenuti invisibili», sicché «(...) neanche il reato, l'azione chiaramente

criminale, è più visibile quale atto manifesto. Il diritto penale non tratta più dell'autore che entra in un conflitto personale con la vittima o con la società. Il diritto penale deve reagire a processi disfunzionali»[7].

2. *Criptovalute e dogmatica di categorie nel diritto penale del sospetto.*

Non è revocabile in dubbio che l'intrinseca *opacità* che le caratterizza faccia delle criptovalute un potenziale strumento per chi abbia interesse a riciclare proventi di origine illecita riducendo i rischi di tracciabilità e conseguente identificazione del soggetto agente. D'altra parte, le *cryptocurrencies* sono il naturale sbocco del *cybercrime* e possono costituire lo strumento di elezione per gli acquisti nei mercati illegali del *darkweb* o per altri usi illeciti.

Procediamo per gradi.

Il proliferare delle criptovalute e la diffusione generalizzata di questo strumento tra i consociati le rende, al contempo: *i)* bersaglio di condotte predatorie, *ii)* 'moneta' di scambio, *iii)* strumento di realizzazione dell'illecito. Insomma, i *crypto-assets* possono essere variamente inquadrabili nella struttura prismatica del fatto tipizzato: da *oggetto materiale* della condotta illecita a *prezzo*, *prodotto* o *profitto* del reato, finanche a forma di manifestazione ovvero nota modale di perpetuazione dell'illecito penale. Da questo punto di vista, possono registrarsi due livelli di operatività delle criptovalute: il primo è quello in cui la criptovaluta assume le sembianze di mezzo alternativo alla moneta tradizionale; essa può manifestarsi come il valore trasferito in pagamento per l'acquisto di materiale illecito nel mercato reale o virtuale ovvero può costituire tanto il *target* delle condotte illecite (attacchi a piattaforme di *Exchange* o *Wallet Provider*) quanto il risultato da esse ottenuto sotto forma di prodotto di schemi estorsivi *cyber* (come nel caso di *ransomware*) o *non-cyber* (es. ricatti sessuali). Il secondo livello eleva la criptovaluta a tratto caratterizzante della fattispecie criminosa, richiamando alla mente il suo utilizzo in ambito *malware* (es. *clipboard malware*, *mining botnet*) e il *cyberlaundering* che, sfruttando l'anonimato delle transazioni e la natura ubiqua delle monete virtuali, rappresenta il rischio più elevato della *peer to peer e-money* (così S. Nakamoto ha definito il *Bitcoin*)[8].

A confermarlo, il *report* dell'*Internet Cybercrime Centre* (EC3) di Europol[9] che rivela il rapporto di proporzione diretta tra la capitalizzazione del mercato delle criptovalute e lo sviluppo del *cybercrime*, che si riflette di conseguenza sul riciclaggio digitale c.d. integrale. In tale contesto, il crimine può avvalersi dei servizi di *mixing* (noti anche come *cryptocurrency tumbler*) e sfruttare sofisticate tecniche di trasferimento della valuta virtuale

che, utilizzando conti di rimbalzo (conti *bounce*) o collettori (conti *pool* o *pot*) in combinazione con la tecnologia *Blockchain* rendono quasi impossibile la ricostruzione dei passaggi intermedi [tra fase di ingresso (*gateway*) e uscita (*withdrawing*)], garantendone l'anonimato[10]. In queste circostanze, la curvatura criminosa delle proprietà della criptovaluta le consentono di interpretare a pieno la nota decettiva della fattispecie a forma vincolata, esprimendo esattamente il nucleo di offensività proprio del «riciclaggio».

Sul piano tecnico, può ricavarsene un dato non trascurabile: le criptovalute rivelano la natura di attività «*"a* doppio uso*": vale a dire non* di per sé *illecite, ma che* possono *essere e sono per lo più utilizzate per scopi illeciti, sistematicamente ed efficacemente, non solo occasionalmente*»[11].

La bidimensionalità che consente di declinare lo strumento in questione secondo il paradigma lecito-illecito è la ragione che dovrebbe contenere il dilagare delle logiche del *sospetto* e l'affermarsi di un diritto penale rivolto al *rischio*, anziché al *fatto*[12]. In tal senso, una funzione fondamentale è quella svolta dalle categorie del diritto penale classico (pericolo e causalità, *in primis*)[13], in grado di ristabilire la proiezione della condotta (da cui la legge fa dipendere l'esistenza del delitto) in termini offensivi. Anziché cedere agli automatismi della presunzione, per dirsi penalmente rilevante l'impiego di criptovalute deve puntare a un risultato dannoso o pericoloso, impedendosi in questo modo lo slittamento epistemologico dalla prevenzione alla precauzione che può condurre a una dogmatica del rischio (nomologicamente) incerto.

Qualche dubbio è generato dall'indice di sospetto che il sistema sembra implicitamente attribuire all'utilizzo della criptovaluta. Depongono in tal senso gli *schemi di comportamenti anomali* e gli obblighi di comunicazione della propria operatività al Ministero dell'Economia e delle Finanze, gravanti sui prestatori di servizi relativi all'utilizzo di valuta virtuale ai fini dell'efficiente popolamento della sezione speciale di cui al comma 8-*bis* dell'art. 17-*bis*, D. Lgs. 141/2010. Insomma, la *cryptocurrency* sembra di per sé giustificativa dei "*ragionevoli motivi per sospettare*" e, dunque, il suo impiego potrebbe indurre gli obbligati a spiccare una s.o.s. (segnalazione di operazione sospetta) ogni qualvolta ne riscontrino l'utilizzo nelle operazioni oggetto di adeguata verifica (se non altro agendo in funzione 'difensiva' per sterilizzare i rischi sanzionatori derivanti dall'inosservanza delle relative disposizioni). A confermarlo è la stessa analisi qualitativa delle segnalazioni, come rappresentata dal Direttore della UIF nel corso della *Presentazione del rapporto annuale dell'Unità di Informazione Finanziaria per l'Italia*[14].

Al contrario, il principio di offensività può segnare la misura oltre la quale non è possibile espandere il diritto

penale del rischio[15], espungendo da tale perimetro le opzioni normative fondate sulla precauzione, che «non sembrano comunque riconducibili alla consueta tecnica di normazione del pericolo astratto o presunto, la cui struttura teleologica rimanda pur sempre alla disponibilità di leggi scientifiche o regole di esperienza "corroborate"»[16].

3. *Utilizzo illecito delle criptovalute.*

È innegabile che l'informatizzazione di gran parte dei rapporti economici (e sociali) abbia elevato il concetto di *sicurezza informatica* a interesse primario pretendendo un proporzionale irrobustimento del presidio penalistico, chiamato a garantirne l'affidabilità anche mediante l'introduzione di nuove *modalità di lesione* che contemplino le attività criminali aventi ad oggetto gli strumenti di pagamento elettronici e virtuali[17]. Il livello di protezione è stato rafforzato e, grazie anche all'impulso del legislatore comunitario (da ultimo con la direttiva UE 2019/713)[18], oggi prevede l'incriminazione di condotte che vanno dall'indebito utilizzo e falsificazione della criptovaluta, all'acquisizione illecita e all'impiego della stessa (anche per finalità di riciclaggio), fino al trasferimento fraudolento, arrivando a punire la detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti *strumenti di pagamento diversi dai contanti*[19] ovvero l'abusivo esercizio dei "*prestatori di servizi relativi all'utilizzo di valuta virtuale*", cui sono ascrivibili anche le violazioni dei cc.dd. obblighi antiriciclaggio.

Insomma, un complesso reticolo sanzionatorio caratterizzato da una tutela multistrato, i cui livelli superficiali – più distanti dal nucleo valoriale da preservare – rivelano un'ispirazione 'preventiva' da condizionare all'effettivo pregiudizio dell'interesse tutelato (anche in termini di semplice messa in pericolo) per evitare il progressivo svuotamento dei contenuti dell'offesa e la temibile regressione al *funzionalismo penale*[20].

Agli illeciti immediatamente riconducibili alla criptovaluta deve poi aggiungersi la «*possibile connessione con fenomeni criminali caratterizzati dall'utilizzo di tecnologie informatiche quali* phishing *o* ransomware*, con truffe realizzate attraverso siti Internet o clonazione di carte di credito, ovvero al sospetto di reimpiego di fondi derivanti da attività commerciali non dichiarate, spesso svolte online. Rilevano, altresì, gli acquisti di* Virtual asset *con fondi che potrebbero derivare da frodi, distrazioni di fondi o schemi piramidali*»[21].

Naturalmente, gran parte di tali condotte risultano sussumibili già nella modellistica sanzionatoria dei reati

informatici previsti dagli artt. 615-*ter* (accesso abusivo ad un sistema informatico o telematico), 615-*quater* (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici), 617-*quinquies* (installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche) e 635-*bis* (danneggiamento di informazioni, dati e programmi informatici) del codice penale.

D'altra parte, le condotte dei cybercriminali spesso si risolvono in vicende di natura estorsiva (art. 629 c.p.), legate alla diffusione di *malware*, che consentono l'intrusione informatica e il sequestro di dati sbloccati a fronte di un riscatto in *bitcoin*[22]. Insomma, fenomenologie che attingono all'ampio armamentario penalistico costituito da una pletora di reati nell'ambito dei quali la criptovaluta non sempre è il *mezzo* di pagamento o la *modalità* mediante la quale viene posta in essere la condotta, ma spesso soltanto il *fine* per il quale viene commesso il reato (si pensi alle truffe perpetrate mediante gli schemi Ponzi), magari attraverso quelle che appaiono come vere e proprie ipotesi di sostituzione di persona (art. 494 c.p.)[23]. Molti di questi casi possono integrare la comune fattispecie di estorsione (art. 629 c.p.) in concorso con crimini informatici quali l'accesso abusivo a sistema informatico *ex* art. 615-*ter* c.p. (laddove l'*Hacker* abbia inoculato il *ransomware* nel computer della vittima) ovvero il danneggiamento di informazioni, dati e programmi informatici *ex* art. 635-*bis* c.p. (ove il virus inoculato sia per esempio un *cryptolocker* in grado di impedire il funzionamento del *software* attaccato). E, spesso, il coinvolgimento a titolo di concorso dell'*Exchanger* che ha venduto le criptovalute utilizzate per il pagamento del riscatto – cui l'Ufficio di Procura contesta la fattispecie realizzata dal *cyber estorsore* ai sensi dell'art. 110 c.p. – è erroneamente indotto dall'inserimento del sito dell'ignaro 'cambiavalute' nella schermata di *ransomware alert* che lo indica quale riferimento presso il quale è possibile acquistare le criptovalute[24].

Diversamente, le novità introdotte con il Decreto legislativo 8 novembre 2021, n. 184 incidono direttamente sugli strumenti di pagamento diversi dai contanti, punendone l'indebito utilizzo e la falsificazione (art. 493-*ter* c.p.) ovvero il trasferimento mediante frode informatica (art. 640-*ter* c.p.). Frequentemente attivata per la repressione delle condotte di *phishing*,la frode informatica è focalizzata sul funzionamento del sistema informatico o telematico, cui oggi fa da *pendant* la nuova fattispecie di *detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti* (art. 493-*quater* c.p.). Delitti che, se commessi *nell'interesse o a vantaggio dell'ente*, possono fondarne la responsabilità *ex* Decreto legislativo 8 giugno 2001, n. 231, in virtù del nuovo art. 25-*octies.1* che ne ha ampliato il catalogo dei reati-matrice.

In ogni caso, l'utilizzo illecito delle criptovalute resta prevalentemente agganciato al riciclaggio. I flussi di

segnalazione di operazioni sospette, infatti, evidenziano «*un'operatività finanziaria apparentemente connessa all'acquisto di* Bitcoin *da parte di soggetti indagati per i reati di traffico di stupefacenti, riciclaggio e auto-riciclaggio. L'operatività sui conti loro intestati si caratterizza da un lato per i frequenti e rilevanti versamenti e prelevamenti di contante non giustificati dalle attività da loro svolte e, dall'altro, per i numerosi bonifici da e verso società estere specializzate nella compravendita di criptovalute e conti correnti di cui sono titolari persone residenti all'estero coinvolte negli stessi procedimenti penali*»[25].

4. *Prevenzione e repressione del riciclaggio mediante criptovalute.*

Si è già detto della genetica predisposizione delle criptovalute all'anonimato e non può trascurarsene l'enorme potenziale scaturente dalla combinazione con le caratteristiche che rendono la rete luogo ideale per il compimento di attività criminali di ogni genere: "«delocalizzazione» *(il fatto illecito non è immediatamente individuato nell'ambito di un specifico* locus commissi delicti*);* «dematerializzazione» *(dovuta al contenuto digitale delle informazioni, dei servizi e del denaro che circola nella rete);* «dispersione» *(difficoltà di identificare l'autore dell'illecito ai fini dell'imputazione della relativa responsabilità penale)*"[26].

Per questa ragione, la incompleta panoramica delle forme di utilizzo illecito non può distrarre gli strumenti di *law enforcement* dalle nuove frontiere del riciclaggio mediante criptovalute. La estrema flessibilità della "valuta virtuale", infatti, favorisce la rapidità delle operazioni di trasferimento illecito di capitali, allargando gli orizzonti operativi e contenendone i costi, proprio in quell'ottica di massimizzazione del profitto costantemente perseguita dalla criminalità economica. In altri termini, sia che si tratti di *riciclaggio digitale strumentale* (in cui la rete subentra in maniera consistente nelle fasi di *layering* e di *integration*, vale a dire dopo che con la fase di *placement* il denaro di provenienza illecita ha subito un processo di finanziarizzazione) sia che si tratti *di riciclaggio digitale integrale* (dove la ripulitura è integralmente *online*, stante l'origine digitale del provento che ne è oggetto), le *cryptocurrencies* possono giocare un ruolo fondamentale nell'ostacolare l'identificazione della provenienza illecita della ricchezza oggetto di trasferimento[27].

Il paradosso per cui un registro distribuito e decentralizzato (*Distributed Ledger Technlology* o *DLT*), caratterizzato dalla trasparenza e dalla (tendenziale) immutabilità e irrepudiabilità, che sfrutta la crittografia asimmetrica per la protezione e l'autenticazione delle transazioni (attraverso chiavi pubbliche e private)[28], venga convertito in 'veicolo' di *Altcoins* e, quindi, piegato all'offuscamento (se non alla totale cancellazione)

del c.d. *paper trail*, disturbando la tracciabilità di denaro, beni o altre utilità di illecita provenienza, induce a individuare nelle fattispecie di riciclaggio e reimpiego il prevalente utilizzo illecito delle criptovalute.

Si tratta di una declinazione patologica ben nota al legislatore nazionale che, in attuazione degli *input* comunitari – da ultimo, la Direttiva (UE) 2018/843, cosiddetta *V direttiva antiriciclaggio* –, ha progressivamente implementato la disciplina concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento al terrorismo (D.lgs. 21 novembre 2007, n. 231), inserendo nella categoria degli "*altri operatori non finanziari*" (art. 3, comma 5) anche "*i prestatori di servizi relativi all'utilizzo di valuta virtuale*" e "*i prestatori di servizi di portafoglio digitale*". Si tratta, appunto, degli *Exchanger* e dei *Wallet provider* che oggi rinvengono una puntuale definizione all'art. 1, comma 2, lett. *ff)* e *ff-bis)* del D.lgs. 231/2007, che li identifica, rispettivamente, con le seguenti nozioni: ff. "*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*"; ff-bis. "*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*".

In verità, l'espansione dei destinatari della disciplina antiriciclaggio è frutto della stratificazione normativa che, nel caso in esame, ha condotto alla graduale integrazione del novero degli obbligati con l'inserimento della figura dell'*Exchanger*, attraverso il D.lgs. 25 maggio 2017, n. 90, di recepimento della IV Direttiva UE n. 849/2015, e, solo successivamente, di quella del *Wallet provider*, mediante il D.lgs. 4 ottobre 2019, n. 125, di recepimento della già citata V Direttiva UE n. 843/2018[29].

In tal modo, figure centrali nella gestione delle criptovalute vengono gravate dagli obblighi antiriciclaggio *ex* art. 3, comma 5, lettere *i)* e *i-bis)* del D.lgs. 231/07, che estende il perimetro della collaborazione attiva alle operazioni aventi ad oggetto la valuta virtuale, ossia "*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*" [art. 1, comma 2, *lett. qq)*][30].

Il coinvolgimento esteso al *Wallet provider* tiene conto del fatto che l'impiego (illecito) della criptovaluta può

avvenire anche in assenza di processi di conversione, secondo analisi empiriche in base alle quali «*given the limited scale of contained VC environments, money laundering involving VCs is likely to occur through two generic methods. First, criminals could place dirty fiat currency into a bank or other financial institutions, convert those funds to VCs using a VC exchange, and then engage in a variety of VC-based transfers or purchases to obscure the funds' criminal origin. Second, criminals could sell illegal goods or services for VCs, eventually convert those to fiat currency, and subsequently fund transactions and purchases designed to conceal their illicit source*»[31]. D'altra parte, ogni qualvolta il cyberlaundering ha ad oggetto ricchezza derivante da reati-presupposto per così dire *online integrated*, la figura del *Wallet provider* diviene predominante per il monitoraggio delle operazioni, essendo questa la figura deputata a fornire agli *users* i *virtual currency wallet* (portafogli elettronici) che agevolano le condotte di immagazzinamento, detenzione e trasferimento di *Bitcoin* (o altre criptovalute), nonché i rapporti tra *users* e venditori.

La *ratio* replica quella immaginata dal legislatore comunitario che ne ha plasticamente tratteggiato i contorni nell'VIII Considerando della V Direttiva antiriciclaggio, affermando che «*I prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale (vale a dire le monete e le banconote considerate a corso legale e la moneta elettronica di un paese, accettate quale mezzo di scambio nel paese emittente) e i prestatori di servizi di portafoglio digitale non sono soggetti all'obbligo dell'Unione di individuare le attività sospette. Pertanto, i gruppi terroristici possono essere in grado di trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme. È, pertanto, di fondamentale importanza ampliare l'ambito di applicazione della direttiva (UE) 2015/849 in modo da includere i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale. Ai fini dell'antiriciclaggio e del contrasto del finanziamento del terrorismo (AML/CFT), le autorità competenti dovrebbero essere in grado di monitorare, attraverso i soggetti obbligati, l'uso delle valute virtuali. Tale monitoraggio consentirebbe un approccio equilibrato e proporzionale, salvaguardando i progressi tecnici e l'elevato livello di trasparenza raggiunto in materia di finanziamenti alternativi e imprenditorialità sociale*».

In estrema sintesi, per quanto concerne le criptovalute, lo schema preventivo opera su due livelli: da un lato, vengono arruolate figure professionali che occupano una posizione potenzialmente contigua alle operazioni in valuta virtuale[32], sfruttando le informazioni privilegiate di *Exchanger* e *Wallet provider* (obbligati alla adeguata verifica della clientela e alla conservazione della relativa documentazione) anche grazie all'obbligo di segnalazione delle operazioni sospette, che scatta quando gli obbligati "sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o

di finanziamento del terrorismo o che comunque i fondi, *indipendentemente dalla loro entità, provengano da attività criminosa*" (art. 35, comma 1); dall'altro, vengono previsti oneri di iscrizione in una speciale sezione del registro dei cambiavalute gestito dall'Organismo degli Agenti e dei Mediatori (art. 128-*undecies* T.U.B.) con espressa comunicazione al MEF dell'inizio dell'operatività mediante la quale gli operatori in criptovalute aderiscono al sistema pubblico antifrode (art. 17-*bis*, comma 8-*bis*, D.lgs. 141/10).

Gli obblighi traslati in capo ai *prestatori di servizi relativi all'utilizzo di valuta virtuale* e *di servizi di portafoglio digitale* espongono tali figure alla potenziale integrazione dell'illecito amministrativo di *esercizio abusivo ex* art. 17-*bis*, comma 5, D.lgs. 141/10 e, in caso di violazione degli obblighi antiriciclaggio, alla contestazione di una o più delle fattispecie penali positivizzate all'art. 55, D.lgs. 231/07 (oltre che al corredo degli illeciti amministrativi di cui agli artt. 56 ss., D.lgs. 231/07)[33].

Il legislatore interviene con sistemi di monitoraggio prevalentemente incentrati sull'*accesso*, utilizzando il filtro dell'iscrizione all'albo quale condizione essenziale per esercitare le attività riguardanti la gestione delle valute e i servizi collegati al portafoglio digitale sul territorio nazionale. Un arretramento della focale sanzionatoria indotta dalla difficoltà di trovare strumenti in grado di attingere gli illeciti commessi nella gestione di quegli stessi servizi, cui viene fornita una tutela sbilanciata sul concetto di *controllo*, dove la sanzione presidia la generale "riserva di attività", prevenendo pericoli che si presumono generati da un esercizio non autorizzato[34].

In questo modo, la prevenzione assume la conformazione di tipo 'precauzionale' già indiziata dalla cultura del "*sospetto*" nella quale si innerva la disciplina antiriciclaggio e trovano linfa gli indicatori di anomalia del GAFI, che nel settembre 2020 ha pubblicato il *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* in cui ribadisce che «*Virtual assets (VA) and related services have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. The ability to transact across borders rapidly not only allows criminals to acquire, move, and store assets digitally often outside the regulated financial system, but also to obfuscate the origin or destination of the funds and make it harder for reporting entities to identify suspicious activity in a timely manner. These factors add hurdles to the detection and investigation of criminal activity by national authorities*»[35].

Come noto, tali indicatori di anomalia possono favorire l'individuazione di casi di uso illecito di *virtual assets*, supportando le Autorità di controllo nell'analisi delle s.o.s. (e nelle attività di vigilanza antiriciclaggio in

generale), nonché gli operatori (inclusi i *Virtual Asset Service Providers*), i professionisti (notai, commercialisti, avvocati, ecc.), le istituzioni finanziarie e gli altri soggetti obbligati a rilevare e segnalare operazioni sospette (previa corretta *customer due diligence*).

Tuttavia, tale profilo è frequentemente utilizzato come 'scivolo' penalistico che consente di convertire la violazione amministrativa in realizzazione del precetto penale sulla base del non condivisibile automatismo per cui alla violazione della norma antiriciclaggio (*rectius*, all'omessa segnalazione di operazione sospetta) corrisponde la integrazione del delitto di riciclaggio (art. 648-*bis* c.p.), non a caso considerato laboratorio di sperimentazione di *crime control* del mondo globalizzato.

Analogamente, nella rilettura giurisprudenziale il delitto di *riciclaggio*, pur essendo un reato di pericolo, assume i tratti del delitto *commissivo mediante omissione* (eventualmente realizzato con *dolo eventuale*), dirigendosi verso comportamenti di sospetto all'apparenza estranei al penalmente rilevante[36].

Il rischio è che tale fattispecie smarrisca le nobili finalità che ne avevano giustificato l'inserimento nel Codice penale per fronteggiare una delle più gravi forme di criminalità economica, trasformandosi in una forma di controllo a largo spettro, in grado di agganciare la sanzione penale all'incertezza del sospetto. Un profilo meritevole di attenzione anche per gli effetti collaterali insiti nella potenziale creazione di categorie di "capri espiatori" dell'antiriciclaggio, figure – come quelle degli operatori in criptovalute – esposte al *climax* ascendente di un arsenale sanzionatorio che dalle sanzioni amministrative e penali del D.lgs. 231/2007 si espande agli strumenti repressivi, prevalentemente rappresentati dalle stigmatizzanti fattispecie di ricettazione (art. 648 c.p.), riciclaggio (art. 648-*bis* c.p.), autoriciclaggio (art. 648-*ter*.1 c.p.) e impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.).

Le preoccupazioni appena espresse sono destinate ad accrescersi con il definitivo scollamento tra *fattispecie e tipo* generato dalla normativa di recepimento della direttiva UE 2018/1673 (c.d. *VI Direttiva antiriciclaggio*). Infatti, al fine di conformarsi all'ampia nozione di "attività criminosa" accolta dalla Direttiva[37], il citato D.lgs. 8 novembre 2021, n. 195trasfigura il *Tatbestand* originariamente cristallizzato nella struttura precettiva delle fattispecie appena richiamate. Segnatamente, il decreto attuativo ha provveduto all'estensione del novero dei reati-presupposto, ricomprendendovi anche le *contravvenzioni*, da un lato, e i *delitti colposi*, dall'altro [art. 1, comma 1, lett. *c)*, n. 3; art. 1, comma 1, lett. *d)*, n. 1; art. 1, comma 1, lett. *f)*, n. 1].

Tralasciando le imprecisioni del tessuto precettivo, che consegnano all'operatore una fattispecie di

autoriciclaggio (art. 648-*ter*.1c.p.) da *contravvenzione* (comma 2)[38], il risultato è che, oggi, le risorse illecite acquisite dal ricettatore (art. 648 c.p.) o dissimulate dal riciclatore (art. 648-*bis* c.p.) oppure ancora reimpiegate in circuiti economici leciti (artt. 648-*ter* e 648-*ter*.1 c.p.) potranno essere generate anche da un illecito penale di modesta consistenza offensiva o *non* sorretto dalla volontà criminosa[39].

Il problema di superfetazione applicativa è reale e trova nell'attuale giurisprudenza di legittimità i precursori del rischio-penale gravante sugli stessi operatori in criptovaluta[40]. D'altra parte, non è revocabile in dubbio che – a prescindere dalla sua controversa qualificazione giuridica – la valuta virtuale rientri nell'oggetto materiale delle condotte di riciclaggio e reimpiego, quantomeno sub specie di "*altra utilità*"[41]. E, fermo restando che le attività di ostacolo punibili sono solo quelle che «*in qualche modo incidano, materialmente o giuridicamente, sul bene stesso*»[42], non appare possibile affermare così nettamente che "*nei Bitcoin, l'unica operazione dissimulatoria riguarda l'eventuale intestatario della moneta virtuale, il quale sarebbe coperto da uno pseudo anonimato. Da un punto di vista materiale il bene non subisce alcuna opera di camuffamento, risultando le transazioni in Bitcoin perfettamente tracciabili e visibili*"[43].

Il monito è però utile a riaffermare con decisione la necessità di un controllo critico sull'incriminazione che utilizzi il paradigma dell'offesa dell'interesse tutelato come stella polare dell'interprete, evitando che '*nemico*'divenga lo strumento nato per contrastarlo[44].

4.1. *Criptoattività e autoriciclaggio: il cyber self-laundering.*

Le criptovalute possono configurare lo strumento di operazioni di *cyber self-laundering*, astrattamente sussumibili nella fattispecie di cui all'art. 648-*ter*.1 c.p. (autoriciclaggio).

A tal riguardo, vale la pena ricordare che il delitto si perfeziona quando: *i.* la condotta è integrata dall'autore (o concorrente) del reato-presupposto; *ii.* l'impiego, la sostituzione o il trasferimento di denaro, beni o altre utilità è destinato ad attività economiche, finanziarie, imprenditoriali o speculative («in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa»)[45]. Sotto il primo profilo, la configurazione di tale fattispecie sarà più probabile nelle ipotesi di riciclaggio digitale c.d. integrale, restando tuttavia plausibile un autoriciclaggio derivante da reato presupposto realizzato *offline*. Diversamente, la seconda condizione non sarà soddisfatta con il semplice acquisto di valuta virtuale, da solo insufficiente a realizzare il

disvalore del tipo.

Tanto premesso, non può aprioristicamente escludersi il rischio penalistico da autoriciclaggio, realizzabile (ad esempio per l'*Exchanger*)anche a titolo di concorso[46]. Significativa, in tal senso, una recente pronuncia della Cassazione (Cass. pen., Sez. II, 7 ottobre 2021-25 gennaio 2022, n. 2868) che ha riconosciuto la sussistenza del reato di autoriciclaggio in capo all'autore del reato-matrice laddove i profitti di un'attività illecita vengono convertiti in criptovaluta da una società terza (nel caso di specie, impegnata professionalmente al cambio da euro in Bitcoin). Richiamata la natura dell'art. 648-*ter*.1 c.p. come reato di pericolo, i Giudici ribadiscono che la fattispecie si perfeziona con condotte idonee *ex ante* a ostacolare concretamente l'identificazione della provenienza delittuosa delle utilità provenienti da reato, affermando che «*le operazioni realizzate attraverso il trasferimento di valuta verso società estere che si interponevano nell'acquisto di criptovalute ed effettuate anche a mezzo di prestanome ponevano un serio ostacolo alla identificazione del ricorrente come beneficiario finale delle transazioni ed effettivo titolare di bitcoin acquistati non da lui ma dalle società estere che fungevano da exchanger di criptovalute*». E addirittura ci si spinge oltre, affermando che «*all'attività di cambio della valuta deve essere attribuito carattere finanziario, tanto che in Italia essa è regolamentata dalla legge ed il soggetto che la esercita deve essere iscritto in appositi registri (il D.lgs. 1 settembre 1993, n. 385, art. 155, comma 5, recante il Testo Unico delle Leggi in materia bancaria e creditizia, stabilisce che i soggetti che esercitano professionalmente l'attività di cambiavalute, sono iscritti in un'apposita sezione dell'Elenco previsto dall'art. 106, comma 1, del T.U.)*».

Senza entrare nel merito di un approdo giurisprudenziale il cui carattere assolutistico ingenera più dubbi di quanti sia chiamato a fugarne[47], è necessario prendere atto che la prassi ritiene l'autoriciclaggio integrato dalla preliminare operazione di cambio della valuta cui il disponente da corso servendosi di società di cambiavalute (*rectius*, di *Exchanger* di criptovalute). La Cassazione, infatti, afferma con nettezza che «*la condotta del ricorrente rientra tra quelle punite dalla norma incriminatrice contestatagli, per avere dato corso al trasferimento del profitto dei reati presupposto in una attività finanziaria costituita dal cambio della valuta posto in essere su suo mandato da società estere. Ciò consente di ritenere del tutto irrilevante verificare quale fosse stato l'utilizzo ancora successivo dei bitcoin infine ottenuti dal ricorrente (...)*».

A tale motivazione fa da eco un'ancor più recente pronuncia dei giudici di legittimità (Cass. pen., Sez. II, 7 luglio 2022 - 13 luglio 2022, n. 27023) che equipara l'acquisto di valuta virtuale all'investimento (di profitti illeciti) in operazioni di natura finanziaria (idonee a ostacolare la tracciabilità e la ricostruzione della origine delittuosa del denaro). Insomma, le *cryptocurrencies* vengono ritenute strumenti finanziari in quanto tali riconducibili all'ambito delle "attività speculative", in quanto «*le valute virtuali possono essere utilizzate per*

scopi diversi dal pagamento e comprendere prodotti di riserva di valore a fini di risparmio ed investimento (sul punto, il parere della BCE riportato a pag. 18 dell'ordinanza, recepito nella V direttiva UE antiriciclaggio 2018/843)». La stigmatizzazione dei *crypto-assets* sembra derivare dal fatto che con essi «*è possibile garantire un alto grado di anonimato (sistema c.d.* permissionless*), senza previsione di alcun controllo sull'ingresso di nuovi "nodi" e sulla provenienza del denaro convertito (si è anche sottolineato come sia ormai noto il vasto numero di criptovalute utilizzate nel* darkweb*, proprio per le loro peculiari caratteristiche, e che alcune di esse, attraverso l'uso di tecniche crittografiche avanzate, garantiscono un elevato livello di* privacy *sia in relazione alla persona dell'utente sia in relazione all'oggetto delle compravendite)*».

Ebbene, anche in questo caso il pericolo è quello di una espansione incontrollata della fattispecie di reato, che deve essere sottratta all'esuberanza propria del diritto penale del rischio e sottoposta a una ermeneutica normativamente orientata.

Il programma epistemologicamente verificabile del *tipo* astrattamente positivizzato consente, infatti, di operare una netta distinzione tra la mera conversione di valuta, difficilmente in grado di attivare la sanzione dell'art. 648-*ter*.1 c.p., e la 'destinazione' pretesa dalla fattispecie, in cui rientrerebbe la stessa attività di cambiavalute, intesa come attività *lato sensu* economica, nella quale l'operatore in criptovaluta potrebbe investire il provento di reato (eventualmente già ottenuto in *Bitcoin* o altra valuta virtuale) per finalità speculative. In altri termini, diversamente dai casi in cui si limitino ad effettuare il *cambio di valuta* su impulso del cliente, i prestatori di servizi relativi all'utilizzo di valuta virtuale (che svolgono tale attività anche in forma societaria) potranno essi stessi rispondere di «autoriciclaggio» (in assetto monosoggettivo o plurisoggettivo), laddove impieghino valuta virtuale o reale, generata da reati (*online* od *offline*) eventualmente realizzati in concorso con altri (ad es. *hackers*), nell'attività di cambiavalute svolta "a titolo professionale". In questo caso, infatti, l'attività svolta dall'*Exchanger* rileverà come attività economica, finanziaria, imprenditoriale o speculativa cui le somme vengono destinate, incarnando la *ratio* – ancor prima che la lettera – dell'art. 648-*ter*.1 c.p., con conseguente responsabilità della persona fisica o dell'ente per autoriciclaggio integrato tramite impiego di criptovalute[48].

5. *'231' e criptovalute: la responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali*.

Gran parte delle fattispecie passate in rassegna possono attivare il D.lgs. 8 giugno 2001, n. 231 recante la disciplina della responsabilità amministrativa dell'ente da reato. Sicuramente, tale responsabilità può sorgere nelle ipotesi di ricettazione (art. 648 c.p.), riciclaggio (art. 648-*bis* c.p.), autoriciclaggio (art. 648-*ter*.1

c.p.) e reimpiego (art. 648-*ter* c.p.), eventualmente afferenti ai *crypto assets*, integrate da soggetto apicale o subordinato nell'*interesse o a vantaggio* dell'ente di cui è dipendente. In simili circostanze, infatti, la contestazione può essere estesa alla società (eventualmente un *Wallet provider* o un *Exchanger* che eserciti tali servizi in forma organizzata) per il tramite dell'art. 25-*octies*, D.lgs. 231/2001, in forza del quale «*in relazione ai reati di cui agli artt. 648, 648-bis, 648-ter e 648ter.1 del codice penale, si applica all'ente la sanzione pecuniaria da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote. Nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'art. 9, comma 2, per una durata non superiore a due anni (…)*»[49].

L'analisi del diritto vivente induce a ritenere elevato – soprattutto alla luce dell'ampliamento delle fattispecie incluse nell'art. 25-*octies* – il rischio-reato anche per gli operatori di *cryptocurrencies* che si rendessero autori di dolose violazioni degli obblighi di segnalazione, integrando la suddetta omissione (non impeditiva) nella consapevolezza della illecita provenienza del denaro oggetto dell'operazione stessa.

In simili circostanze, la combinazione delle '231' (d.lgs. 231/2001 e d.lgs. 231/2007) trova nelle fattispecie di (auto)riciclaggio e reimpiego la verticalizzazione della punibilità destinata a colpire la *societas*.

All'elevato grado di stigmatizzazione non corrisponde tuttavia un adeguato meccanismo di controllo del *tipo*, sottoposto alla costante erosione della giurisprudenza e definitivamente slabbrato dal recente intervento legislativo (D.lgs. 8 novembre 2021, n. 195). Sicché, le nobili aspirazioni che hanno condotto al superamento di una responsabilità *ex delicto* di natura esclusivamente antropomorfica e alla elaborazione di criteri di imputazione autonomi per l'ente rischiano di essere vanificate dalla scarsa capacità selettiva di meccanismi ascrittivi deformati o inattuati dalla prassi[50].

In altri termini, le possibilità che un ente possa evitare una condanna per riciclaggio risultano veramente molto basse per la combinazione di due aspetti esiziali: da un lato, gli elevati *standards* pretesi in sede di valutazione della "idoneità" dei modelli organizzativi e gestionali, che segna la scarsa efficacia 'esimente' ad essi riconosciuta nelle sentenze penali; dall'altro, il graduale abbassamento della base probatoria, che non pretende l'accertamento giudiziale del reato-presupposto (ritenendosi bastevole la prova logica) e si accontenta del dolo eventuale come supporto psicologico di condotte che possono arrestarsi all'ipotetico pregiudizio arrecato alla ricostruzione del *paper trail*. Valutazioni discrezionali che riferite alle "valute virtuali" rischiano di consegnare il processo ermeneutico al meccanismo della presunzione, dove l'equazione cripto-

valuta = cripto-attività è in grado di conferire carattere automaticamente illecito alle operazioni che le riguardano.

La problematica si iperbolizza con riferimento all'*autoriciclaggio* (art. 648-*ter.*1c.p.) a causa della sostanziale elusione del *numerus clausus* posto alla base della responsabilità dell'ente e del principio di legalità rafforzata, che dovrebbero invece garantire l'ente impendendo che esso sia «ritenuto responsabile per un fatto costituente reato se la sua responsabilità amministrativa in relazione a quel reato e le relative sanzioni non sono espressamente previste da una legge entrata in vigore prima della commissione del fatto» (art. 2, D.lgs. 231/2001)[51].

In questo caso, il rischio è che la forza espansiva delle fattispecie di (auto)riciclaggio e reimpiego dilati il catalogo 'formale' dei reati-presupposto, mettendo in crisi i sistemi di *compliance* dell'ente, se non addirittura i criteri di imputazione previsti dagli artt. 6 e 7 del D.lgs. 231/2001 sui quali si regge il microsistema che consente al *societas delinquere potest* di convivere con i principi costituzionali di un diritto penale moderno.

---

[1] E. U. Savona, *Criminalità organizzata – concetti e definizioni*, consultabile in *open source* al seguente link: *www.jus.unitn.it/users/dinicola/criminologia/topics/materiale/dispensa_5_1.pdf*, 1.

[2] In argomento, le lucide considerazioni di G. Forti, *Il crimine economico: prospettive criminologiche e politico-criminali*, in M. Catenacci, *Temi di diritto penale dell'economia e dell'ambiente*, Giappichelli, Torino, 2009, pp. 3 ss.

[3] L'espressione è mutuata da L. Donato, *Diritto penale ed economia: criminalità, imprese, banche*, in L. Donato, D. Masciandaro (*a cura di*), *Moneta, banca, finanza. Gli abusi del mercato*, Hoepli, Milano,2001, p. 51.

[4] Così, E. H. Sutherland, *Il crimine dei colletti bianchi. La versione integrale*, G. Forti (a cura di), presentazione Geis-Goff, Giuffrè, Milano, 1987, pp. 299 s. In argomento, si rinvia a A. R. Castaldo, M. Naddeo, *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio*, Cedam, Padova, 2010, spec. pp. 47 ss. Di recente, l'interesse della criminalità per le più moderne tecnologie e, segnatamente, per gli strumenti che consentono

un rapido e invisibile passaggio di denaro come le criptovalute è evidenziato dalla Direzione Investigativa Antimafia – DIA, 26 marzo 2022, *Relazione del Ministro dell'Interno al Parlamento*, I semestre 2021, pagg. 401 ss.

[5] Già in questi termini in M. Naddeo, *Il diritto penale dell'economia nell'era del Fintech*, in *Fintech: Law, Technology and Finance*, Bocconi Legal Papers, n. 16/2021, pagg. 127 ss. Una ricostruzione degli effetti sociali e giuridici della rivoluzione tecnologica è offerta da L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime*, Utet, Torino, 2019, pagg. 35 ss.; L. Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Cedam, Padova, 2004, pp. 56 ss. Sul *locus commissi delicti*, il riferimento è a R. Flor, *I limiti del principio di territorialità nel "cyberspace". Rilievi critici alla luce del recente orientamento delle sezioni unite*, in *Dir. pen. proc.*, 2015, pagg. 1296 ss.

[6] M. Amato, L. Fantacci, *Per un pugno di* Bitcoin, Giuffrè, Milano, 2016, p. 3.

Sebbene alla base delle transazioni in criptovaluta siano poste chiavi trasmesse in flussi pubblici astrattamente riconducibili a una persona, dalla prospettiva investigativa "*non c'è modo di risalire alla loro vera identità, né a quella digitale (un indirizzo IP, un indirizzo e-mail), né tanto meno a quella fisica. Tutto quello che si può fare per cercare di individuare gli utenti bitcoin è monitorare un singolo indirizzo e da queste informazioni tentare di riuscire a identificare possibili possessori dell'indirizzo. La possibilità di risalire alle identità che si celano negli account è però fortemente depotenziata dalla possibilità per gli utenti di ottenere un nuovo indirizzo bitcoin per ogni transazione*", letteralmente A. Laudati, *Prefazione* in R. Razzante, *Bitcoin e criptovalute. Profili fiscali, giuridici e finanziari*, Maggioli Editore, Rimini, 2018, p. 8.

[7] K. Volk, *Criminalità organizzata e criminalità economica*, in S. Moccia (*a cura di*), *Criminalità organizzata e risposte ordinamentali. Tra efficienza e garanzia*, Edizioni Scientifiche Italiane, Napoli, 1999, pp. 364 ss.

[8] Un'analisi organizzata della casistica maggiormente rappresentativa è offerta da G. P. Accinni, *Cybersecurity e criptovalute. Profili di rilevanza penale dopo la quinta direttiva* in *Sistema penale*, n. 5/2020, pp. 215 ss.

[9] Il riferimento è all'*Internet Organised Crime Threat Assessment* (IOCTA) 2017, fruibile sul portale istituzionale

al link seguente: *www.europol.europa.eu*.

[10] Approfondimenti in O. Calzone, *Servizi di mixing e Monero*, in *Gnosis*, 28 luglio 2017, in *open source* al sito istituzionale del SISR *https://www. sicurezzanazionale.gov.it*.

[11] Letteralmente, L. Picotti, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dr. pen. ec.*, 3-4/2018, p. 605.

[12] In argomento, per tutti A.R. Castaldo, *La concretizzazione del rischio giuridicamente rilevante*, in *Riv. it. dir. proc. pen*., 1995, pagg. 1096 ss. (in particolare pagg. 1102), per cui "*l'intenzionalità dell'offesa, tipica dell'illecito doloso, abbassa il quorum di rischi che l'ordinamento è disposto a tollerare, ampliando così l'area del rischio significativo, imputabile all'autore*"; V. Militello, *Diritto penale del rischio e rischi del diritto penale fra scienza e società*, in *Europe in Crisis: Crime, Criminal Justice, and the Way Forward. Essays in honour of Nestor Courakis*, vol. II, *Essays in English, German, French, and Italian*,Ant. N. Sakkoulas Publishers L.P., Athens, 2017, pagg. 223 ss.

[13] D. Castronuovo, *Le sfide della politica criminale al cospetto delle generazioni future e del principio di precauzione: il caso OGM*, in *Riv. trim. dir. pen. ec.*, n. 3/2013, pagg. 402 ss.

[14] C. Clemente, *Presentazione del Rapporto Annuale dell'Unità di Informazione Finanziaria per l'Italia (anno 2017)*, in www.uif.it, p. 5. In argomento, E. Messina, *Bitcoin e riciclaggio*, in *Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale*, B. Quattrociocchi (*a cura di*), Giappichelli, Torino, 2017, pp. 381 ss.

[15] Sulla ipertrofia del diritto penale, C. E. Paliero, *«Minima non curat praetor». Ipertrofia del diritto penale e decriminalizzazione dei reati bagatellari*, Cedam, Padova, 1985, *passim*; C. Sotis, *Il diritto senza codice. Uno studio sul sistema penale europeo vigente*, Giuffrè, Milano, 2007, pp. 207 e ss., nonché pp. 310 ss.

[16] D. Castronuovo, *Principio di precauzione e diritto penale. Paradigmi dell'incertezza nella struttura del reato, «I libri»* di *Archivio penale*, VIII, Roma, 2012, pagg. 40 ss. L'Autore analizza il principio di precauzione come "fattore espansivo" del diritto penale, traendone conferme nelle legislazione e nella giurisprudenza penale, rimarcando anche qualche sorprendente «*smentita, almeno parziale, nella concreta gestione giurisprudenziale di alcune discipline legislative fortemente sensibili all'approccio precauzionale, là dove il principio in questione entri in conflitto con i principi penalistici classici: in particolare, legalità, offensività,* ultima ratio, *personalità-colpevolezza*».

[17] Pone il bene della integrità e sicurezza informatica in posizione strumentale alla tutela di altri beni giuridici finali, L. Picotti, *Cybersecurity: quid novi?*, in *Diritto di internet*, 2020, pp. 11 ss.; l'approccio europeo è investigato da R. Flor, *Cybersecurity ed il contrasto ai cyber-Attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di internet*, 2020, pp. 460 ss.

[18] La Direttiva UE 2019/713 relativa alla *lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti* ha trovato attuazione in Italia con il Decreto legislativo 8 novembre 2021, n. 184, pubblicato in Gazzetta Ufficiale n. 284 del 29 novembre 2021 ed entrato in vigore il 14 dicembre 2021. Per un commento alla Direttiva in questione, R. M. Vadalà, *La disciplina penale degli usi e degli abusi delle valute virtuali*, in *Diritto e internet*, n. 3/2020, pp. 397 ss.

[19] Dal punto di vista nozionistico, è opportuno precisare che in base all'art. 2 della Direttiva UE 2019/713 "*si intende per: a) «strumento di pagamento diverso dai contanti» un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali; b) «dispositivo, oggetto o record protetto» un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta, per esempio mediante disegno, codice o firma; c) «mezzo di scambio digitale» qualsiasi moneta elettronica definita all'articolo 2, punto 2, della direttiva 2009/110/ CE del Parlamento europeo e del Consiglio (12) e la valuta virtuale; d) «valuta virtuale» 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; e) «sistema di informazione» un sistema di informazione quale definito all'articolo 2, lettera a), della direttiva 2013/40/UE; f) «dati informatici» i dati informatici quali definiti all'articolo 2, lettera b), della direttiva 2013/40/UE; g) «persona giuridica» qualsiasi entità che abbia personalità giuridica in forza del diritto applicabile, ad eccezione degli Stati o di altri organismi pubblici nell'esercizio dei pubblici poteri e delle organizzazioni internazionali pubbliche*".

[20] In argomento, L. Picotti, *Sicurezza, informatica e diritto penale*, in M. Donini, M. Pavarini (a cura di), *Sicurezza e diritto penale*, BUP, Bologna 2011, pagg. 217 ss.; I. Salvadori, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in *Riv.it. di dir. proc. pen.*, 2/2017, pagg. 757 ss.

[21] Così, testualmente, la Comunicazione dell'Unità nazionale d'informazione finanziaria UIF del 28 maggio 2019, reperibile al seguente indirizzo *https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/Comunicazione_VV_2019.pdf*.

[22] Svariate sono le forme di *Ransomware attacks* che convivono con le più comuni frodi ai *miners* coinvolti in transazioni trappola (art. 640 c.p.) o sottrazioni di chiavi private di accesso ai conti perpetrate nei confronti di altri *Exchangers* o *Wallet providers* (art. 624 c.p.). Le fenomenologie in questione sono analizzate da F. Boncompagni, *Crimini informatici e criptovalute*, in S. Capaccioli (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, Milano, 2021, pagg. 302 ss.

[23] Sul punto, si rinvia a R. Flor, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. dir. proc. pen*., n. 2-3/2007 pp. 899 ss.; F. Cajani, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, pagg. 1194 ss.

[24] Sulla fenomenologia dell'estorsione con richiesta di pagamento in criptovalute e i reati configurabili, si veda F. Boncompagni, *Crimini informatici* cit., pagg. 312 ss.; P. Dal Checco, *Ransomware e ricatti virtuali: violazioni della privacy e dei propri dati, nuove modalità di estorsione e di pagamento*, in F. Federici, A. Allegria, M. Di Stefano (a cura di), *Il diritto del web. Rete, intelligence e Nuove Tecnologie*, Cedam, Padova, 2017, pagg. 368 ss.

[25] Cfr. Rapporto annuale UIF, Comunicazione cit., pagg. 47 s.

[26] Testualmente, E. Simoncini, *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, in *Riv. trim. dir. pen. ec.*, n. 4/2015, pagg. 897 ss.

[27] Sul riciclaggio digitale si rinvia a: S. Mulinari, *Cyberlaundering: riciclaggio di capitali, finanziamento del terrorismo e crimine organizzato nell'era digitale*, Torino, 2003, pagg. 62 ss.; L. Picotti, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio* in *Riv. trim. dir. pen. ec.*, n. 3-4/2018, pagg. 592 ss.

[28] Si tratta della descrizione della *Blockchain* fornita da A. Rosato, *Profili penali delle criptovalute*, in *Quaderni di C.R.S.T.* (Centro Ricerca Sicurezza e Terrorismo, diretto da R. Razzante), Pacini Giuridica, Pisa, 2021, pagg. 13 ss.

[29] Sulla opportunità di perfezionare la integrazione della categoria dei destinatari con la figura dei *prestatori di servizi di portafoglio digitale* sia consentito il rinvio a M. Naddeo, *Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale*, in *Dir. pen. proc.*, n. 1-2019, pagg. 101 ss.

[30] La disposizione ricalca la definizione offerta dalla Banca d'Italia nella sua *Comunicazione del 30 gennaio 2015* avente ad oggetto proprio le *Valute virtuali*, quando la UIF ne segnalava l'indice di anomalia, allo scopo di prevenire l'utilizzo del sistema economico-finanziario a fini di riciclaggio e finanziamento del terrorismo.

[31] Sono le considerazioni di D. Carlisle, *Virtual Currencies and Financial Crime. Challenges and Opportunities*, Royal United Services Institute for Defence and Security Studies, RUSI, *Occasional Paper*, marzo 2017, p. 14. Nello stesso senso si era pronunciata anche la Banca Centrale Europea, evidenziando come il coinvolgimento dell'*exchanger* non fosse sempre necessario, vista la possibilità di scambiare beni e servizi *online* con l'impiego di criptomoneta, così BCE, *Opinione della Banca Europea Centrale* del 12 ottobre 2016 *on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending* Directive 2009/101/EC (CON/2016/49).

[32] L. Sturzo, *Bitcoin e riciclaggio 2.0*, in *Riv. trim. dir. pen. cont.*, n. 5-2018, pag. 29, considera gli *Exchangers* «*custodi del rispetto della normativa antiriciclaggio da parte degli utenti Bitcoin, in quanto unici soggetti in grado di individuare l'identità dell'utente di bitcoin prima che lo stesso sparisca dietro un account composto da numeri e lettere anonime*».

[33] Viste le peculiarità della criptovaluta, non sembra che il *Cryptocurrency Exchange* possa integrare con la sua condotta *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)*. Il dubbio, posto da Banca d'Italia in un'*avvertenza sull'utilizzo delle cosiddette "valute virtuali"* datata 30 gennaio 2015, non è fugato dall'attuale assetto normativo. Di contrario avviso chi sostiene che "*oggi ogni incertezza appare superata dall'espresso riconoscimento di tale categoria da parte del legislatore, e da contestuale obbligo di registrazione degli exchanger in una apposita sezione del registro dei cambiavalute (art. 17-bis d.lgs. 141/2010)*", così R. Lucev, F. Boncompagni, *Criptovalute e profili di rischio penale nella attività degli exchanger*, in *Giurisprudenza penale web*, n. 3-2018, p. 2. Sulla natura giuridica del Bitcoin, si veda anche N. Vardi, *Criptovalute e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. Inf.*, 1-2015, pp. 450

ss.; G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. Inf.,* 1-2015, pp. 431 ss.

[34] In argomento, E. Montani, *La tutela del corretto svolgimento dell'attività di intermediazione e bancaria*, in *Trattato teorico pratico di diritto penale*, F. Palazzo, E. Paliero (*diretto da*), vol. VIII, *Reati in materia economica*, a cura di A. Alessandri, Giappichelli, Torino, 2012, p. 223. Analogamente, la prevalenza di fattispecie avamposto caratterizza la materia del diritto penale bancario e finanziario, per tutti C. Pedrazzi, *Mercati finanziari (nuova disciplina penale)*, in *Dig. disc. pen.*, vol. VII, Utet, Torino, 2000, p. 455.

[35] Così, FATF (2020), *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, FATF, Paris, France, liberamente fruibile dal link *www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html*.

[36] In questi termini, E. Cappa, *La direttiva UE 1673/2018 sulla lotta al riciclaggio mediante il diritto penale. Criticità per il settore bancario*, in *Dir. Banc.*, maggio 2021, pagg. 7 s. L'Autore evidenzia come legittimare l'utilizzo delle condotte omissive tipiche della disciplina antiriciclaggio al fine di integrare il precetto di cui all'art. 648-*bis* c.p., *ha consentito la formulazione illogica (anche se "utile" in chiave meramente repressiva) di sillogismi (pseudo) deduttivi in cui la "premessa maggiore" è integrata dall'inosservanza della normativa antiriciclaggio, la "premessa minore" dal legame tra detta violazione e l'integrazione dell'art. 648-bis c.p. (a cui fa seguito la punibilità per riciclaggio dell'autore della violazione amministrativa*. Si veda anche, ivi citato, F. Di Vizio, *Il riciclaggio nella prospettiva penale ed in quella amministrativa. Definizioni di riciclaggio*, in *Quaderni della Banca d'Italia*, n. 8/2017, *passim*.

[37] All'art. 2, par. 1, la Direttiva in esame declina la nozione di "attività criminosa" come "*qualsiasi tipo di coinvolgimento criminale nella commissione di un qualsiasi reato punibile, conformemente al diritto nazionale, con una pena detentiva o con una misura privativa della libertà di durata massima superiore ad un anno ovvero, per gli Stati membri il cui ordinamento giuridico prevede una soglia minima per i reati, di un qualsiasi reato punibile con una pena detentiva o con una misura privativa della libertà di durata minima superiore a sei mesi». Per poi proseguire con l'elencazione di una serie di figure criminose (tra cui la partecipazione ad un gruppo criminale organizzato, il terrorismo, la tratta di essere umani ed il traffico di migranti, lo sfruttamento sessuale, il traffico illecito di sostanze stupefacenti, di armi, di beni rubati, rapina, omicidio, lesioni gravi, reati fiscali ed ambientali ecc.), che appartengono comunque alla categoria*".

[38] Art. 648-*ter* c.p. (autoriciclaggio). "*1. Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa. 2. La pena è della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi. 3. La pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. 4. Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 416.bis.1. 5. Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale. 6. La pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale. 7. La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto. 8. Si applica l'ultimo comma dell'articolo 648*".

[39] Saluta, invece, positivamente l'intervento riformatore, F. Bellagamba, *In dirittura d'arrivo la riforma del riciclaggio: alcune proposte di modifica per andare oltre il mancato recepimento della direttiva europea*, in *Sistema penale*, 11 ottobre 2021. L'Autore sostiene che "*tale interpolazione faccia giustizia di una duplice incongruenza letterale-sistematica che affligge le previsioni vigenti*". Da un lato "l'ambiguità del riferimento al "delitto" quale *presupposto positivo*per la configurazione delle relative fattispecie, quando, per indicare il *presupposto negativo* (e, cioè, la vera e propria clausola di riserva), si ricorre al lemma "reato", innescandosi, così, un corto circuito interno"; dall'altro "la già prevista punibilità della ricettazione (art. 648 c.p.) e dell'impiego di denaro di provenienza illecita (art. 648 *ter* c.p.) anche a fronte di delitti-presupposto *colposi*e la contraria, espressa, limitazione degli artt. 648 *bis* e 648 *ter*.1 c.p. ai soli delitti "*non colposi*"

In senso critico, G. Pastelli, *Riflessioni critiche sulla riforma dei reati di ricettazione, riciclaggio, reimpiego e autoriciclaggio di cui al d.lgs. 8 novembre 2021, n. 195*, in *Sistema penale*, 08 dicembre 2021; nella stessa rivista R. M. Vadalà, *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, 6 maggio 2020.

[40] In materia, N. Mainieri, *La Cassazione penale esamina le valute virtuali sotto il profile del Testo Unico della Finanza – le precedenti qualificazioni e I richiami della Direttiva penale sulla lotta al riciclaggio mediante uso del*

penale (n. 2018/1673 UE), in *Giur. Pen.*, n. 10/2020.

[41] Considera le criptovalute «*beni, come definiti dal Codice civile, e anche se non lo fossero rientrerebbero certamente nel concetto di altre utilità*», S. Capaccioli, *Criptovalute e bitcoin: un'analisi giuridica*, Giuffrè, Milano, 2015, p. 252.

[42] A. Maugeri, *L'autoriciclaggio dei proventi dei delitti tributari: ulteriore espressione di voracità statuale o utile strumento di politica criminale?* in E. Mezzetti, D. Piva (a cura di), P*unire l'Autoriciclaggio. Come, quando e perché*, Giappichelli, Torino, 2016, pag. 140.

[43] In questi termini, G. J. Sicignano, *L'acquisto di bitcoin con denaro di provenienza illicita,* in *Arch. Pen.*, n. 2/2020, pag. 15, il quale afferma che "*se il problema dei bitcoin è che garantiscono l'anonimato ai loro utilizzatori, appare evidente che, alla luce della dottrina e giurisprudenza appena citata, non sembra ricorrere nel nostro caso l'ostacolo di cui all'art 648 bis c.p.*".

[44] M. Donini, *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in *Riv. trim. dir. pen. cont*., n. 4/2013, *passim*.

[45] In argomento, M. Lanzi, *Autoriciclaggio*, in V. Maiello, L. Della Ragione (a cura di), *Riciclaggio e reati nella gestione dei flussi di denaro sporco*, Giuffrè, Milano, 2018, pagg. 339 ss. G. J. Sicignano, *L'acquisto di bitcoin con denaro di provenienza illicita*, cit., pagg. 20, per il quale «*si deve escludere che i bitcoin configurino una attività speculati- va, difettando il requisito della natura finanziaria o economica della condotta. Non è qui in discussione se i bitcoin rappresentino o meno un prodotto finanziario, ma se concretizzino una «attività» finanziaria o economica con fine speculativo. Questo è sicuramente da escludere*».

[46] Da un punto di vista fenomenologico, è probabile che la nuova figura di 'cambiavalute' entri in contatto con l'autore del reato-presupposto, intenzionato ad usufruire dei suoi servizi a scopo di riciclaggio, quando quest'ultimo è già in possesso della valuta (virtuale o reale) di provenienza illecita da sottoporre al processo di conversione. L'apporto arrecato in sede di (auto)riciclaggio consentirebbe di configurare in capo all'Exchanger il concorso nell'altrui condotta di «autoriciclaggio», secondo lo schema del «concorso dell'extraneus nel reato proprio». In tal senso, invece, L. Sturzo, *op. cit*., pp. 28 s., che prendendo le mosse da Cass. pen., Sez. II, 14 luglio 2017, n. 42561, ritiene «*verosimile che il terzo exchanger possa essere ritenuto concorrente extraneus nel reato proprio, in quanto l'autore del reato presupposto non avrebbe potuto procedere al*

trasferimento del bene (bitcoin) proveniente dal delitto non colposo (es. traffico di stupefacenti) in un'attività economica finanziaria (attività di cambia valute) ostacolandone concretamente l'identificazione della loro provenienza in mancanza del contributo da questi realizzato». In materia di realizzazione plurisoggettiva dell'autoriciclaggio si è, di recente, pronunciato il giudice di legittimità: Cass. pen., Sez. II, 17 gennaio 2018 - dep. 18 aprile 2018, n. 17235.

[47] Sulla possibilità che i *crypto assets* possano rientrare nella categoria di "strumenti finanziari" o "prodotti finanziari" si rinvia a F. Dalaiti, *Cripto-valute e abusivismo finanziario: crypto-analogia o interpretazione estensiva?*, in *Sistema penale*, n. 1/2021, pagg. 52 ss.

[48] Al riguardo, sia consentito il rinvio a M. Naddeo, *Autoriciclaggio: i compromessi di un difficile inquadramento sistematico*, in *Riv. trim. dir. pen. ec.*, n. 3-4, 2016, pp. 697 ss.

[49] Ove accertata, la integrazione dell'art. 25-*octies*, d.lgs. 231/01 consente la confisca (e, in via cautelare, il sequestro preventivo) del profitto del reato. In argomento, R. Lucev, F. Boncompagni, *Criptovalute e profili di rischio penale nella attività degli exchanger*, cit., pp. 6 ss. In termini di semplificazione probatoria, C. Mancini, *Riciclaggio e responsabilità degli enti. I modelli organizzativi*, in E. Cappa, D. Cerqua (a cura di), *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*, Giuffrè, Milano, 2012, pagg. 104 ss.

[50] Segnala le difficoltà di recuperare una capacità selettiva al meccanismo di corresponsabilizzazione dell'ente, A. Gullo, *La responsabilità dell'ente e il sistema dei delitti di riciclaggio*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Diritto penale dell'economia*, Utet, Torino, 2017, pagg. 3500 ss. In argomento, anche le considerazioni di F. D'Arcangelo, *Il ruolo della responsabilità da reato degli enti nel contrasto al riciclaggio*, in *Resp. amm. soc.*, 4/2008, pagg. 41 ss.

[51] Analogamente, G. J. Sicignano, *231 e criptovalute. La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali*, Pacini Giuridica, Pisa, 2021, pagg. 229 ss. In argomento, A. R. Castaldo, *Costruzione normativa e difficoltà applicative dell'autoriciclaggio*, in Borsari (a cura di), *Itinerari di diritto penale dell'economia*, Cedam, Padova, 2018, pagg. 417 ss.; A. Rossi, *Note in prima lettura su responsabilità diretta degli enti ai sensi del d.lgs. 231/2001 e autoriciclaggio: criticità, incertezze, illazioni ed azzardi esegetici*, in *Riv. trim. Dir. pen. cont.*, 1/2015, pagg. 127 ss.; A Nisco, *Responsabilità degli enti, antiriciclaggio e autoriciclaggio: virtuose sinergie e problematiche interferenze*, in R. Borsari (a cura di), *Responsabilità da reato degli enti. Un consuntivo critico*, UP, Padova, 2016, pagg. 344 ss.