Università degli Studi di Padova

Dipartimento di Diritto Privato e Critica del Diritto
Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in
Giurisprudenza
a.a. 2021/2022

Diritto Penale dell'Economia

CYBERLAUNDERING E CRIPTOVALUTE: NUOVE FRONTIERE DEL DELITTO DI RICICLAGGIO

Relatrice: Chiar.ma Prof.ssa Debora Provolo

Laureanda: Elisabetta Piazza
Matricola: 1171413

Dedico questo mio lavoro ai miei genitori, a mio fratello Tommaso e alle mie sorelle Giulia e Costanza.

Vi ringrazio per aver reso più leggere le difficoltà di questo percorso e per aver condiviso con me ogni soddisfazione.

Padova, 15 luglio 2022

INDICE

CAPITOLO I

IL DELITTO DI RICICLAGGIO NELL'ORDINAMENTO PENALE ITALIANO: INQUADRAMENTO GENERALE

1.1 Il fenomeno del riciclaggio: profili economici.

Alla luce della fondamentale rilevanza che il delitto di riciclaggio riveste nel nostro ordinamento e tenendo conto del ruolo che esso ricopre in un sistema economico-sociale che si propone di essere sempre più trasparente, si ritiene necessario svolgere sin d'ora una breve premessa ai fini della presente trattazione.

In via di prima approssimazione e per motivi di chiarezza introduttiva, pare appropriato fornire una prima definizione di riciclaggio come un processo di ripulitura del denaro o di altri beni provenienti da attività illecite, i quali vengono reintrodotti nel circolo economico legale al fine di occultarne l'origine illecita e di trarre ulteriori guadagni, in apparenza, leciti.

Prima di addentrarsi nell'analisi prettamente giuridica del riciclaggio così come sanzionato all'art. 648 *bis* c.p., conviene innanzitutto soffermarsi brevemente sulla connotazione del riciclaggio come fenomeno economico-finanziario, fonte di effetti affatto trascurabili sia sotto un profilo

microeconomico che, secondo più ampie vedute, macroeconomico. A chi scrive sembra opportuno avviare il proprio esame, assumendo, in primo luogo, una prospettiva di tipo microeconomico, indagando la natura dell'approccio tipico del soggetto riciclatore di denaro, inteso come singolo agente economico.

Il tratto più peculiare della sua attività si sostanzia nel ricorso, di regola, ad un metodo di tipo razionale, basato su un'analisi comparativa tra costi e benefici, nella pianificazione ed esecuzione della sua attività criminosa. Più precisamente e secondo la scienza economica, nella funzione di utilità del potenziale criminale, i benefici sono rappresentati dal reddito prodotto dall'attività criminosa, mentre i costi sono determinati da due variabili: l'entità della sanzione e la probabilità che questa venga comminata.[1]

Le ragioni sottese a questo tipo di analisi costi-benefici sono da ricondursi al perseguimento della funzione economica tipica del riciclaggio – così come individuata dalla dottrina – *di trasformare potere d'acquisto potenziale* – in quanto i capitali illeciti non possono essere utilizzati direttamente per motivi di consumo, investimento o di risparmio – *in potere d'acquisto effettivo*[2]*,* grazie alla ripulitura degli stessi in capitale lecito. In questi termini, può dirsi che il riciclaggio svolga una c.d. *funzione monetaria illegale*[3].

Infatti, poiché, come sopra richiamato, l'approccio microeconomico allo studio del fenomeno di riciclaggio indirizza necessariamente all'osservazione del tipo di scelta compiuta dal soggetto criminale, è prioritario mettere in

[1] Per un'analisi approfondita del metodo criminale improntato alla razionalità, si rinvia al contributo dello studioso G.S. BECKER, *"Crime and Punishement: an economical approach*", in *Essays in the Economics of Crime and Punishment*, 1974, pp. 1-54.
[2] D. MASCIANDARO, "*Economia del riciclaggio e della politica antiriciclaggio*", in Giornale degli Economisti ed Annali di Economia, 1995, pp. 211-228. Sul punto si veda anche *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*, (a cura di) E. CAPPA e L.D. CERQUA, 2012, pp. 56 e ss.
[3] D. MASCIANDARO, *Riciclaggio dei capitali illeciti: profili di analisi economica*, in *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*., in (a cura di) E. CAPPA E L.D. CERQUA, 2012, pp. 15 e ss.

evidenza come ogni decisione sia ponderata sull'utilità derivante dall'azione criminosa. Detta utilità è decrescente quanto più risulta elevata la probabilità di scoperta del reato e della severità della sanzione, ma è crescente quanto più alto sia il rendimento realizzato attraverso la pulizia del denaro "sporco". L'obiettivo primario perseguito, quindi, dal soggetto criminale consiste nell'individuazione di un valore ottimale delle risorse da riciclare, valore che – se superato – comporta una perdita di convenienza nella realizzazione di attività di riciclaggio.

Da ultimo, nel quadro microeconomico appena – seppur brevemente – descritto, si deve tenere conto di un ulteriore fattore: la propensione a riciclare. Quest'ultima risulta legata da un forte nesso di dipendenza a molteplici parametri, primi tra i quali l'asprezza delle politiche antiriciclaggio, che naturalmente riduce tale propensione. *A contrario*, di fronte ad un vertiginoso aumento della redditività del denaro ripulito grazie ad investimenti a basso costo, la propensione a riciclare fisiologicamente cresce. Il punto di raccordo che consente di proseguire l'analisi in discorso sotto un profilo macroeconomico viene individuato nel momento di introduzione del denaro "sporco", una volta ripulito e per questo liberato dalla piaga dell'illegalità, nel circuito economico legale. Tale immissione nel sistema economico finanziario comporta, naturalmente, la produzione a catena di molteplici effetti negativi[4].

[4] Il Fondo monetario internazionale ha, sul piano macroeconomico, indicato come potenziali conseguenze del riciclaggio: a) le variazioni della domanda di capitali che non appaiono coerenti con le variazioni registrate nei fondamentali; b) la volatilità dei tassi di cambio e dei tassi di interesse a causa di trasferimenti di fondi transfrontalieri non previsti; c) la crescita della instabilità dei passivi e dei rischi per la qualità degli attivi delle istituzioni finanziarie (che creano, in generale, rischi di sistema per la stabilità del settore finanziario e per gli sviluppi monetari); d) gli effetti negativi sul gettito fiscale e sulla ripartizione della spesa pubblica a causa di un'errata valutazione del reddito e della ricchezza; e) gli effetti di contaminazione delle operazioni legali dovute alla preoccupazione degli operatori di un loro possibile coinvolgimento in ambienti criminali; f) gli effetti distributivi specifici su altri paesi e, cioè, l'effetto "*bolla*" dei prezzi degli attivi dovuti alla disponibilità di denaro sporco, v. *Macroeconomic Implication of Money Laundering*, Documento presentato alla riunione plenaria del GAFI del giugno 1996.

In primo luogo, si assiste all'allarmante ingresso nella dimensione economico-finanziaria legale di attori criminali.[5] Tale ingresso scatena a sua volta un ulteriore effetto – forse il più deleterio – che, come è stato correttamente messo in luce in seguito all'osservazione fenomenologica delle condotte di riciclaggio, minaccia violentemente il regolare funzionamento dei mercati. Si tratta, nello specifico, della violazione della *par condicio* tra operatori di mercato, con ciò intendendo che chi investe i proventi illeciti è posto in una condizione assai più vantaggiosa rispetto a chi deve procurarsi per vie lecite i mezzi necessari per le operazioni finanziarie.

Ne deriva che, a valle, il profitto finale dell'imprenditore inserito nel circuito legale risulti, dunque, danneggiato dal metodo criminale di gestione delle attività economiche[6]. In altre parole, ad essere sfalsato e alterato è il sistema concorrenziale tipico dell'economia di mercato: investire – a basso costo – denaro frutto di attività illecite nel circuito legale comporta l'eliminazione dal mercato di attori sani, non capaci di sostenere le condizioni concorrenziali così vantaggiose dei *competitors* criminali. Sul punto, non si può evitare di menzionare come queste attività criminose comportino necessariamente la lesione dei principi costituzionali posti a fondamento del c.d. libero mercato[7], così come tutelato *ex* art. 41 Cost.

Pur senza alcuna pretesa di esaustività, proseguendo con una breve analisi delle ricadute negative che il riciclaggio di denaro realizza sul versante economico, per ragioni di completezza è necessario segnalare la produzione del c.d. *effetto moltiplicativo del volume dell'attività economica afferente a soggetti criminali*[8].

---

[5] Sul punto, si veda V. MAIELLO, *Il riciclaggio: fenomenologia ed evoluzione della fattispecie normativa, sez. I, Il fenomeno criminale* in L. DELLA RAGIONE; V. MAIELLO (a cura di) *Riciclaggio e reati nella gestione dei flussi di denaro sporco, aggiornato al d.lgs. n. 90/2017*, 2018, pp. 4 e ss.

[6] Cfr. V. MAIELLO, *op. ult. cit.,* in L. DELLA RAGIONE, V. MAIELLO (a cura di) *op. ult. cit.*, p. 4 e ss.

[7] Sul punto, si veda anche V. MAIELLO, *op. ult. cit.* in L. DELLA RAGIONE; V. MAIELLO (a cura di) *op. ult. cit.* pp. 16 e ss.

[8] Cfr. D. MASCIANDARO, *op. ult. cit.,* p. 214.

Ad oggi, è ormai patrimonio comune e condiviso la consapevolezza che la liberalizzazione dei traffici commerciali e della circolazione dei beni abbia reso estremamente più agile e flessibile lo svolgimento di attività illecite, rendendo di certo non così difficoltosa la ricollocazione delle risorse illecite anche all'esterno del territorio nazionale. Infatti, non si può tralasciare come la globalizzazione, seppur si contraddistingua come fenomeno complessivamente molto positivo, presenti d'altronde alcune ambiguità. In altre parole, se da un canto, si connota come un'occasione unica per lo sviluppo economico e il miglioramento degli *standard* di vita dei popoli, aumentando le *performances* delle economie, grazie ad un'allocazione delle risorse maggiormente efficiente, dall'altro, se non adeguatamente governata, la globalizzazione "presenta rischi di destabilizzanti squilibri, di crescente iniquità distributiva tra Paesi e all'interno dei singoli Paesi".[9]

Sia guardando al fenomeno di riciclaggio sotto un profilo microeconomico che macroeconomico, sembra in ogni caso calzante poter attribuire al riciclaggio la caratteristica della poliedricità, potendo esso assumere – per l'appunto – le forme più disparate[10], e che è fonte a sua volta di una pluralità di effetti ed eventi che si riverberano oltre i confini di un solo Stato. Sul punto si osserva che "l'utilizzo di beni o altre utilità economiche di provenienza illecita, per il loro basso costo e per le caratteristiche dimensionali e transnazionali dei fenomeni delittuosi più significativi, a cui si ricollegano, può alterare l'assetto economico-finanziario di un Paese e, talvolta, di intere aree regionali"[11].

---

[9] Cfr. C. SANTINI, *Globalisation and Offshore Dimension – Building Integrity Confidence and Cooperation*, Relazione tenuta al *Nineteenth International Symposium on Economic Crime*, Cambridge, 12 settembre 2001, in *Journal of Money Laundering Control*, Volume V, n. 4, London, 2002.

[10] Sulle forme di riciclaggio, v. *infra* cap. I, par. 1.4 e, successivamente, cap. II.

[11] Così Banca d'Italia, Quaderni di Ricerca Giuridica, *Lineamenti della disciplina internazionale di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo*, n. 69, (a cura di) M. CONDEMI E F. DE PASQUALE, 2008, p. 15

Dunque, come sopra richiamato, connotandosi il riciclaggio dapprima come fenomeno economico e solo successivamente come delitto, giova osservare come questa impostazione abbia guidato anche gli interventi della comunità internazionale. Essa, infatti, ha agito in prima battuta sotto un profilo preventivo e solo in un momento successivo sotto un profilo repressivo-sanzionatorio.

A suffragio di quanto appena osservato, si veda la prima Risoluzione del Comitato dei Ministri del Consiglio d'Europa del 1980[12] in vista dell'attività di regolamentazione in materia di riciclaggio ove non si fece alcuna menzione degli aspetti penali del fenomeno. Solo in un momento successivo, con la Convenzione di Vienna del 19 dicembre 1988, finalizzata alla criminalizzazione del riciclaggio, si dispose che ciascuna parte – e dunque ciascuno Stato – dovesse adottare i provvedimenti necessari per "attribuire il carattere di reato" ad una serie di condotte, tra le quali figurano la conversione, il trasferimento, la dissimulazione o la contraffazione dell'origine (o delle altre circostanze) di beni che si conosce essere proventi di reati relativi al traffico di stupefacenti e di sostanze psicotrope.[13]

Nel tentativo di aver fornito un inquadramento introduttivo sugli essenziali aspetti economici del delitto di riciclaggio, a chi scrive pare opportuno procedere, al successivo paragrafo, con un accenno di tipo criminologico.

---

[12] Raccomandazione del Comitato dei Ministri del Consiglio d'Europa, 1980, *Misure contro il trasferimento e la custodia di fondi di origine criminale*, n. 80/10

[13] UN Convention against illicit traffic and narcotic drugs and phsychotropic substances, 2008, art. 2: "*In carrying out their obligations under the Convention, the Parties shall take necessary measures, including legislative and administrative measures, in conformity with the fundamental provisions of their respective domestic legislative systems*". Per un inquadramento sul panorama legislativo sovranazionale si veda *infra*, cap. I, par. 1.2.

1.2 Il fenomeno del riciclaggio: profili criminologici.

La scienza criminologica ha veicolato, come tratto distintivo del fenomeno di riciclaggio, il suo carattere trasversale[14] rispetto ad altre fattispecie criminose, ove per trasversalità del fenomeno, si intende una sua intrinseca attitudine ad intrecciarsi alle forme di criminalità organizzata, costituendo così una "considerevole area di intersezione per sovrapposizione"[15] tra criminalità organizzata ed economica.

Da principio, sia nell'assunzione di misure di contrasto al riciclaggio stesso sia nella strutturazione di programmi di propaganda politica, il reato di riciclaggio è sempre stato strettamente correlato alle attività realizzate da organizzazioni criminali, in particolare al traffico di stupefacenti. Dunque, come rilevato in dottrina[16], se negli anni è risultato compito assai arduo metabolizzare l'idea secondo la quale il riciclaggio sia un reato ampiamente diffuso, connesso in via tendenziale a qualunque delitto che sia strumentale alla realizzazione di risorse economiche e non solo al narcotraffico, ad oggi può dirsi che la consapevolezza della multiformità di tale reato si sia ampiamente consolidata.

Si è assistito, infatti, ad un mutamento del profilo criminologico del reato di riciclaggio che si è "evoluto" passando dall'essere fortemente connotato dalle caratteristiche tipiche di un'organizzazione criminale a presentare tratti molto più afferenti all'ambito economico-finanziario. Da ciò ne consegue che il reato di riciclaggio sia stato sempre più correlato ad una pluralità di reati

---

[14] Sul punto si veda A.M. DELL'OSSO, *Riciclaggio di proventi illeciti e sistema penale*, 2017, p. 21.; P.L.VIGNA, *Il fenomeno criminale*, in *op. ult. cit.*, a cura di E. CAPPA e L.D. CERQUA, 2012, pp. 3 e ss.

[15] C.E. PALIERO, *Criminalità economica e criminalità organizzata: due paradigmi a confronto,* in M. BARILLARO (a cura di), *Criminalità organizzata e sfruttamento delle risorse territoriali*, 2004, p. 145

[16] Si veda L. CUZZOCREA, *La ricostruzione del* paper trail *nelle indagini penali,* in (a cura di) M. ARNONE-S. GIAVAZZI, *Riciclaggio e imprese*. *Il contrasto alla circolazione dei proventi illeciti*, 2011, p. 75

presupposto dalla commissione dei quali derivano ingenti profitti da reintrodurre nel mercato legale.

Più precisamente, rifacendosi agli studi di due esperti americani, sono state individuate cinque categorie che racchiudono i principali reati presupposto: (i) narcotraffico; (ii) "blue collar crimes"; (iii) "white collar crimes"; (iv) corruzione; (v) terrorismo.[17]

Alla luce delle considerazioni interdisciplinari sin qui svolte, pur senza alcuna pretesa di esaustività, si ritiene ora necessario mutare la prospettiva di analisi del riciclaggio, non più considerandolo come "fenomeno", bensì propriamente come reato. Per questo, pare ora opportuno proseguire con un inquadramento più specificamente giuridico del delitto di riciclaggio, percorrendo le principali tappe della sua genesi ed evoluzione, a livello sovranazionale e nazionale, e sviscerandone, successivamente, i tratti tipici.

1.3 Le tre fasi del reato di riciclaggio.

Tutte le operazioni di riciclaggio, dalle più semplici alle più articolate, si svolgono secondo un procedimento standardizzato contraddistinto da un'intrinseca suddivisione in tre fasi (c.d. modello trifasico). Ciascuna fase è funzionale, all'esito del procedimento, a disperdere le tracce dell'origine delittuosa del denaro.

Il momento iniziale prende il nome di *placement* nella precisa accezione di "collocamento" delle risorse ottenute dal compimento del reato presupposto, come un furto o il traffico di droga, all'interno del sistema finanziario attraverso depositi bancari oppure unendole ai proventi di un

[17] P. REUTER, E.M. TRUMAN, *Chasing dirty money*, 2004, pp. 40 e ss. Si veda anche la classificazione in quattro categorie: (i) narcotraffico, (ii) evasione fiscale, (iii) terrorismo, (iv) reati di frode, contrabbando, appropriazione indebita, di E. TAKATS, *Domestic money laundering enforcement*, in D. MASCIANDARO, E. TAKATS, B. UNGER, *Black Finance* 2007, p. 197

business legittimo già in corso. Nonostante la forma di *placement* maggiormente considerata sia lo spostamento di contanti in un conto corrente bancario[18], non è tuttavia l'unica possibile.

Infatti, attraverso il collocamento si vogliono semplicemente allontanare i fondi dalla loro fonte originaria – illecita – in un'altra sede che permetterà al riciclatore di denaro di intraprendere ulteriori stratificazioni dei proventi illeciti mascherando la natura criminosa questi importi. Inoltre, non si può trascurare che, naturalmente, il riciclatore di denaro preferirà realizzare il collocamento in settori del sistema economico che siano sottoposti ai controlli meno invasivi da parte delle autorità. Questo comporta che qualora il riciclatore giunga a conoscenza della necessità di contanti da parte di determinate imprese o, talvolta, di banche che abbisognino di liquidità per incrementare i propri depositi, più facilmente si rivolgerà ad essi per avviare il procedimento di riciclaggio.[19] Il *core* di questa fase si ha nel momento in cui il denaro contante viene trasformato in moneta scritturale[20] destinata per sua natura a costituire saldi attivi presso intermediari finanziari. Si segnala che spesso nella prassi si ricorre alla tecnica del c.d. *smurfing*, il quale comporta l'esecuzione di versamenti frazionati, depositando le somme di denaro di provenienza illecita in più conti aperti presso il medesimo istituto bancario oppure presso banche diverse, avvalendosi di prestanome.

Volgendo lo sguardo alla seconda fase caratteristica del reato di riciclaggio, si deve qui parlare di *layering*, da intendersi come "stratificazione". Essa comporta una frenetica movimentazione del capitale, attraverso il ricorso a bonifici bancari, trasferimenti, prestiti e pagamenti al fine di rendere estremamente difficoltosa la riconduzione alla sua origine delittuosa e, da ultimo, far apparire "pulito" il capitale utilizzato.

---

[18] Cfr. D. COX, *Handbook of Anti-Money Laundering*, 2014, pag. 15
[19] Cfr. D. COX, *op.ult cit*., pp. 16-17
[20] R. RAZZANTE, *Il riciclaggio nella giurisprudenza. Normativa e prassi applicative*, 2011, pp. 43-44.

Più in particolare, al fine di ostacolare la tracciabilità dei proventi illeciti, si assiste ad uno spostamento degli stessi attraverso una pluralità di società, le c.d. società *off-shore* o, altrimenti, società fantasma, soggette a giurisdizioni diverse. L'esito di questa costante circolazione interrompe il legame con la fonte primaria dei proventi – per l'appunto, il reato presupposto. Nella casistica di reati di riciclaggio realizzati da criminali professionisti, si è registrato che i fondi illeciti possono circolare fino a dieci volte prima di essere immessi nel sistema bancario.[21]

Terza ed ultima fase del procedimento in analisi è nota con il nome di *integration*, nonché "investimento", il quale comporta l'immissione nel circuito economico legale del capitale illecito al fine di essere assimilato ad altri beni presenti nel mercato. L'obiettivo finale è far apparire questi fondi come legittimi, in modo tale da rendere compito assai arduo il poter distinguere tra denaro lecito e illecito. Tra i metodi più frequenti utilizzati dai riciclatori si rinviene il trasferimento di denaro da una *shell bank* – i.e. banca di comodo di proprietà dei riciclatori – ad una banca legittima. Ancora, i riciclatori di denaro possono alterare fatture al fine di attribuire un maggior valore a beni o servizi, al fine di spostare fondi da un paese all'altro. Da ultimo, si assiste anche alla creazione di società anonime in Paesi in cui il diritto alla segretezza bancaria è garantito.

Tra le tecniche a cui si ricorre con maggiore frequenza ai fini di realizzare quest'ultima fase, si deve far menzione in questa sede del c.d. *loan back*. Più precisamente, si tratta di un c.d. "prestito a se stesso" che assume connotati di liceità in quanto compiuto sotto le vesti di un lecito finanziamento che assicura una parvenza di legalità al denaro. Il soggetto interessato – o, alternativamente, il suo prestanome – offre, però, delle garanzie personali che per la maggior parte sono costituite dal denaro di provenienza illecita.

[21] Cfr. DENNIS COX, *op. ult. cit*., pag. 18

1.4 L'evoluzione normativa del riciclaggio. L'incidenza degli strumenti internazionali sulla fattispecie di cui all'art. 648 *bis* c.p.: dalla Convenzione di New York del 1961 alla Convenzione di Vienna del 1988.

Il primo strumento legislativo di contrasto al fenomeno di riciclaggio fa la sua comparsa nel panorama giuridico internazionale con la Convenzione Unica di New York, sottoscritta il 30 marzo 1961, per combattere il traffico di sostanze stupefacenti[22], il quale rappresentava al tempo la minaccia più temibile a livello globale. Tale Convenzione punisce, per la prima volta, le "operazioni finanziarie"[23] dolosamente compiute relativamente al traffico di sostanze stupefacenti e, naturalmente, volge alla repressione di ogni condotta finalizzata alla produzione e al traffico di dette sostanze.

Nel silenzio degli altri ordinamenti, il Legislatore italiano colse l'occasione presentatasi con la Convenzione di New York e, per primo, agì sul fronte repressivo, mosso dal devastante periodo storico corrente all'epoca in Italia, noto come "anni di piombo". L'emergenza connessa alla criminalità organizzata, seppur legata anche sul territorio italiano al traffico di stupefacenti, riguardava però più da vicino, sempre in Italia, un altro fenomeno criminale: la criminalità organizzata di tipo mafioso e terroristico[24].

Pertanto, non potendo il Legislatore restare indifferente di fronte ad un contesto economico-sociale così pericolosamente traviato, intervenne d'urgenza[25], figurando così come precursore della lotta al riciclaggio,

---

[22] LA CONVENZIONE UNICA SUGLI STUPEFACENTI, ratificata in Italia con l. 5 giugno 1974, n. 412.

[23] LA CONVENZIONE UNICA SUGLI STUPEFACENTI, art. 36, co.2, ii).

[24] Sul punto, V. PLANTAMURA, *Riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e confisca (artt. 648-bis, 648-ter e 648-quater)*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale, parte speciale*, vol. X, *I delitti contro il patrimonio*, 2011, p. 845.

[25] Nella Relazione al d.d.l. di conversione del d.l. 21 marzo 1978, n. 59, introduttivo del reato di riciclaggio nell'ordinamento italiano, viene spiegato, *ab initio*, come fosse indispensabile ricorrere alla decretazione d'urgenza per adottare "*misure dirette a prevenire e reprimere, con opportuna e immediata efficacia, le manifestazioni sempre più preoccupanti della*

seppure, all'epoca, la fattispecie delineata presentasse alcune differenze rispetto alla formulazione attuale.

Prima del 1978 non esisteva un'autonoma fattispecie di riciclaggio: lo spazio di tutela era coperto, seppur parzialmente, dalla ricettazione e dal favoreggiamento reale. Le fattispecie appena menzionate, tuttavia, seppure affini sotto un profilo di *ratio legis*, non si mostrarono sufficienti a fronteggiare il fenomeno sempre più dilagante della reintroduzione di denaro illecito nel circuito legale.

Fu così che il reato di riciclaggio fu introdotto con l'art. 3 del d.l. 21 marzo 1978, n. 59[26]. Nella formulazione originaria dell'art. 648 *bis*[27], rubricato *"Sostituzione di danaro o valori provenienti da rapina aggravata, estorsione aggravata, sequestro di persona a scopo di estorsione",* la *ratio* della disposizione si sostanziava nella repressione del riciclaggio di proventi derivanti da crimini connessi al terrorismo e alla criminalità organizzata, quali ad esempio il sequestro di persona o la rapina.

Proprio per quanto appena evidenziato, può dirsi che la formulazione della rubrica e della disposizione normativa suggeriscano, però, che l'ambito di applicazione della norma non fosse propriamente il contrasto al fenomeno del riciclaggio, ma quanto più che questa costituisse "*uno strumento di lotta, di tipo deterrente, nei confronti dei*

criminalità dilagante e del terrorismo". Sul punto, si veda *ex multis* S. FAIELLA, *Riciclaggio e crimine organizzato transnazionale,* 2009, pp. 16 e ss.

[26] Il d.l. fu poi convertito con modificazioni dalla L. 18 maggio 1978, n. 191. "*Conversione in legge, con modificazioni, del decreto-legge 21 marzo 1978, n. 59, concernente norme penali e processuali per la prevenzione e la repressione di gravi reati*", pubblicato in Gazzetta Ufficiale n. 137 del 19 maggio 1978.

[27] Si riporta di seguito, per facilità al lettore, il testo integrale dell'articolo in versione originaria: "*Chiunque, fuori dei casi di concorso nel reato, compie fatti o atti diretti a sostituire denaro o valori provenienti dai delitti di rapina aggravata, estorsione aggravata o sequestro di persona a scopo di estorsione con altro denaro o altri valori, al fine di procurare a sé o ad altri un profitto o di aiutare gli autori dei delitti suddetti ad assicurarsi il profitto del reato*".

reati presupposto"[28]. L'obiettivo dell'introduzione della disposizione in esame, sul cui raggiungimento però sono sorte molteplici perplessità, risiedeva propriamente nella volontà di conferire autonomia alla fattispecie criminosa, per sanzionare quelle condotte di "trasformazione" dei beni provenienti dai reati presupposto, che in precedenza erano ricompresi dalle previsioni sulla ricettazione e sul favoreggiamento.

I dubbi sulla *ratio* sottostante all'introduzione dell'art. 648 *bis* hanno a lungo interessato la dottrina[29], la quale ha di concerto sostenuto che fosse, invece, proprio la repressione dei reati presupposto il fine ultimo perseguito dal legislatore. Quanto appena statuito è deducibile, *a fortiori*, dalla conformazione originaria del delitto di riciclaggio come delitto "a consumazione anticipata": infatti, l'estensione della tutela a *fatti o atti diretti a sostituire denaro o valori* provenienti da reati presupposto[30] si configura come una vera e propria anticipazione della tutela, idonea ad estendersi anche a condotte puramente prodromiche alla ricettazione.

A suffragio di quanto appena evidenziato, non può sfuggire che, come rilevato dalla dottrina più autorevole[31], si decise di conformare la nuova fattispecie al reato di ricettazione, identificando quest'ultima come il *paradigma*[32] su cui strutturare il nuovo reato, quasi a volerne estendere il

---

[28] S. MOCCIA, *Impiego di capitali illeciti e riciclaggio: la risposta del sistema penale italiano*, in *Riv. it. dir. proc. pen*., 1995, p. 729. Sul punto si veda anche Cass. pen. sez. II, 30 giugno 1980, n. 2347 e Cass. Pen., sez. II, 19 settembre 1988, n. 1101.

[29] Cfr. P. MAGRI, *I delitti contro il patrimonio mediante frode,* in *Trattato di diritto penale. Parte speciale*, (diretto da) G. MARINUCCI, E. DOLCINI, vol. VII, tomo 2, 2007, pp. 419 ss.

[30] Sul punto si segnala Cass. Pen. sez. II, 5 giugno 2015, n.27806, per cui si ritiene che ad oggi sia sufficiente anche una provenienza "mediata" dei proventi illeciti. *Ex multis*, Cass. Pen., 20 giugno 2012, n. 36759; Cass. Pen. sez. II, 6 novembre 2009, n.47375.

[31] Cfr. M. ZANCHETTI*, Riciclaggio di denaro proveniente da reato*, 1997, p. 127 parla di "*filiazione della ricettazion*e"; G. PECORELLA, *Circolazione del denaro e riciclaggio*, in *Riv. It. Dir. e Proc. Pen*., 1991, p. 1222 parla di "*scorporazione dalla ricettazione*"; In A. A. DALIA, *L'attentato agli impianti e il delitto di riciclaggio,* 1982, pp. 66, 69 e 73 ss., si rileva che: «il delitto di "riciclaggio" si presenta come una particolare ipotesi di ricettazione per intromissione che può essere posta in essere non solo per fini di natura patrimoniale, tipici di questa figura di reato, ma anche allo scopo di eludere le investigazioni dell'autorità, aiutando gli autori di quei reati dai quali provengono denaro o valori a guadagnarsi il profitto del delitto» .

[32] A.M. DELL'OSSO, *op. ult., cit*., p. 63

campo di applicazione e inasprire il profilo sanzionatorio. Non è opera difficile, infatti, riscontrare i numerosi punti in comune tra la fattispecie di riciclaggio, così come delineata nella sua formulazione originaria, e il delitto di ricettazione: in via esemplificativa, può dirsi come condividano il bene giuridico tutelato[33] e la clausola di esclusione per i casi di concorso nella realizzazione del reato presupposto. Per concludere, può dirsi che il reato di riciclaggio nella sua formulazione originaria si presentava come autonomo, ma solo formalmente, essendo ancora fortemente connesso al delitto di ricettazione.[34] Proseguendo nella disamina evolutiva della fattispecie in analisi, e nel tentativo di procedere in ordine cronologico tra fonti nazionali e sovranazionali, così come richiamato al paragrafo precedente, nel 1988, a Vienna fu stipulata la Convenzione delle Nazioni Unite contro il traffico illecito di stupefacenti e sostanze psicotrope, la quale fu ratificata in Italia con la l. 19 marzo 1990, n. 55, che recepì la Convenzione, dando esecuzione alle previsioni in essa previste, in linea con il fine ultimo perseguito dalla Convenzione stessa, ossia "privare coloro che praticano il traffico illecito del frutto delle loro attività criminali ed eliminare in tal modo il loro movente principale"[35]. Nonostante la presa di posizione da parte della comunità internazionale non fosse ancora così decisa e, per questo, certamente perfezionabile, non si può non notare che fu la prima volta che sul piano sovranazionale si decise di pronunciarsi e provvedere contro la minaccia sempre più crescente rappresentata dal fenomeno riciclatorio.

[33] Vedi *infra* al par. 1.3, cap. I

[34] Sul punto, è stato evidenziato che tra gli atti o fatti punibili ai sensi dell'art. 648 *bis* c.p. così come formulato *ab origine* dal legislatore, vi erano condotte in precedenza configurabili come ricettazione per intromissione o tentata ricettazione. Fra gli altri: S. FAVA, *Il reato di riciclaggio* (intervento al seminario *Criminalità economica, economia criminale,* Roma, 27-28 maggio 2011) in *Quest. Giust.*, 2012, 4, p. 122; cfr. anche il commento all'art. 648 *bis* c.p. di A. GALLUCCIO, M. C. UBIALI, in G. MARINUCCI, E. DOLCINI, *Codice penale commentato*, tomo 3, 2021, pp. 2833 e ss.

[35] Così recita l'art. 1 della Convenzione di Vienna del 1988.

Fu così che grazie ad un aumento di consapevolezza intorno alla pericolosità del riciclaggio, il legislatore italiano sfruttò a pieno l'occasione fornita dalla Convenzione di Vienna del 1988 e con l'art. 23 della legge di recepimento, richiamata *supra*, intervenne modificando l'assetto originario della norma di cui all'art. 648-*bis* c.p.: per la prima volta comparve la rubrica «*riciclaggio*» in capo all'articolo. Furono apportate diverse modifiche alla formulazione originaria della fattispecie, soprattutto alla luce dell'art.3 della Convenzione di Vienna, il quale prevede che ciascuna Parte contraente della Convenzione debba "attribuire il carattere di reato, conformemente con la sua legislazione nazionale, qualora l'atto sia stato commesso intenzionalmente alla conversione o al trasferimento dei beni, effettuati con la consapevolezza che provengono da uno dei reati stabiliti (…) [produzione e traffico di stupefacenti, n.d.r.] o dalla partecipazione alla sua perpetrazione, al fine di dissimulare o di contraffare l'origine illecita di detti beni o di aiutare qualsiasi persona implicata nella perpetrazione di uno di tali reati a sfuggire alle conseguenze legali dei suoi atti, alla dissimulazione o alla contraffazione della reale natura, origine, luogo, disposizione, movimento o proprietà dei beni o relativi diritti, il cui autore sa essere proveniente da uno dei reati (…) o dalla partecipazione a uno di questi reati".

1.5 (Segue) L'evoluzione normativa del riciclaggio: dalla Convenzione di Strasburgo del 1990 all'attuale formulazione della fattispecie.

In forza del recepimento della Convenzione di Vienna del 1988, si assistette ad una vera e propria trasformazione del reato di riciclaggio: esso perse la sua originaria configurazione di "reato a consumazione anticipata", essendo stato eliminato il riferimento a "atti o fatti diretti a (…)", e assunse

la fisionomia di "reato-ostacolo". Questa accezione, certamente valida ed utilizzabile sino ad oggi, veicola sinteticamente la funzione dissimulatoria del riciclaggio al fine di impedire o rendere notevolmente difficoltosa la tracciabilità e la provenienza del denaro o di altre utilità dai reati presupposto. Infatti, fu estesa la sfera dei reati presupposto del riciclaggio, destinato – per l'appunto – a includere tutti i reati legati alla produzione e al traffico di sostanze stupefacenti o psicotrope e parimenti a incriminare l'occultamento della provenienza di denaro, beni o altre utilità derivanti dai reati-presupposto.

Il legislatore focalizzò così la sua attenzione non più sull'azione di contrasto, in via quasi esclusiva, dei reati presupposto, bensì estese l'oggetto materiale del reato a "denaro, beni o altre utilità" e intervenne anche prevedendo la realizzazione alternativa di condotte di sostituzione di denaro o altre utilità e dissimulazione della loro provenienza illecita.

Da ultimo, per ragioni di mera completezza, si segnala che con la l. 55/1990 di recepimento della Convenzione di Vienna, fu introdotto nell'ordinamento italiano il delitto di "*Impiego di denaro, beni o altre utilità di provenienza illecita*" ex art. 648 *ter* c.p., a cui però si fa semplice riferimento nella presente trattazione, per limiti imposti dalla brevità del presente inquadramento generale sul delitto di riciclaggio[36].

Proseguendo la rassegna dei principali interventi in materia di riciclaggio che si sono susseguiti nel panorama internazionale, giova ora prestare attenzione ai primi interventi di contrasto che hanno indotto le istituzioni dell'Europa Unita a prendere una ferma posizione contro il continuo dilagare del riciclaggio. Il primo tra questi si ebbe il 27 giugno 1980, con la Raccomandazione n. 80/2010, intitolata "*Misure contro il trasferimento e la*

[36] Per una disamina dell'art. 648 *ter* si rinvia a V. PLANTAMURA, *op. ult. cit.*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale, parte speciale*, vol. X, *I delitti contro il patrimonio*, 2011, pp. 850 e ss.; F. MANTOVANI, *Diritto penale – parte speciale*, *Delitti contro il patrimonio*, Vol. II, 2021, pp. 301 e ss.

custodia di fondi di origine criminale". Con questo intervento, i legislatori nazionali furono collettivamente chiamati ad intervenire in ottica preventiva contro l'ingresso dei capitali illeciti all'interno dei sistemi finanziari di ciascuno Stato, migliorando la cooperazione in punto di scambio di informazioni, sia sul piano nazionale che sovranazionale, tra istituti di credito e autorità. Successivamente, l'8 novembre del 1990, il Consiglio d'Europa adottò la "*Convenzione di Strasburgo sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi del reato*"[37].

La portata innovativa della Convenzione si racchiude nell'aver scardinato ciò che fino a quel momento era sempre stato un elenco tassativo di reati presupposto, sostituendolo con una formulazione più generica ma per questo idonea a ricomprendere ogni condotta di conversione o trasferimento, occultamento della provenienza e acquisto o impiego di beni di provenienza illecita.[38]

Nel medesimo anno, furono emanate anche le note 40 Raccomandazioni del FATF/GAFI, cioè il Financial Action Task Force o Gruppo di Azione Finanziaria Internazionale[39]. Tale organismo intergovernativo, costituito per

[37] La menzionata Convenzione fu recepita nell'ordinamento italiano con considerevole ritardo il 9 agosto 1993, con la l. n 328.

[38] Cfr. art. 6, co.1 Convenzione di Strasburgo, di seguito riportato per esteso: "*Ciascuna Parte prende le misure legislative e di altra natura eventualmente necessarie per prevedere come reato secondo la propria legge interna, quando il fatto è commesso intenzionalmente: a. la conversione o il trasferimento di valori patrimoniali, sapendo che essi sono proventi, allo scopo di occultare o dissimulare l'illecita provenienza dei valori patrimoniali stessi o aiutare persone coinvolte nella commissione del reato principale a sottrarsi alle conseguenze giuridiche dei loro atti; b. l'occultamento o la dissimulazione della natura, dell'origine, dell'ubicazione, di atti di disposizione o del movimento di valori patrimoniali, nonché dei diritti di proprietà e degli altri diritti ad essi relativi, sapendo che detti valori patrimoniali sono proventi; e, fatti salvi i suoi principi costituzionali e i concetti fondamentali del suo ordinamento giuridico: c. l'acquisizione, il possesso o l'uso di valori patrimoniali sapendo, nel momento in cui sono ricevuti, che essi sono proventi; d. la partecipazione nella commissione di reati che sono stati previsti a norma del presente articolo, l'associazione o il complotto, allo scopo di commettere tali reati, il tentativo di commetterli, nonché l'assistenza, l'istigazione, il favoreggiamento e la prestazione di consigli per la loro commissione."*

[39] Fu costituito nel 1989 a Parigi, in occasione del quindicesimo summit dei Paesi del G7. Sin dalla sua nascita, fu però da subito aperto all'adesione da parte di altri Stati – quali Australia, Austria, Belgio, Lussemburgo, Olanda e Spagna.

rafforzare l'azione di contrasto al riciclaggio sullo scenario internazionale, svolge ad oggi le seguenti funzioni: in primo luogo, stila annualmente un *report* sulle misure antiriciclaggio – le 40 Raccomandazioni[40] furono inserite nella parte finale del rapporto annuale del 1990. *In secundis*, il GAFI deve svolgere un'azione di sorveglianza sul quadro legislativo di ciascuno Stato, redigendo delle c.d. "Schede Paese"; ancora, deve segnalare alle Autorità nazionali e internazionali ogni sviluppo in punto di sopravvenute tecniche di riciclaggio, avendo cura di strutturare un sistema di dialogo tra Stati ai fini di una incisiva ed omogenea propagazione della disciplina antiriciclaggio.[41]

Alla luce di questi interventi e sollecitazioni, il Consiglio delle Comunità Europee decise, dunque, di agire anch'esso con ulteriore forza perseguendo l'obiettivo di rafforzare nettamente la tutela contro il riciclaggio: nel 1991, fu emanata la Direttiva 308/91/CEE[42]. Si tratta della Prima Direttiva antiriciclaggio, della quale si menziona per importanza, la previsione, come attività necessaria, di garantire che gli enti creditizi e finanziari esigessero l'identificazione dei clienti che allacciassero rapporti di affari o eseguissero operazioni superiori ad un certo valore, onde evitare che coloro che procedono al riciclaggio approfittino dell'anonimato per svolgere le proprie attività criminose.[43]

---

[40] Tali Raccomandazioni subirono poi alcune modifiche nel 1996 e nel 2001, successivamente furono riscritte *in toto* nel 2003. In seguito, si dà conto in questa sede che tali Raccomandazioni sono state riformulate nel 2012 e aggiornate nel 2022. Per il testo integrale, si rinvia il lettore al sito www.fatf-gafi.org.

[41] V. PLANTAMURA, *op. ult. cit.*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale parte speciale vol X: i delitti contro il patrimonio*, 2011, pp. 850 e ss.

[42] La direttiva in analisi è stata recepita in Italia con l'art. 15 della legge 6 febbraio 1996, n. 52 (c.d. legge comunitaria) e con i decreti legislativi 26 maggio 1997, n. 153 e 25 settembre 1999, n. 374.

[43] Cfr. art. 3, direttiva 308/91/CEE. Per un'analisi dettagliata della Direttiva in discorso, si rinvia a F. SCAPELLATO, *Il fenomeno del riciclaggio e la normativa di contrasto*, 2013 pp. 26 e ss.

In estrema sintesi, può dirsi che gli obiettivi perseguiti dalla direttiva siano stati due[44]: incrementare gli obblighi di trasparenza nel mercato finanziario e intercettare operazioni sospette a fini preventivi. Circondato da interventi di primaria rilevanza, il Legislatore italiano il 9 agosto 1993, con la l. n 328, recepì la Convenzione di Strasburgo modificando ulteriormente la fattispecie ex art. 648 *bis* c.p.[45]

Le modifiche apportate furono sostanzialmente di due tipi: da un lato, fu eliminato l'elenco tassativo dei reati-presupposto e fu adottata una formula più generica ed onnicomprensiva che comprende qualsiasi delitto – ora, come si dirà, anche colposo – da cui possano derivare proventi illeciti, dall'altro, sempre in ottica di estensione di tutela, accanto alle due condotte tipiche della sostituzione e del trasferimento, fu inserita una formula aperta di "altre operazioni" volta a ricomprendere qualsiasi altra condotta innominata realizzata per ostacolare l'identificazione dell'origine delittuosa dei beni.

Per concludere l'inquadramento sulla produzione sovranazionale, si fa di seguito breve cenno all'azione sul piano euro unitario di contrasto al riciclaggio: complessivamente sono state emanate, ad oggi, sei direttive antiriciclaggio. La Prima Direttiva, di cui si è esposto *supra*, fu in seguito modificata con la c.d. Seconda Direttiva antiriciclaggio n. 97, emanata il 4 dicembre 2001. Si ritenne necessario intervenire ulteriormente alla luce della costante trasformazione delle tecniche criminali applicate per ripulire il denaro "sporco". Questa Seconda Direttiva ha il merito di aver esteso il novero dei reati presupposto e dei soggetti obbligati a collaborare con le autorità per contrastare il fenomeno del riciclaggio. Più precisamente, la disciplina antiriciclaggio fu estesa a tutte quelle attività e professioni di

[44] A.R. CASTALDO, M. NADDEO, *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio,* 2010, pp. 34 e ss.

[45] La disposizione è stata poi modificata con il d.lgs. n. 195, 8 novembre 2021, emanato in attuazione della Direttiva (UE) 2018/1673 del Parlamento europeo e del Consiglio, del 23 ottobre 2018 in tema di lotta al riciclaggio mediante diritto penale, di cui si darà conto al par. 1.5.1 del presente Capitolo.

carattere anche non finanziario, come ad esempio avvocati, notai e commercialisti

Ulteriori contributi migliorativi in materia di prevenzione al riciclaggio, furono poi introdotti con la c.d. Terza Direttiva antiriciclaggio, emanata il 26 ottobre 2005, relativa "alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo".[46] Con questo più recente intervento venne abrogata la Prima Direttiva antiriciclaggio, nel tentativo di raggiungere una maggiore tutela del mercato unico. Sotto un profilo più tecnico, furono rafforzati gli obblighi di identificazione della clientela, imponendo un controllo adeguato e azioni di accertamento dei soggetti agenti, dello scopo perseguito con l'operazione realizzata per tutto il periodo di durata del rapporto.

La produzione regolamentare delle istituzioni europee in contrasto al riciclaggio non si è, però, fermata alla Terza Direttiva. Si è proseguito, infatti, con ulteriori tre Direttive, sempre incentrate sulla prevenzione e vigilanza contro il delitto di riciclaggio: la Direttiva UE 2015/849 e la Direttiva UE 2018/843 per la cui trattazione più estesa si rinvia al capitolo III del presente elaborato, al fine di analizzare e sviscerare il puntellato tema della normativa antiriciclaggio connessa all'utilizzo di strumenti di recente introduzione, quali le criptovalute e, più nello specifico per la presente trattazione, i Bitcoin. Per completare il breve inquadramento della cornice normativa sul piano sovranazionale, deve essere menzionata anche la Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante diritto penale, che è stata recepita nell'ordinamento italiano con il d. lgs. n. 195/2021 e di cui si darà contro nell'immediato prosieguo della trattazione.

[46] Direttiva 2005/60/CEE

1.5.1 (Segue) La Direttiva (UE) 2018/1673 e il suo recepimento nell'ordinamento italiano con il d. lgs. n. 195/2021.

Non può trascurarsi in questa sede di dar conto del più recente intervento normativo sia sul piano sovranazionale che domestico, che ha condotto ad una modifica della disciplina del reato di riciclaggio *ex* art. 648 *bis* e di autoriciclaggio *ex* art. 648 *ter*.1 c.p.

Prendendo avvio da quanto disposto dal Legislatore eurounitario, con la Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale, è utile in prima battuta appellarsi ad alcuni considerando, che permettono di cogliere con chiarezza la *ratio* e l'urgenza di un simile intervento.

Infatti, rilevato come il delitto di riciclaggio e il finanziamento del terrorismo e la criminalità ad esso connessi siano lesivi per l'integrità, la stabilità e la reputazione del settore finanziario e costituiscano una minaccia per il mercato interno e la sicurezza interna dell'Unione, in apertura della Direttiva in analisi, al considerando numero 1), si dichiara come essa sia finalizzata a "*contrastare il riciclaggio tramite il diritto penale, consentendo una cooperazione transfrontaliera fra le autorità competenti più efficiente e più rapida*". Tale fonte normativa si rende promotrice di un approccio di cooperazione e di collaborazione anche specificamente nei confronti del GAFI e di tutte le altre organizzazioni e organismi internazionali attivi nella lotta contro il riciclaggio e il finanziamento del terrorismo[47].

Ancora, notevole importanza connota il considerando n. 7), il quale sottolinea come, alla luce delle ricadute negative per la sfera pubblica e per l'integrità delle istituzioni pubbliche, dei reati di riciclaggio realizzati da soggetti che ricoprono cariche istituzionali, ciascuno Stato membro dovrebbe avere la possibilità di introdurre nei propri ordinamenti delle sanzioni più severe per i titolari di cariche pubbliche.

[47] Si veda il considerando n. 3) della Direttiva (UE) 2018/1673.

Le principali novità della Direttiva in discorso possono essere sintetizzate, in via generale, richiamando in primo luogo la previsione *ex* art. 3, in tema di reati di riciclaggio. In particolare, si dispone un'elencazione molto dettagliata delle condotte che si richiede agli Stati siano sanzionate, qualora siano realizzate intenzionalmente[48].

Inoltre, viene prevista la possibilità di sanzionare il delitto di riciclaggio come reato colposo: precisamente, si dà l'opportunità agli Stati di sanzionare tutti i casi in cui l'autore del reato sospettava o avrebbe dovuto essere a conoscenza che i beni provenivano da un'attività criminosa. Da ultimo, nella Direttiva in analisi, vengono anche previste nuove norme in materia di giurisdizione e litispendenza volte a rendere più rapida ed efficiente la cooperazione transfrontaliera tra le autorità[49].

La Direttiva di cui si è appena dato breve conto è stata recepita nell'ordinamento italiano con il d. lgs. n. 195 del 2021[50], il quale ha apportato notevoli modifiche – e molto mirate – alla disciplina di riciclaggio, di cui si darà un breve inquadramento nel prosieguo della trattazione. Infatti, nella relazione illustrativa del d.lgs. in commento, il Legislatore ha precisato che l'ordinamento italiano era "già largamente conforme alle disposizioni contenute nella Direttiva (UE) 2018/1673" e che, dunque, con la norma di

[48] Trattasi, precisamente delle seguenti condotte: a) la conversione o il trasferimento di beni, effettuati essendo nella consapevolezza che i beni provengono da un'attività criminosa, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche della propria condotta; b) l'occultamento o la dissimulazione della reale natura, della provenienza, dell'ubicazione, della disposizione, del movimento, della proprietà dei beni o dei diritti sugli stessi nella consapevolezza che i beni provengono da un'attività criminosa; c) l'acquisto, la detenzione o l'utilizzazione di beni nella consapevolezza, al momento della loro ricezione, che i beni provengono da un'attività criminosa.

[49] M.A. MORABITO, *Lo schema di decreto legislativo per l'attuazione della direttiva UE 2018/1673 sulla lotta al riciclaggio mediante il diritto penale: analisi e considerazioni*, in Giurisprudenza penale Web, 9, 2021, p. 2

[50] Pubblicato in G.U. n. 285, 30 novembre 2021. Si segnala, inoltre, che il d. lgs. 8 novembre 2021, n. 195 è stato introdotto con urgenza in seguito alla comunicazione da parte della Commissione europea nei confronti dell'Italia dell'avvio di un procedimento di infrazione per il mancato recepimento della Direttiva (UE) 2018/1673 scaduto il 3 dicembre 2020.

recepimento si è provveduto soltanto all'inserimento di "interventi di dettaglio, volti a estendere il campo di applicazione di alcune norme nazionali già esistenti"[51].

La norma di recepimento interna si pone in continuità con gli obiettivi della normativa eurounitaria, ma si connota per una struttura "puntiforme", avendo apportato delle modifiche minimali sulle fattispecie riformate[52].

Più precisamente, la novella in discorso è stata foriera di alcune rilevanti novità relativamente ai reati di riciclaggio e autoriciclaggio. In primo luogo, una novità di non trascurabile importanza, concerne l'introduzione della punibilità per reato di riciclaggio anche nel caso di reato presupposto costituito da delitto colposo, contrariamente a quanto previsto ai sensi della normativa precedente. *In secundis,* il Legislatore ha esteso il novero dei reati presupposto di ricettazione, riciclaggio, reimpiego e autoriciclaggio alle contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi, prevedendo in questo caso una risposta sanzionatoria più lieve. Sul punto, attenta dottrina[53] ha messo in luce come anche relativamente ai beni derivanti da contravvenzioni, siano applicabili i medesimi criteri già delineati dalla giurisprudenza in relazione ai reati presupposto: ciò comporta che le c.d. contravvenzioni-presupposto rilevino sia se siano dolose che colpose.

1.6 Il delitto di riciclaggio *ex* art. 648 *bis* c.p.: il bene giuridico tutelato.

Alla luce delle considerazioni appena svolte in tema di evoluzione normativa del reato di riciclaggio, sia sotto un profilo sovranazionale che

[51] Relazione illustrativa al d.lgs. 8 novembre 2021, n. 195, p. 4.

[52] G. PESTELLI, *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 12/2021, p. 50.

[53] G. PESTELLI, *op. ult. cit*., p. 52

nazionale, è necessario affrontare l'annosa questione del bene giuridico tutelato dalla disposizione ex art. 648-bis c.p.[54]

Limitandosi, in prima battuta, ad osservare che la fattispecie del delitto di riciclaggio è stata inserita nel titolo XIII del Libro II del Codice Penale, e dunque tra i delitti contro il patrimonio, sembrerebbe quasi naturale potersi limitare ad individuare il bene giuridico tutelato semplicemente nel patrimonio e, pertanto, la questione potrebbe, *prima facie*, risultare scevra da ogni tipo di problematica.

Tuttavia, ad oggi, la dottrina maggioritaria esclude che il patrimonio sia realmente il bene giuridico tutelato ex art. 648-bis c.p. *A fortiori*, l'offesa al patrimonio, provocata dal riciclaggio, emerge e rileva solo in via secondaria, potendo anche mancare la realizzazione di un vero e proprio danno economico.

Dunque, soprattutto alla luce delle sopravvenute modifiche normative interne e comunitarie, si è resa necessaria una rilettura del concetto di patrimonio che ha condotto, in seguito alla classificazione del reato di riciclaggio come "reato-ostacolo", ad attribuire un valore preponderante, tra i beni tutelati, all'amministrazione della giustizia. Questo ruolo primario assegnatole si fonda sull'osservazione per cui la fattispecie ex art. 648-bis c.p. incrimina qualsiasi condotta volta ad ostacolare l'identificazione della provenienza illecita del denaro o di altri beni o utilità (c.d. *paper trail*)[55]

[54] Per completezza, si riporta di seguito il testo integrale dell'art. 648 *bis* c.p.: "Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000.

La pena è della reclusione da due a sei 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.

La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale.

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.

Si applica l'ultimo comma dell'articolo 648."

[55] Una definizione precisa di *paper trail* può aversi in "pista di carta che, documentando i trasferimenti e le sostituzioni dei proventi illeciti, permette di risalire alla fonte e a

concretizzandosi dunque in un ostacolo per l'autorità giudiziaria nell'azione di accertamento dei reati e nella ricerca dei soggetti responsabili.

In dottrina, deve però segnalarsi la formazione di un orientamento che può dirsi contrario a quanto appena esposto. In particolare, tale corrente di pensiero ha posto a fondamento della propria elaborazione la caratteristica, ritenuta intrinseca alla fattispecie di riciclaggio, della c.d. polifunzionalità del riciclaggio, la quale a sua volta si manifesta in una disgregazione dei beni giuridici protetti[56]. Più precisamente, ricorrendo ad un'interpretazione quanto più estensiva del concetto di patrimonio, tale orientamento vi ha ricompreso una pluralità di beni giuridici da tutelare, quali la concorrenza, l'economia pubblica, il regolare funzionamento dei mercati, la buona amministrazione della giustizia e la tutela del risparmio.[57]

Ancora, è doveroso segnalare come tra i tentativi di e individuazione del bene giuridico tutelato, sempre in dottrina si sia fatto ricorso ad una divisione di categorie tra beni giuridici strumentali e beni giuridici finali[58]. Fedelmente a questo orientamento, può dirsi che l'amministrazione della giustizia figurerebbe come bene strumentale, mentre l'ordine pubblico ed economico – all'interno dei quali sarebbero peraltro ricompresi altri beni, come la tutela del risparmio, del libero mercato e della concorrenza – figurerebbero come beni finali. In quanto tali, la loro integrità risulterebbe solamente minacciata

documentarne l'origine delittuosa", tratta da L.D. CERQUA, *Il delitto di riciclaggio di proventi illeciti*, in *op. ult. cit. (a cura di)* E. CAPPA E L.D. CERQUA, *2012,* pp. 55 e ss.

[56] L. DELLA RAGIONE; V. MAIELLO (a cura di) *op. ult. cit.,* p. 62

[57] A suffragio di questa visione, si esprimono: M. ANGELINI, *Il reato di riciclaggio (art. 648 bis c.p.). Aspetti dogmatici e problemi applicativi*, 2008, p. 19 ss.; P. MAGRI, *I delitti contro il patrimonio mediante frode,* in *Trattato di diritto penale. Parte speciale*, diretto da G. MARINUCCI, E. DOLCINI, vol. VII, tomo 2, 2007, 426 ss.; V. PLANTAMURA, *Tipo d'autore o bene giuridico tutelato per l'interpretazione, e la riforma, del delitto di riciclaggio?*, in *Riv. trim. dir. pen. econ*., 1-2, 2009, p. 165 ss.

[58] Cfr. A. MANNA, *Il bene giuridico tutelato nei delitti di riciclaggio e reimpiego: dal patrimonio all'amministrazione della giustizia, sino all'ordine pubblico e all'ordine economico*, in AA. VV. *Riciclaggio e reati connessi all'intermediazione finanziaria*, (a cura di) A. MANNA, 1999, p. 53 e ss.

a seguito della realizzazione del delitto di riciclaggio, mentre invece l'offesa vera e propria colpirebbe direttamente il bene giuridico strumentale, ossia l'amministrazione della giustizia. Avendo dunque ripercorso, seppur brevemente, le tappe principali del procedimento di individuazione del bene giuridico oggetto di tutela, può dunque concludersi, a fondamento delle ragioni appena esposte, che sia accoglibile con favore la tesi che individua nell'amministrazione della giustizia il bene preminente tutelato.

1.6.1 La condotta tipica.

La disposizione ex art. 648 *bis* c.p. si configura come norma mista alternativa o, altrimenti, norma a più fattispecie[59] in quanto il reato può realizzarsi attraverso l'attuazione, alternativa, di ciascuna condotta indicata dalla norma e, parimenti, il reato rimane unico qualora vengano attuate anche più tra le condotte previste.

La norma indica, nello specifico, tre condotte criminose: la sostituzione, il trasferimento e il compimento di altre operazioni in modo da ostacolare l'individuazione della provenienza illecita di beni o altre utilità che provengano dalla realizzazione del delitto presupposto.

Al fine di una maggiore comprensione del delitto in analisi, non si può trascurare la definizione specifica che è stata attribuita ad ogni singola condotta. In primo luogo, a chi scrive pare opportuno procedere in via ordinata affrontando l'esame della condotta di *sostituzione* del denaro, di beni o di altre utilità di provenienza delittuosa, resa dalla dottrina maggioritaria come azione volta a *rimpiazzare un bene iniziale con un bene finale*[60]. Si

[59] A. DELL'OSSO, *Riciclaggio di proventi illeciti e sistema penale,* 2017, p. 104;
[60] A. DELL'OSSO, *op. ult. cit*., p. 104. *Ex multis*, cfr. G. FIANDACA-E.MUSCO, *Diritto penale. Parte speciale*, 2015 p. 262; C. LONGOBARDO, *Riciclaggio (art. 648-bis c.p)* in *I reati contro il patrimonio,* (a cura di) S. FIORE, 2010, p. 848; F. MANTOVANI, *Diritto penale. Delitti contro il patrimonio*, 2012, p. 283.

tratta, in via più estesa, di operazioni bancarie, finanziarie, commerciali – quali il deposito bancario e il successivo ritiro del denaro, acquisto e vendita di materie prime – attraverso le quali il denaro o il bene di provenienza illecita viene rimpiazzato con altro denaro o bene "pulito"[61].

Anche in giurisprudenza sono rinvenibili riscontri definitori con riguardo alla condotta di sostituzione, accolti e condivisi anche dalla dottrina. In particolare, la sostituzione si configurerebbe come condotta a struttura bifasica, scandita in un momento ricettivo e in un momento sostitutivo. In altre parole, riprendendo quanto recepito in giurisprudenza si dovrebbe parlare di un *flusso finanziario "di andata" e uno corrispondente "di ritorno"*. Ancora, sempre tra le pronunce della Suprema Corte, sono rinvenibili ulteriori definizioni, tra le quali si riporta la seguente, che a chi scrive pare meritevole di menzione per completezza: "*per sostituzione, deve intendersi la condotta posta in essere sul denaro, bene od utilità di provenienza delittuosa, specificamente diretta alla sua trasformazione parziale o totale ovvero ad ostacolare l'accertamento sull'origine della "res", anche senza incidere direttamente, mediante alterazione dei dati esteriori, sulla cosa in quanto tale."*[62]

La seconda condotta presa in considerazione dall' art. 648 *bis* c.p. è il trasferimento dei proventi criminosi, che costituisce una specificazione dell'attività di sostituzione. In tal caso, così come descritta dalla dottrina, tale condotta si sostanzia nello "*spostare il provento delittuoso, nell'identica composizione qualitativa, nel patrimonio altrui, attraverso gli strumenti ripulitivi negoziali o, comunque giuridici*"[63]. Naturalmente, il fine ultimo perseguito è quello di far perdere le tracce della provenienza dei proventi

[61] Sul punto si veda Cass. pen. sez V, 1° ottobre 1996, la quale fornisce una definizione di sostituzione come "*rendere diverso il bene ricevuto*", con ciò intendendo la sostituzione di denaro o altri beni "sporchi" con altri "puliti".
[62] Così Cass. pen., sez II, 11 aprile 2014, n. 1771.
[63] F. MANTOVANI, *op. ult. cit.* p. 272

delittuosi, trattandosi, nella sostanza, di uno spostamento dei proventi da un titolare ad un altro.

La questione interpretativa che più ha interessato tale definizione e che è stata fonte di contrasti dottrinali – seppur con una rilevanza pratica marginale – riguarda l'accezione di trasferimento in senso giuridico e quindi da intendersi come trasferimento della titolarità del bene ovvero, diversamente, in senso puramente fisico. Ad oggi, si ritiene in via prevalente che l'accezione di trasferimento sia da intendersi in senso giuridico, come traslazione interpersonale della proprietà o del possesso della *res*.[64] In via contrapposta, l'accezione di trasferimento fisico, o materiale, è invece il frutto di elaborazioni afferenti quanto più ad un'analisi di tipo criminologico del riciclaggio, fondata sul rilievo per cui anche uno spostamento puramente materiale del bene può essere d'impedimento alla tracciabilità della sua provenienza.

Ad unire queste due posizioni conflittuali, è intervenuta la giurisprudenza, la quale ha dato vita ad un orientamento comprensivo di entrambe le accezioni sopra esposte della condotta di trasferimento. Se dimostratasi favorevole ad intendere il trasferimento in senso propriamente giuridico, essa non ha però escluso la sua attuabilità anche sotto un profilo materiale, adducendo che "*integra il delitto di riciclaggio anche il mero trasferimento di un bene da un luogo ad un altro, ove idoneo a rendere di fatto più difficoltosa l'identificazione della sua provenienza delittuosa*."[65]

Per completare il quadro generale delle condotte tipiche previste ex art. 648 *bis* c.p. non rimane che fornire una definizione dell'ultima voce prevista dalla norma, ossia il compimento di altre operazioni di ostacolo all'identificazione dell'origine dei proventi delittuosi. Non può trascurarsi come, alla luce della sua generica formulazione, così come peraltro è

[64] Cfr. G. FIANDACA-E.MUSCO, *op. ult. cit.*, pp. 257 e ss.
[65] Cfr. Cass. pen., sez. II, 13 luglio 2020, n. 23774

sostenuto dalla dottrina maggioritaria, si tratti di una categoria puramente residuale. Essa ricomprende ogni altra attività – che dunque non sia di sostituzione o trasferimento – che frapponga ostacoli all'identificazione del denaro, beni o altro di provenienza illecita.

Quest'ampia categoria funge, pertanto, da perno verso il quale ricondurre ogni condotta non tipizzata dalla norma e rispecchia, in tal senso, la natura del riciclaggio come fenomeno poliedrico, che può dunque assumere una molteplicità di forme ed essere attuato ricorrendo ad una pluralità di tecniche disparate. Si ritiene, dunque, che il tessuto repressivo, che il legislatore ha voluto improntare, sia destinato a colmare qualsiasi potenziale lacuna normativa, non lasciando priva di sanzione alcuna forma di riciclaggio.[66]

Pur volendo apprezzare tale estensione di tutela, non si può tuttavia trascurare la carenza di specificità della previsione normativa, tale da provocare notevoli problemi applicativi. Sul punto furono addirittura sollevati dei dubbi di incostituzionalità per lesione dei principi di legalità e determinatezza, poi risolti grazie alla messa in luce della stretta connessione sussistente tra il compimento di "altre operazioni" e il fine ultimo perseguito, ossia l'occultamento della provenienza delittuosa.[67]

Notando come la norma utilizzi l'espressione "compiere operazioni" e dunque potendo escludere dal novero delle attività incriminate qualsiasi condotta omissiva, non risulta tuttavia sufficiente limitarsi a questa distinzione al fine di dare corpo alla condotta in analisi.

In soccorso a tale operazione definitoria, la giurisprudenza è intervenuta pronunciandosi sul concetto di "idoneità a ostacolare" definendolo come "*rendere difficile l'accertamento della provenienza della res, attraverso un qualsiasi espediente*"[68]. È così che, nel respingere le critiche mosse in punto

[66] Cfr. FIANDACA MUSCO, *op ult cit*., p. 262
[67] Cfr. A.R. CASTALDO-M. NADDEO, *op. ult. cit.*, 2010, p. 140
[68] Cfr. Cass. pen., sez. II, 12 gennaio 2006, n. 2818. Più di recente, si veda Cass. pen., sez. II, 9 marzo 2015, n. 26208

di vaghezza e indeterminatezza nella formulazione della fattispecie, può dirsi come la previsione di tale ultima categoria sancisca la configurazione del reato di riciclaggio come reato a forma libera, essendo sufficiente ogni condotta idonea a provocare un *effetto dissimulatorio* consistente nell'ostacolare o rendere più difficoltosa la ricerca dell'autore del delitto presupposto[69].

Per completezza si segnala brevemente in questa sede l'esistenza di un ulteriore orientamento dottrinale, secondo il quale la formulazione di questa terza ipotesi sia tanto generica e onnicomprensiva da rendere superflua la previsione delle altre due forme alternative di condotta di sostituzione o trasferimento.[70]

1.6.2 L'elemento soggettivo.

Proseguendo l'inquadramento generale del reato di riciclaggio, per quanto concerne l'elemento soggettivo, dottrina e giurisprudenza concordano nell'identificarlo con il dolo generico. Ciò a differenza della previgente versione della fattispecie, dove invece il legislatore aveva previsto la necessaria sussistenza, come elemento psicologico, del dolo specifico[71].

Ad oggi, invece, il reato di riciclaggio si configura come reato di mera condotta e di pericolo concreto, connotato solamente dal dolo generico, il quale può definirsi come coscienza e volontà di compiere attività ostative – quali la sostituzione o la trasformazione o altre operazioni – ai fini di

[69] Sul punto si veda A.M. DELL'OSSO, *op. ult. cit*. p. 110. *Ex multis*, cfr. Cass. pen., 5 ottobre 2011, n. 39756. Si veda anche Cass. pen., sez. V, 18 gennaio 2018, n.5459, che recita: "*la condotta posta in essere dall'agente deve essere idonea a ostacolare l'identificazione della provenienza del bene, non essendo sufficiente la sola ricezione di somme oggetto di distrazione. Affinché si integri la fattispecie di cui all'articolo 648-bis, infatti, occorre un quid pluris consistente nel compimento da parte dell'agente di un'attività volta a ostacolare la tracciabilità della provenienza del bene."*

[70] Sul punto si veda FIANDACA-MUSCO, *op.ult.cit*. p. 266

[71] Cfr. G. FORTE, *L'elemento soggettivo nel riciclaggio*, in A. MANNA (a cura di), *Riciclaggio e reati connessi all'intermediazione mobiliare,* 2000, pp. 168 e ss.

mascherare la connessione tra oggetto del reato e la sua provenienza. Manca, dunque, nella disposizione ex art. 648-*bis* c.p., qualsiasi riferimento ad intenzioni specifiche o a scopi di guadagno perseguiti dal soggetto. In altre parole, si richiede che il soggetto criminale attui, consapevolmente, una condotta idonea a realizzare il pericolo di dissimulazione contrastato dalla fattispecie.

Il tentativo definitorio appena compiuto rispecchia l'orientamento dottrinale che, sul punto, si è rivelato tendenzialmente uniforme[72]. Potrebbe d'altro canto risultare di giovamento – per un'adeguata comprensione dell'elemento soggettivo in analisi – prestare attenzione ad alcune recenti pronunce giurisprudenziali sul punto. Più precisamente, anche la Corte di Cassazione penale ha dimostrato di condividere l'assunto proposto dalla dottrina secondo il quale l'elemento soggettivo del delitto di riciclaggio consista nella coscienza e volontà di ostacolare l'accertamento della provenienza delittuosa dei beni e nella consapevolezza di tale provenienza[73]. Inoltre, sempre secondo giurisprudenza, la consapevolezza dell'agente circa la provenienza delittuosa dei beni può essere desunta da qualsiasi elemento e sussiste quando gli indizi sono gravi e univoci da autorizzare la conclusione che i beni ricevuti per la sostituzione siano di derivazione delittuosa, specifica e anche mediata.[74] Ad oggi, pertanto, non si richiede più la consapevolezza dello specifico reato da cui il denaro i beni o le altre utilità provengono: "*non è necessario che il delitto presupposto risulti giudizialmente accertato, (…), è sufficiente che non sia stato escluso nella sua materialità in modo definitivo*

[72]Cfr. E. MEZZETTI, *Reati contro il patrimonio, in Trattato di diritto penale. Parte speciale*, GROSSO C. F., PADOVANI T., PAGLIARO (diretto da), 2013, p. 656; ANTOLISEI F., *Manuale di diritto penale. Parte speciale*, 2016, pagg. 607; P.MAGRI, *Delitti contro il patrimonio mediante frode*, in *Trattato di diritto penale. Parte speciale*, (diretto da) G. MARINUCCI, E. DOLCINI, vol. VII, tomo 2, 2007, pp. 459 e ss.

[73] Cfr. Cass. Pen., sez. II, 14 giugno 2018, n. 29920; Cass. pen., sez V, 2 febbraio 2017, n. 25924. In senso conforme, si veda anche Cass. Pen., sez II, 11 giugno 2015, n. 41330; Cass. Pen., sez. II, 7 gennaio 2011, n. 546; Cass. Pen., sez. VI, 18 dicembre 2007, n. 16980

[74] Cass. Pen. sez II, 6 novembre 2009, n. 47375. Si veda anche Cass. Pen., sez II, 5 giugno 2015, n. 27806.

e che il giudice ne abbia ritenuto anche solo incidenter tantum la sua sussistenza".[75]

Visto *l'excursus* giurisprudenziale finalizzato a cogliere maggiormente le sfumature dell'elemento soggettivo in analisi, è doveroso segnalare in questa sede una più recente evoluzione dell'orientamento della Suprema Corte, la quale, in tempi più recenti, ha ritenuto sufficiente la sussistenza del dolo eventuale dell'attore; in altri termini, può essere ritenuto responsabile di riciclaggio anche colui che agisce avendo presente la concreta possibilità della provenienza delittuosa del denaro ricevuto ed investito, e ne accetta consapevolmente il rischio[76].

Ciò comporta che il soggetto agente avrebbe agito allo stesso modo, anche se avesse saputo della provenienza illecita dei beni o delle altre utilità.

1.6.3 Il soggetto attivo del reato.

Sotto il profilo del soggetto attivo, il reato di riciclaggio ex art. 648 *bis* c.p. si configura come un reato comune, in quanto la disposizione di legge prevede che possa essere commesso da *chiunque*[77]. Non si richiede, dunque, che il soggetto autore del reato possieda specifici requisiti o caratteristiche. A conforto di tale categorizzazione, ricorre il secondo comma dell'art. 648 *bis* c.p., il quale prevede come aggravante la qualificazione dell'individuo agente come esercente un'attività professionale[78].

[75] Cass. Pen., sez II, 6 novembre 2009, n. 47375
[76] Cass. Pen., sez. II, 23 ottobre 2018, n. 56633
[77] Cfr. V. PLANTAMURA, *Riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e confisca (artt. 648-bis, 648-ter e 648-quater)*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale, parte speciale*, vol. X, *I delitti contro il patrimonio*, 2011, p. 866
[78] V. MAIELLO, L. DELLA RAGIONE, *op. ult. cit*., p. 74.

Ai fini di completezza, deve tuttavia segnalarsi l'opinione promossa da un autorevole filone dottrinale[79], la quale identifica – con più precisione – il reato di riciclaggio come reato a soggettività ristretta.

Tale classificazione discende dalla valorizzazione della clausola iniziale di esclusione della punibilità del soggetto che abbia commesso o concorso a commettere il reato presupposto[80]. Trattasi, più precisamente, di quel tratto peculiare della fattispecie in analisi, conosciuto come "beneficio dell'autoriciclaggio", ad oggi non più presente nel nostro ordinamento, grazie all'autonoma configurazione del reato di autoriciclaggio che il Legislatore ha disposto con la l. n. 186 del 2014[81].

Può, dunque, riprendersi quanto sostenuto dalla dottrina più autorevole, secondo la quale "a dispetto dell'etichetta di reato comune, la descrizione del soggetto attivo risulta arricchita dalla necessaria carenza di partecipazione nel reato base"[82].

1.6.4 Consumazione e tentativo.

Il reato di riciclaggio, configurandosi come reato a forma libera, può essere commesso ricorrendo a modalità diverse[83]. Tale ampio ventaglio di condotte realizzabili comporta, sotto un profilo esegetico, difficoltà nel comprendere quando il reato possa considerarsi commesso.

---

[79] Per tutti, si veda DEMURO, *Il bene giuridico proprio quale contenuto dei reati a soggettività ristretta*, in Riv. it. dir. e proc. pen., 1998, pp. 845 ss.
[80] R. ACQUAROLI, *Il riciclaggio*, in *Trattato teorico-pratico di diritto penale*, vol. VII, diretto da PALAZZO, PALIERO, 2015, p. 907
[81] Vedi *infra*, par. 1.7.
[82] V. MAIELLO, L. DELLA RAGIONE, *op. ult. cit*., p. 76. In argomento e, più precisamente, per una lettura critica della clausola di esclusione della punibilità, si rinvia a G.M. FLICK, *La repressione del riciclaggio ed il controllo dell'intermediazione finanziaria. Problemi attuali e prospettive*, in *Riv. it. dir. proc. pen*., 1990.
[83] V. MAIELLO, L. DELLA RAGIONE, *op. ult. cit*., p 153.

Perché il reato di riciclaggio possa dirsi consumato, autorevole dottrina[84] afferma che il soggetto agente debba aver realizzato l'attività di sostituzione, trasferimento o di altre operazioni di occultamento dell'origine illecita dei proventi.

Sul punto, la giurisprudenza[85] ha affermato che il reato di riciclaggio può configurarsi non solo come delitto a consumazione istantanea, ma anche come reato permanente, qualora l'autore lo esegua in modo frammentario e progressivo.

Per quanto concerne il tentativo, esso si ritiene configurabile appellandosi ai principi generali, con ciò intendendosi che il delitto di riciclaggio può configurarsi anche nel caso di un'operazione tentata, ma non effettivamente realizzata. La giurisprudenza si è pronunciata a più riprese sul punto. In primo luogo, ha previsto che "è configurabile il delitto di riciclaggio in quanto nella vigente formulazione della fattispecie non è costruito come delitto a consumazione anticipata"[86]. Ancora, si fa menzione di due pronunce di merito che hanno sancito la configurabilità del tentativo "per aver posto in essere atti idonei, diretti in modo non equivoco" a realizzare un'operazione di riciclaggio[87].

1.6.5 Le circostanze aggravanti e attenuanti speciali.

Non può mancarsi di far cenno anche alle circostanze aggravanti ed attenuanti speciali previste ex art. 648 *bis* c.p.

---

[84] G. MARINUCCI, E. DOLCINI, *Codice penale commentato*, 2021, p. 2842

[85] Cfr. Cass. Pen., 29 aprile 2009, n. 246561

[86] Cass. Pen., 14 gennaio 2010, n. 17694. Si segnala che, in precedenza, il delitto di riciclaggio si configurava al contrario come delitto a consumazione anticipata; pertanto, non era al tempo configurabile il tentativo, come ribadito da Cass. Pen., 2 febbraio 1983, in Giust. Pen., 1984, II, 296. In argomento, si veda anche ANTOLISEI, *op. ult. cit*.

[87] Trib. Nuoro, 3 novembre 2000; Corte App. Cagliari, 19 febbraio 2002. In particolare, è stata riconosciuta la configurabilità del tentativo relativamente al compimento di "atti idonei, diretti in modo non equivoco a cambiare un assegno provento di rapina, atti consistiti, in particolare, nell'aver inviato a un terzo presso un istituto di credito per il cambio di un assegno di accertata provenienza da rapina".

In particolare, ai sensi del comma terzo della disposizione in analisi, si prevede una circostanza aggravante di tipo soggettivo, secondo la quale "la pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale". La *ratio* sottostante alla previsione di tale aggravante risiede nella *voluntas legis* di impedire che il soggetto agente, sfruttando la maggiore idoneità di alcune attività a ripulire proventi illeciti, ricorra a professionisti ed esperti capaci operanti in specifici settori di fornire un contributo decisivo alla dispersione delle tracce del denaro.

Sempre sul punto, si ritiene che parlando di "attività professionali", il significato di professione debba essere inteso in senso ampio, in modo tale da ricomprendere tutte le attività regolamentate pubblicisticamente in via diretta e indiretta[88].

In dottrina si registrano peraltro posizioni differenti per la definizione di attività professionali. Una prima corrente[89] sostiene che per definire l'attività professionale in vista dell'applicazione dell'aggravante sia necessario fare riferimento all'art. 26 della l. n. 55/1990, secondo il quale è possibile irrogare provvedimenti disciplinari, di sospensione o revoca del titolo abilitante quando i fatti previsti ex art. 648 bis c.p. "siano commessi nell'esercizio di attività bancaria, professionale di cambiavalute ovvero altra attività soggetta ad autorizzazione, licenza, iscrizione in appositi albi o registri". Un'altra corrente[90], invece, perimetra il significato di "attività professionale" riferendosi al d. lgs. n. 231/2007 il quale ha individuato determinate categorie di persone fisiche e giuridiche soggette alla normativa antiriciclaggio e, per questo, obbligate a svolgere operazioni di verifica, controllo, registrazione e segnalazione di operazioni sospette[91].

[88] V. MAIELLO, L. DELLA RAGIONE, *op. ult. cit,* p. 162
[89] V. P. MAGRI, *op. ult. cit*., p. 479
[90] C. LONGOBARDO, *op. ult. cit*., pp. 750 ss.
[91] Trattasi, a titolo esemplificativi, di professionisti, revisori contabili, società di gestione con competenze finanziarie.

Anche la giurisprudenza è intervenuta sul punto, precisando che "le operazioni di ripulitura del denaro sporco effettuate da esperti nel settore bancario integrano l'aggravante del fatto commesso nell'esercizio di un'attività professionale, che, per la sua natura oggettiva, si estende a tutti i concorrenti del reato"[92].

La circostanza attenuante è prevista, invece, al comma quarto del medesimo articolo e si applica nel caso in cui "il denaro, i beni o le altre utilità provengano da un delitto per il quale è prevista la pena della reclusione inferiore nel massimo a cinque anni". Di tale circostanza attenuante può dirsi brevemente che la *ratio* ad essa sottostante viene individuata nella volontà di trovare un equilibrio tra l'estensione generica dei reati presupposto e il principio di obbligatorietà della legge penale, il quale, come sottolineato da autorevole dottrina[93], "impone di attivare la macchina processuale anche in presenza di condotte sostanzialmente inoffensive, riequilibrando le pene nei casi di reati presupposto meno gravi".

1.7 Brevi cenni sul reato di autoriciclaggio

Per i limiti imposti dalla presente trattazione, essendo l'elaborato focalizzato sul reato di riciclaggio e le sue più recenti evoluzioni, segue per completezza solo un più breve inquadramento sul delitto di autoriciclaggio.

Esso fa il suo ingresso nell'ordinamento italiano con la l. 15 dicembre 2014 n. 246[94], in vigore dal 1° gennaio 2015, all'articolo 648-*ter*.1 c.p. In forza delle spinte sovranazionali[95] e della lacuna di diritto presente

[92] Cass. Pen. sez. II, 24 aprile 2012, n. 43534.
[93] V. MAIELLO, L. DELLA RAGIONE, *op. ult. cit.*
[94] La presente legge è titolata "Disposizioni in materia di emersione e rientro dei capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio". Con il d.lgs. 8 giugno 2011, n. 231 è stata inserita nell'elenco dei reati presupposto in tema di responsabilità degli enti.
[95] L'OCSE, nel Rapporto sull'Italia del 2011, aveva evidenziato come la lacuna normativa dell'ordinamento italiano costituisse un punto di grande debolezza nella lotta anticorruzione e nel procedimento di tutela della legalità e della trasparenza dell'ordinamento economico-finanziario. Ancora, in anni precedenti, nel 2006, il Fondo Monetario Internazionale

nell'ordinamento italiano, al pari di quanto accadde per il reato di riciclaggio, il legislatore – seppur dopo anni – decise di intervenire per reprimere la condotta di chi "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".

Al pari del delitto di riciclaggio, come sopra esposto in premessa[96], anche l'illecito in analisi è frutto di una complessa evoluzione normativa, spinta pur sempre dalla volontà di contrastare i disastrosi effetti distortivi che l'impiego di proventi illeciti genera sul mercato. Infatti, non si poteva trascurare al tempo come anche la disponibilità "in proprio" di proventi illeciti da parte dello stesso soggetto che ha agito per realizzarli, fosse altrettanto pericolosa, in quanto tale da porre l'individuo stesso in una situazione vantaggiosa rispetto ai concorrenti sul mercato rispettosi delle norme che lo disciplinano.[97] In altre parole, la *ratio legis* resa sottesa all'incriminazione dell'autoriciclaggio parrebbe essere quella di voler congelare quanto ricavato dall'attività illecita da parte del soggetto che ha realizzato il reato presupposto, impedendone così un'utilizzazione ancor più lesiva dell'ordine economico. Per queste ragioni divenne sempre più urgente anche la previsione di un sistema sanzionatorio destinato specificamente nei confronti dell'autore del delitto presupposto che realizzi ulteriori attività aventi ad oggetto proventi delittuosi.

Vale anche in relazione all'autoriciclaggio, la considerazione per cui i delitti contro la circolazione illecita di denaro e di beni, seppur configurati in origine dal legislatore in rapporto di dipendenza dalla disciplina dei reati

sollecitava l'introduzione della punibilità dell'autoriciclaggio in soccorso all'azione investigativa e repressiva condotta dalle autorità italiane.

[96] Si rinvia *supra* al paragrafo 1.1 del presente capitolo

[97] Cfr. F. MUCCIARELLI, *Qualche nota sul delitto di autoriciclaggio*, in *Diritto Penale Contemporaneo*, 1/2015, pp. 108 e ss.

presupposto, hanno assunto gradualmente una sempre più ferma autonomia, enfatizzando così il disvalore che ontologicamente connota le attività di impiego di proventi illeciti.[98]

Per una completa comprensione del delitto in esame, giova naturalmente tenere in debita considerazione quanto sopra esposto in punto di riciclaggio. Su questo fronte, infatti, molteplici sono le analogie tra le due fattispecie criminose, seppur contraddistinte da alcune non trascurabili differenze.

In primo luogo, è opportuno chiarire sin d'ora che il reato di autoriciclaggio si configura come fattispecie pluri-offensiva, in quanto molteplici risultano i beni giuridici tutelati dalla norma. Su questo punto, si richiama quanto *supra* esposto per il reato di riciclaggio e, dunque, il riferimento alla lesione primaria dell'amministrazione della giustizia.

Da un punto di vista del soggetto attivo, a differenza del reato di riciclaggio disciplinato ex art. 648-bis c.p., tratto distintivo del delitto ex art. 648 *ter*.1 c.p., si rinviene nel fatto che l'autore deve essere necessariamente colui che ha preso parte alla realizzazione del delitto presupposto da cui è derivato il provento oggetto di reinvestimento. In questo senso, l'autoriciclaggio rientra nella categoria dei reati propri. Con riguardo ai reati-presupposto, anche la disciplina dell'autoriciclaggio è stata modificata dal d.lgs. 8 novembre 2021, n. 195 – di cui *supra*[99] – il quale ha esteso il novero dei reati presupposto ai reati colposi, includendovi anche le contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi.

Volgendo poi lo sguardo alla condotta incriminata, emergono caratteri accostabili alla fattispecie di riciclaggio e impiego. Infatti, vengono punite rispettivamente le condotte di impiego, sostituzione e trasferimento così come sanciti nelle disposizioni ex artt. 648 e 648 *bis* c.p.

---

[98] R. BARTOLI, M. PELISSERO, S. SEMINARA, *Diritto penale. Lineamenti di parte speciale, 2021*, p. 390

[99] Cfr. par. 1.4.1, cap. I.

Alla previsione di tali condotte, il legislatore ha accostato una c.d. clausola modale, la quale richiede una concreta idoneità ad ostacolare l'origine delittuosa dei proventi. In particolare, tale clausola è fonte di due non trascurabili risvolti esegetici: *in primis*, risulta tale da ricomprendere tutti quei comportamenti – che anche se non propriamente realizzati artificiosamente – rendano obiettivamente difficoltosa l'individuazione della provenienza criminosa del bene.[100] Inoltre, la previsione del requisito della concretezza, che – si noti – è manchevole nella configurazione del delitto di riciclaggio, richiama l'interprete della legge ad un'attività esegetica molto rigorosa e puntuale che si concreta nell'esigenza di attuare un accertamento integrale sulla capacità ostacolatrice della condotta realizzata. In tal senso, vengono in rilievo non tutte le condotte re-introduttive di beni illeciti nel circuito economico legale, ma solo quelle che si distinguono per idoneità ad ostacolare concretamente tale provenienza.

Ad aggiungere maggiore specificità alla condotta incriminata, ricorre un ulteriore requisito previsto dal legislatore, il quale ha previsto che le condotte siano volte a realizzare operazioni economiche che fungano da ostacolo per l'identificazione della provenienza delittuosa dei proventi. Le condotte assumono rilevanza penale se si manifestano in (i) "attività economiche", con ciò intendendosi, ex art. 2082 c.c., ogni attività organizzata per la produzione o lo scambio di beni o servizi; (ii) "attività finanziarie", ossia attività connessa alla circolazione di denaro o di titoli o di intermediazione immobiliare, e da ultimo (iii) "attività imprenditoriali" - una delle forme dell'attività economica

[100] Cfr. F. MUCCIARELLI, *op. ult. cit., p.115*. Sul punto, si veda anche Cass. Pen., sez. II, 7 ottobre 2021, n. 2868, secondo la quale "*Ai fini dell'integrazione del reato di autoriciclaggio, non occorre che l'agente ponga in essere una condotta di impiego, sostituzione o trasferimento del denaro, beni o altre utilità che comporti un assoluto impedimento alla identificazione della provenienza delittuosa degli stessi, essendo, al contrario, sufficiente una qualunque attività, concretamente idonea anche solo ad ostacolare gli accertamenti sulla loro provenienza*".

o “speculative”, cioè qualunque attività volta ad ottenere un vantaggio avvalendosi di situazioni favorevoli[101].

Per concludere, in punto di elemento soggettivo, è richiesto il dolo generico, definibile come coscienza e volontà di realizzare le condotte previste dalla norma, associata alla consapevolezza della provenienza delittuosa del denaro, dei beni o delle altre utilità.[102]

A completare il quadro della presente trattazione, non possono non menzionarsi le circostanze aggravanti e attenuanti e la clausola di non punibilità prevista al comma 4 dell’art. 648 ter.1 c.p.

Nel tentativo di dare breve conto delle circostanze del reato in analisi, si ritiene opportuno procedere seguendo la struttura della fattispecie. In particolare, il terzo comma prevede una prima circostanza attenuante nell’ipotesi in cui i proventi derivino da delitti puniti con la reclusione inferiore a cinque anni. Trattasi in altre parole, della previsione di una pena ridotta a fronte di un reato presupposto considerato meno grave dal Legislatore[103].

Il quarto comma dell’art. 648 *ter*.1 c.p. prevede invece la c.d. aggravante mafiosa: più precisamente, saranno applicate comunque le sanzioni previste

[101] In ANTOLISEI, *op. ult. cit.*, pag. 622 e in FIANDACA-MUSCO, *op. ult.cit*., p. 273, si sottolinea come “l’attività economica” sia una formula così generica tale che avrebbe potuto ricomprendere anche le altre. Dunque, alla luce di questa critica, l’elenco presente ex art. 648.1-*ter* c.p. risulta assai ridondante.

[102] Cfr. Cass. Pen, 7 marzo 2019, n. 13795; Cass. Pen. 14 luglio 2016, n. 33704. Sul punto si veda anche R. BARTOLI, M. PELISSERO, S. SEMINARA, *op. ult. cit*., p. 390 e ss.

[103] La natura di questa circostanza è assai discussa. In dottrina, si è registrato un orientamento che individua in questo comma una fattispecie di reato autonoma. Sul punto, cfr. F. MUCCIARELLI, *op. ult. cit.*, in Diritto Penale Contemporaneo, 1, 2015, p. 122; G. COCCO*, Il c.d. Autoriciclaggio – art. 648-ter1*, in G. COCCO (a cura di), *Trattato breve di diritto penale. Parte speciale. Vol. II: I reati contro i beni economici,* 2015 p. 320. A favore della configurazione della disposizione come circostanza attenuante, si veda A. DELL’OSSO*, Il reato di autoriciclaggio: la politica criminale cede il passo a esigenze mediatiche e investigative,* in *Riv. it. dir. proc. pen.,* 2015, pp. 809 e ss.; A. CIRAULO, voce *Autoriciclaggio*, in *Digesto disc. pen*., IX agg., 2016, p. 130.

al primo comma dell'articolo[104], qualora il reato presupposto sia commesso aggravato dalla circostanza della "mafiosità" ex art. 416 bis c.p.[105]

Delle ultime due circostanze previste dalla norma, la prima è un'aggravante. Si tratta della medesima circostanza prevista per il delitto di riciclaggio al comma secondo dell'articolo 648 bis c.p., ossia quando i fatti siano stati realizzati nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale. L'ultima circostanza è, invece, attenuante ad effetto speciale ed è prevista al comma sesto dell'art. 648 *ter*.1 c.p.; essa si applica nei confronti dei soggetti c.d. collaboratori.

Tali sono coloro che si siano efficacemente operati 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. Tale previsione si connota per il suo carattere premiale sia verso chi contribuisca a neutralizzare l'offensività della condotta, sia verso chi aiuti le autorità a rinvenire i proventi illeciti ed accertarne la provenienza[106].

Per quanto concerne, invece, la clausola di non punibilità prevista al comma 5 dell'art. 648 ter.1 c.p., trattasi di una clausola altrimenti conosciuta anche come di "mero utilizzo o godimento personale". In particolare, il comma 5 prevede che "*Fuori dai 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*".

Alla luce dell'inquadramento generale appena fornito sul reato di riciclaggio e, nel presente paragrafo, anche sull'autoriciclaggio, si può ora procedere nell'indagine delle sue più recenti manifestazioni, in particolare nella forma del c.d. *cyberlaundering*. In prima battuta, ai fini della presente elaborazione, si cercherà di comprendere l'applicabilità della normativa ex

[104] Trattasi, in particolare, della reclusione da due a otto anni e di una multa da 5.000 a 25.000 euro.
[105] R. BARTOLI, M. PELISSERO, S. SEMINARA, *op. ult. cit.*, 2021, p. 396.
[106] L. DELLA RAGIONE, V. MAIELLO, *op. ult. cit*., p. 360.

artt. 648-bis e 648.1-ter c.p. ai casi in cui il riciclaggio si svolga tramite l'utilizzo delle nuove tecnologie e le relative problematiche.

CAPITOLO II

IL *CYBERLAUNDERING*: IL DELITTO DI RICICLAGGIO ATTRAVERSO LA LENTE DEI *CYBERCRIMES*

2.1 Premessa: l'interazione tra nuove tecnologie informatiche e diritto penale.

Considerando quanto sopra esposto in tema di riciclaggio, si avvia ora la trattazione di un tema tanto spinoso quanto stimolante ed in costante evoluzione: in particolare, trattasi del fenomeno del *cyberlaundering*.

Il *cyberlaundering* costituisce la manifestazione più recente ed evoluta del delitto di riciclaggio, che sfrutta i vantaggi e le potenzialità di Internet[107] e i suoi lati più ambigui e rischiosi, per il perseguimento di finalità illecite.

Obiettivo del presente elaborato è quello di fornire in primo luogo una definizione completa del fenomeno in discorso, percorrendo un tentativo definitorio appropriato e funzionale – in un secondo momento – ad una più approfondita analisi della normativa di contrasto, sia domestica che

[107] Per una definizione di Internet, v. L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, 2019, p. 38. L'Autore mette in luce come Internet sia la "rete delle reti", con ciò ad indicare che si tratti di una Rete costituita a sua volta da reti pubbliche e private. La Rete in senso stretto riguarda, come spiegato nel prosieguo della trattazione, i soli aspetti meramente materiali e tecnici di Internet, quali fibre ottiche, *server*, *router* etc.

sovranazionale. In secondo luogo, si cercherà di vagliare l'ipotesi di applicabilità della disciplina ex artt. 648 *bis* e 648 *ter*.1 c.p. ai fini della punibilità di condotte di riciclaggio compiute parzialmente o interamente *online*.

Naturalmente, prima di avviare una simile indagine, è necessario addentrarsi nella dimensione spazio-temporale in cui il *cyberlaundering* ha luogo. Lasciando innanzitutto spazio circoscritto ad una riflessione d'impronta più criminologica, può senz'altro affermarsi che in seguito alla c.d. "rivoluzione cibernetica"[108], - la quale, come sottolineato da autorevole dottrina[109], è tale poiché "il fenomeno coinvolge ogni aspetto della vita e degli interessi delle persone e della collettività" - è stato necessario rileggere e reinterpretare il concetto di "Rete", sussumendolo nella più ampia categoria del *Cyberspace*.

Infatti, se da un lato, la Rete, intesa *strictu sensu*, si riferisce ai soli aspetti meramente materiali e tecnici di Internet, quali fibre ottiche, *server*, *router* etc., la nozione di *Cyberspace* ricomprende, invece, il rapporto esistente, sotto un profilo non solo tecnico ma anche sociologico, tra l'utilizzo delle nuove tecnologie informatiche (TIC) e la dimensione virtuale di Internet.

È così che proprio il ruolo dominante della rivoluzione informatica e le sue ricadute su ogni settore economico-sociale non paiono ormai più trascurabili soprattutto con riguardo all'impatto avuto su ogni ordinamento giuridico e, per quanto sia di nostro interesse, sul diritto penale.

---

[108] In argomento, per una più approfondita analisi sulla rivoluzione cibernetica si veda L. PICOTTI, *Cybercrime e diritto penale*, in V. SELLAROLI, C. PARODI, *Diritto penale dell'informatica,* 2020, pp. 710 e ss. Nel contributo, si mette in luce come la rivoluzione cibernetica si caratterizzi, da un lato, per una sempre più accentuata componente di automazione, da intendersi come elaborazione dei dati e implementazione di appositi algoritmi capaci di apprendere e auto-correggersi e, dall'altro, l'iper-connettività, la quale permette una trasmissione assai rapida dei dati raccolti ed elaborati.

[109] Per tutti, si veda L. PICOTTI, *op. ult. cit.*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, 2019, pp. 39 e ss.

Se, infatti, un tempo poteva parlarsi più semplicemente di "diritto penale dell'informatica", come semplice branca specialistica del diritto penale, ad oggi tale classificazione può ritenersi superata in favore di una rilettura più attuale di tutto l'ordinamento penale – e anche civile – alla luce dell'influenza delle nuove tecnologie.

Sul punto, infatti è ormai pacifico come la rivoluzione cibernetica e il costante sviluppo delle nuove tecnologie impongano un adeguamento costante del diritto affinché, da un lato sia data tutela contro i più recenti fenomeni criminosi, dall'altro affinché sia sempre perseguita la funzione regolatrice tipica di ogni ordinamento giuridico.

Con l'obiettivo di perseguire queste due principali finalità, non solo sul piano interno ma anche sovranazionale, la soluzione più appropriata non potrà che essere l'armonizzazione del sistema regolatorio e sanzionatorio partendo dal fondamentale assunto che quanto risulti sanzionato "off-line" non possa restare impunito "on-line".[110] Traslando questo principio nella realtà giuridica, la sola via a disposizione del Legislatore parrebbe innanzitutto essere quella di perimetrare le condotte e i contenuti che si realizzano nel *Cyberspace*.

Rifiutando, quindi, un approccio tradizionalista e quanto più conservatore nella sua accezione più negativa, che comporterebbe la mera interpretazione di nuovi fenomeni criminosi alla luce delle categorie già esistenti e delle fattispecie già tipizzate, sembra utile compiere uno sforzo ulteriore al fine di rispondere efficacemente alle nuove minacce cibernetiche, assumendo *in primis* una visione d'insieme e onnicomprensiva, che solo in un momento successivo riesca a declinarsi in provvedimenti interni da parte ciascun legislatore nazionale[111].

---

[110] L. PICOTTI, *op. ult. cit.*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, 2019, p. 42.

[111] Per ulteriori riflessioni sul punto, cfr. L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in *Tutela penale della persona e nuove tecnologie*, L. PICOTTI (a cura di), 2013, p. 29 s.

È così che oggigiorno, essendo il binomio diritto penale e rivoluzione tecnologica una fonte inesauribile di questioni aperte, potrebbe essere utile prendere le mosse dall'ampia categoria dei *cybercrimes*, per poi calarsi concretamente nel delitto di riciclaggio e del riciclaggio *online*, nel più modesto tentativo di dare risposta a quesiti definitori e di disciplina che impegnano ad oggi la dottrina più autorevole.

2.2 I *Cybercrimes*

L'evoluzione di cui *supra* ha comportato una categorizzazione delle fattispecie criminose più complessa, la quale richiede di concentrare la propria attenzione su due principali categorie di reati.

La prima categoria che venne a configurarsi, contemporaneamente allo sviluppo di Internet, fu quella dei c.d. reati informatici[112]. A questi si fa riferimento nell'ordinamento italiano con la l. 21 dicembre 1993[113], la quale li configurava come reati realizzabili in sistemi telematici chiusi o ad accesso circoscritto, come ad esempio nelle reti di singole aziende o in riferimento a specifici settori.

Da questa categoria rimanevano, dunque, escluse tutte quelle condotte criminose realizzabili *online* da chiunque e potenzialmente offensive verso un numero indefinito di vittime. Tali reati hanno

[112] A loro volta, si classificano in *reati informatici in senso stretto*, i quali contengono, nella tipizzazione della fattispecie, l'espressa menzione e disciplina di elementi tecnico-informatici – o altrimenti, di automatizzazione di dati o informazioni – che costituiscono il cuore della fattispecie incriminatrice. La seconda categoria è quella dei *reati informatici in senso lato*, ossia reati tradizionali, tipizzati dal Legislatore senza un espresso riferimento all'elemento informatico, ma realizzati servendosi di strumenti informatici. Su questo tipo di distinzione, si veda L. PICOTTI, *op. ult. cit.*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, 2019, pp. 76-77. C. PARODI, S. LOMBARDO, L. GHIRARDI, *Riciclaggio e aggiotaggio telematicco*, in C. PARODI, V. SELLAROLI (a cura di), *Diritto penale dell'informatica: reati della rete e sulla rete*, 2020, p. 445 e ss. In riferimento ai reati cibernetici, si può proporre la medesima distinzione, come si vedrà *infra*.

[113] Trattasi della prima legge contro la criminalità informatica. In argomento si veda il commentario di F. MUCCIARELLI, L. PICOTTI, G. RINALDI, UGOCCIONI, in *Legislazione penale*, 1 e 2, 1996.

oggigiorno trovato un'autonoma categorizzazione: si tratta, di preciso, dei reati cibernetici.[114]

Come i reati informatici, anche i reati cibernetici si distinguono in "reati cibernetici in senso stretto", ove la fattispecie incriminatrice contiene un elemento essenziale o di circostanza che richiama espressamente la rete o il *web*. Altra categoria è quella dei "reati cibernetici in senso lato", i quali si configurano come reati già tipizzati tradizionalmente dal Legislatore, ma che prevedono elementi tipici del fatto di reato che solo in via implicita o interpretativa sono compatibili con la loro realizzazione concreta nel *Cyberspace*[115].

I c.d. *Cybercrimes* si caratterizzano, dunque, per un elemento chiave imprescindibile: la libera accessibilità ad Internet da parte del pubblico. Sotto questo profilo, può dirsi che il libero accesso *online* costituisca il frutto del processo di globalizzazione – anche tecnologica – iniziato dagli anni '90. Tuttavia, se da un lato, come sopra si accennava in punto di globalizzazione, questa ha indubbiamente migliorato lo stile di vita di gran parte della società, deve però sottolinearsi come abbia parimenti contribuito al dilagare di condotte criminose.

Infatti, ad essere aumentata, come effetto della rivoluzione cibernetica, è la possibilità di commettere crimini offerta ogni giorno ad ogni individuo. In altre parole, le nuove tecnologie, essendo divenute "strumenti democratici", conferiscono a chiunque l'occasione di compiere atti illeciti.[116]

Nel tentativo di orientare la presente trattazione verso una lettura del reato di riciclaggio, il quale – come visto nel precedente capitolo – si configura *in primis* come fenomeno economico, a chi scrive sembra

---

[114] Per tutti, L. PICOTTI, *op. ult. cit.*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, 2019, p. 48

[115] L. PICOTTI, *op. ult. cit.*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, 2019, pp. 76-77.

[116] Cfr. E. SAVONA E M. MIGNONE, *The fox and the hunters: how IC Technologies change the crime race,* in *Crime and Technology*, 2004

opportuno precisare che il *cyberspace* esercita, relativamente alla commissione di reati di tipo economico, quali il riciclaggio e l'autoriciclaggio, una determinante forza attrattiva nei confronti di individui criminali. Tale forza risiede principalmente nella "dematerializzazione" delle risorse connesse alla natura digitale del denaro e alla correlata difficoltà di identificare l'autore del reato.

Accanto a questa notazione di tipo prettamente economico, si possono poi richiamare altri tratti distintivi, riconducibili più in generale alla categoria dei reati cibernetici. Si noti, ad esempio, come all'esistenza di risorse "rarefatte", si affianca un ulteriore incentivo per la criminalità, ossia la c.d. "deterritorializzazione" dell'utente, che si ritrova capace di agire da più "spazi informatici" in uno stesso momento.[117] Ed è proprio questa delocalizzazione che pone un notevole problema in punto di giurisdizione, in quanto, comportando l'indeterminatezza del *locus commissi delicti*, agevola operazioni tra più Paesi, in particolare sfruttando quelli con normative antiriciclaggio meno aggressive.

Inoltre, nel *Cyberspace* si assiste anche ad una "detemporalizzazione" delle attività, le quali possono essere realizzate automaticamente attraverso operazioni preimpostate, senza la necessaria azione fisica dell'individuo di fronte al dispositivo[118].

Da ultimo, estremamente rilevante ai fini dell'analisi in discorso, è l'osservazione secondo la quale la dimensione cibernetica non si concretizza solo nel c.d. *surface web*, ma si compone anche di una componente "oscura", il c.d. *dark web*[119]. Con riguardo al primo, trattasi

---

[117] Cfr. F. POMES, *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, in Riv. Trim. Dir. Pen. Contemp., 2/2019, p. 166. In argomento, v. R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in (a cura di) A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *op. ult. cit.,* 2019, pp 142 e ss.

[118] R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di internet*, in Diritto Penale Contemporaneo, 2010, p. 1

[119] In argomento, si veda P. PERRI; G. ZICCARDI, *Dizionario Legal tech*, 2020; V. L. PICOTTI, *Cybercrime e diritto penale,* in V. SELLAROLI, C. PARODI, *op. ult. cit.,* 2020, pp. 712 e ss.

di una dimensione "pubblica" ed accessibile a chiunque senza la necessità di inserire alcun tipo di particolare configurazione. Il secondo, invece, si presenta come dimensione virtuale, ad alta potenzialità criminosa, che si fonda su *policies* di alta sicurezza e anonimato. Più in particolare, esso costituisce parte del c.d. Deep Web[120] e il suo significato può essere efficacemente reso ricorrendo all'espressione "rete nascosta", ossia quella rete raggiungibile via Internet solo attraverso *software* specifici, configurazioni e accessi autorizzativi, dai contenuti per la maggior parte criptati, dove lo scambio dei dati tra utenti è assicurato e protetto dalla difficoltà della crittografia utilizzata[121].

In un contesto tanto rivoluzionario, quanto pericoloso, il *cyberlaundering* ha iniziato a diffondersi con l'avvento di Internet e delle nuove tecnologie, sfruttati sempre più da individui criminali per finalità illecite sin dai tempi del boom tecnologico negli anni '90.[122]

Accanto all'annullamento della dimensione spazio-temporale appena menzionata, ulteriore elemento chiave che consente ancor di più lo sfruttamento delle nuove tecnologie per compiere attività criminose è l'eccezionale rapidità con cui vengono processati i dati[123] e, naturalmente una connessione Internet veloce ed accessibile.

---

[120] Per una definizione completa, si veda R. R. P. BRAGA, A. A. B. LUNA, *Dark Web and Bitcoin: an anaylsis of the impact of digital anonymate and cryptocurrencies in the practice of money laundering crime*, in *Direito e Desenvolvimento*, 2018, p. 275 ove si dice che "il Deep Web si riferisce a qualsiasi contenuto su Internet che, per vari motivi, non può essere raggiunto da motori di ricerca come Google."
In argomento, si veda anche V. CIANCAGLINI, *Below the Surface: Exploring the Deep Web,* 2015.

[121] Per un breve approfondimento sul tema "deep web" e "dark web" si veda il successivo paragrafo 2.3.

[122] Per il rapporto tra criminalità e nuove tecnologie si veda A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA *op. ult. cit.*, 2019

[123] Tecnicamente, i computers sono dotati di un processore centrale, c.d. CPU, misurato in giga herts (GHz), il quale determina la velocità con cui i dati sono stati processati. Un altro elemento che influisce sulla velocità è la c.d. Random Access Memory (RAM) e le schede video. All'interno del primo vengono depositati *files*, attraverso il secondo è possibile la formazione istantanea di foto, video e immagini di ogni specie. La dotazione completa e aggiornata di tali componenti permette di agire da remoto a velocità istantanea.

La dimensione cibernetica, dunque, presenta, oltre alle caratteristiche appena citate, un ulteriore tratto distintivo, che tuttavia sembra arrecare più svantaggi che benefici[124]: trattasi della condizione di anonimato in cui possono versare gli utenti che interagiscono *online*. Così, se da un lato la realtà cibernetica permette libertà di espressione e tutela del diritto all'anonimato, dando la possibilità di agire ed esprimersi non svelando la propria identità, dall'altro può essere di gran lunga sfruttata da parte di individui criminali per agire perseguendo scopi criminosi, senza pericolo di essere tracciati.

Una parte della dottrina[125] ritiene che nella macrocategoria dei reati cibernetici possa essere poi compiuta una ulteriore distinzione tra *computer crimes*, ove il computer e i sistemi informatici costituiscono la finalità delle attività criminali e i c.d. *computer facilitated crimes,* ove i computer e le nuove tecnologie figurano come mezzi essenziali per la commissione dei crimini.

Pur non rinvenendo in dottrina e giurisprudenza una definizione unanime e condivisa di *cybercrimes*, può dirsi tuttavia che tale categoria ricomprenda tutte quelle condotte lesive di interessi penalmente rilevanti, che siano a loro volta riconducibili ai "reati informatici", presenti ormai in molti ordinamenti nazionali.

Alla luce delle considerazioni sin qui svolte, sembra plausibile affermare che il *cyberlaundering* possa essere senz'altro analizzato in riferimento alla categoria dei *cybercrimes*, pur dovendo tenere conto di alcuni problemi definitori, di cui si darà conto *infra*, che ostacolano l'inquadramento del *cyberlaundering* in modo esclusivo all'interno della predetta categoria.

---

[124] D.A. LESLIE, *Legal Principles for Combatting Cyberlaundering, Law, Governance and Technology Series*, 2014, p. 59.

[125] R. FLOR, *op. ult. cit*., 2018; cfr. anche F. POMES, *op. ult. cit*., pp. 19 e ss.

2.3 (Segue) Lo sfruttamento del *deep web*

Come sopra accennato, per le sue caratteristiche tipiche, non è solo Internet, nella sua tradizionale dimensione di "*world-wide-web*" (www), a incentivare il compimento di attività criminose – e nello specifico, di riciclaggio *online* – ma anche in particolare una sua parte più "oscura": il c.d. *deep web*[126]. Riferendosi a questa dimensione nascosta, è utile fare riferimento a "tutto il materiale accessibile via reti alternative, che sfruttano Internet solo come "veicolo" per spostare dei dati volutamente frammentati ed offuscati onde garantire il più possibile l'anonimato"[127].

Per limiti imposti dalla presente trattazione e rinviando, dunque, ad altre fonti[128] l'analisi tecnico-informatica del funzionamento della rete "nascosta", per ragioni di coerenza espositiva, sembra invece qui opportuno mettere in luce come questa dimensione cibernetica offra notevole supporto per la realizzazione di attività criminose, in particolare perché, come accennato *supra*, consente – in una sua parte – di agire in una completa condizione di anonimato.

Se da un lato vi sono parti del *deep web* dove il nome e l'indirizzo dell'utente sono visibili e rintracciabili, all'interno delle reti anonime sono attivi dei sistemi ulteriori che permettono all'utente di non svelare la propria identità e, anzi, offuscano le tracce che permettono di identificare la persona che si nasconde dietro questi sistemi. In altre parole, è possibile navigare, ma

---

[126] Si ritiene completa la definizione riportata in M. BALDUZZI, *Cybercrime in the Deep Web*, 2015 "*The Deep Web is any internet content that, for various reasons, cannot be or is not indexed by search engines like Google. This definition thus includes dynnaimc web pages, blocjed sites (like those where you need to answer a CAPTCHA to access), unlinked sites, private sites (like those that require login credentials), non-HTNL/contextual/scripted content, and limited-access networks."*

[127] V. LAGI*, Deep web, dark web e indagini informatiche*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA*, op. ult. cit*., p. 1708. A conforto di questa definizione, ricorre la stima compiuta da Bright Planet nel 2000. Era stato calcolato che il Web si componesse di più di 550 miliardi di documenti, quando invece Google ne aveva indicizzati solo 2 miliardi.

[128] J. JONES, *Tor: accessing the deep web and dark web with Tor. How to set up Tor, stay anonymous onlune, avoid NSA spying and access the deep web and dark web*, 2017; G. BALENA, *Il web nascosto: i segreti della rete e del deerk web: deep web, dark web e criptovalute*, 2020.

nascondendo il proprio indirizzo IP, come se il *browser* non fosse stato utilizzato.

Necessario strumento di accesso a questo tipo di navigazione anonima è la VPN anonima[129]. Trattasi, più precisamente, di un *server* situato in uno Stato estero che pone forti ostacoli di rintracciabilità, gestito solitamente da un'azienda privata che garantisce l'anonimato. Una volta in rete, l'utente "anonimo", persegue il suo obiettivo di rimanere non tracciato e non tracciabile per navigare – eventualmente anche visitando pagine *web* presenti nella rete Internet pubblica e accessibile.

In questi casi, poiché l'utilizzo di un *browser* può lasciare tracce dei dati identificativi, spesso viene utilizzato il c.d. *The Onion Router* (TOR), appositamente creato per non lasciare alcuna traccia.

All'interno di questa dimensione anonima del *deep web*, si rinviene una sua parte ancor più recondita, il *dark web*. Come d'intuito può suggerire l'espressione, esso costituisce terreno ancor più fertile per la commissione di reati sfruttando reti anonime.

Nonostante siano argomento approfondito nel capitolo III del presente elaborato, giova sin d'ora tenere conto come la potenzialità criminosa del *dark web*[130] emerga soprattutto con riguardo alle criptovalute.

Considerando, ad esempio, la criptovaluta Bitcoin, da un lato le transazioni sono anonime alla luce della mancata corrispondenza che può sussistere tra indirizzo del portafoglio utilizzato e della reale identità dell'utente, ma d'altro canto ogni transazione rimane pubblica e può essere analizzata dagli investitori.

Per ulteriori approfondimenti sul punto ed un'analisi dei profili di rischio connessi al riciclaggio di denaro, si rinvia *infra*.

---

[129] In argomento N. MARK, *Designing the Total Area Network: Intranets, VPN's, and Enterprise Networks Explained.,* 2000.

[130] Cfr. M. BALDUZZI, *op. ult. cit*., 2015.

2.4 Il *cyberlaundering*: un frammentato orizzonte definitorio.

È ora di assoluta importanza comprendere in quale categoria sussumere il *cyberlaundering* per vagliare non solo i profili di responsabilità che esso comporta, ma anche le possibili soluzioni di disciplina che il Legislatore potrebbe approntare.

In via di prima approssimazione, inquadrandolo come forma più "avanzata" di riciclaggio, può dirsi certamente, come poi si vedrà nel prosieguo della trattazione, che il *cyberlaundering* presenti molteplici caratteristiche in comune con il riciclaggio tradizionale, ma ciò non toglie che non possono essere trascurati i profili di novità tipici dei *cybercrimes* che richiedono, per l'appunto, ulteriori sforzi interpretativi e di disciplina.

In prima battuta, il *cyberlaundering* sembra definibile *latu sensu*, riconducendolo alla macrocategoria dei *cybercrimes*, come utilizzo di un dispositivo, quale un *computer*, per realizzare un'operazione che comporti benefici economici, tangibili o intangibili, che derivino da un'attività criminale[131]. Questo fenomeno può essere considerato come lo sviluppo più moderno del reato di riciclaggio così come disciplinato ex art. 648-bis c.p.

Tuttavia, non si può trascurare come l'orizzonte definitorio del *cyberlaundering* sia puntellato da una molteplicità di elementi propri sia del reato di riciclaggio, sia dei c.d. *cybercrimes*; pertanto, non parrebbe del tutto appropriato riferirsi nettamente ad una delle anzidette categorie, al contrario parrebbe opportuno pervenire ad una classificazione che dia pari rilevanza agli elementi caratteristici di entrambi.

Trattasi, in particolare, di un fenomeno che comprende l'insieme delle attività illecite finalizzate a "ripulire" (letteralmente "lavare") non solo il denaro (c.d. *money laundering*), ma più in generale i capitali, i beni, i valori o altre "utilità" di provenienza delittuosa, ricorrendo a sistemi "cibernetici"[132]

[131] La definizione proviene da D.A. LESLIE, *op. ult. cit.*, p. 55.

[132] Tale definizione è fornita da L. PICOTTI, *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in Riv. Trim. Dir. pen. dell'economia, 3-4, 2018, pp. 590-591.

e tecniche avanzate che impongono lo sfruttamento di *software* e dispositivi più moderni.[133]

Pur essendo dunque un'attività criminosa commessa nel *Cyberspace*, il principale interrogativo che concerne questo fenomeno riguarda la sua effettiva riconducibilità alla categoria dei c.d. *cybercrimes.* Se per alcuni questa classificazione è assai pacifica, altri non mancano di porne in luce alcuni profili più problematici.

Procedendo con ordine, la prima ipotesi definitoria del *cyberlaundering* si limita a ricondurlo alla categoria dei *cybercrimes*[134]. Se, tuttavia, fosse inteso come semplice sottocategoria dei *cybercrimes,* autorevole dottrina[135] ritiene che perderebbe rilevanza la disciplina tradizionale del riciclaggio e che il tentativo regolatorio perseguito dal legislatore dovrebbe essere, invece, principalmente focalizzato sugli elementi informatici[136], configurando una disciplina volta ad evitare un utilizzo distorto degli strumenti informatici. In questo modo, si rischierebbe, però, di non prestare la dovuta attenzione agli elementi caratteristici del reato di riciclaggio. Sembra dunque opportuno non limitarsi ad una classificazione tanto intuitiva, quanto semplicistica del fenomeno in discorso.

[133] Tali sistemi cibernetici, ad oggi, implicano l'utilizzo della "rete", da intendersi non solo come *web*, comprensivo di Internet, ma anche della sua parte più "oscura" del *dark web*[133] a scopi criminosi.

[134] Cfr. L. PICOTTI, *op. ult. cit*., p.592

[135] Cfr. A. LESLIE, *op. ult. cit*., p. 61

[136] Si richiama la definizione di informatica, così come data in M. FOURMAN, *Informatics*, 2002. Reperibile al link: http://www.inf.ed.ac.uk/publications/online/0139.pdf. "L'informatica è la scienza dell'informazione, la pratica dell'elaborazione delle informazioni e l'ingegneria dei sistemi informativi. L'informatica studia la struttura, gli algoritmi, il comportamento e le interazioni dei sistemi naturali e artificiali che immagazzinano, elaborano, accedono e comunicano informazioni, ad esempio il computer. Sviluppa inoltre i propri fondamenti concettuali e teorici e utilizza i fondamenti sviluppati in altri campi."

È così che, alla luce di un altro filone dottrinale, il *cyberlaundering* si configurerebbe puramente come tecnica di riciclaggio[137], che si distingue dal riciclaggio tradizionale per la movimentazione digitale del denaro. Potrebbe risultare anche parzialmente corretto definire il *cyberlaundering* come tecnica di riciclaggio, utilizzando il termine "tecnica" nell'accezione di strumento volto a realizzare un determinato fine, i.e. quello riciclatorio. Questa definizione presenta però una debolezza simmetrica rispetto alla precedente: ostinarsi a categorizzare il *cyberlaundering* ricorrendo solo alla categoria del reato di riciclaggio espone al rischio di trattazioni eccessivamente semplicistiche facendo ricorso a categorie generali, che trascurano le sottili peculiarità del fenomeno in discorso[138].

Infatti, il fatto che un individuo criminale utilizzi risorse informatiche per riciclare denaro o altre utilità, non rende dette risorse informatiche un mero strumento per raggiungere fini illeciti, ma parte integrante di tutta l'attività criminosa.

È per questo che, a chi scrive, sembra senz'altro più preciso e utile ricorrere ad una terza ipotesi definitoria di *cyberlaundering*, come fenomeno ibrido, riassumibile sinteticamente con l'espressione di certo innovativa di "money laundering 2.0"[139]. Più nello specifico, sembra più puntuale mantenere concettualmente distinti da un lato il reato di riciclaggio di denaro, nella sua forma più tradizionale, dall'altro il ricorso alle nuove tecnologie e a tutti i prodotti da esse derivati – come si vedrà, le criptovalute – che diventano così non solo lo strumento ma anche il fine stesso delle attività riciclatorie.

Può dunque concludersi che, ad un livello più avanzato, vista la sua configurazione prettamente tecnologica, ma presentando la stessa struttura

---

[137] J. HUNT, *The new frontier of money laundering: How terrorist organisations use cyberlaundering to fund their activities, and how governments are trying to stop them. Information and Communications Technology Law* 20, 2011, p. 133.

[138] A favore di questa critica si pronuncia L. PICOTTI, *Profili penali del cyberlaundering*: *le nuove tecniche di riciclaggio*, in Riv. trim. dir. pen. econ., 2018, p. 608

[139] A. LESLIE, *op. ult. cit*., p. 62

"tradizionale" del reato di riciclaggio, il *cyberlaundering* da un lato presenti tratti riconducibili alla categoria generale dei *cybercrimes,* dall'altro mantenga contestualmente la struttura tipica della fattispecie di riciclaggio, richiedendo in tal senso al Legislatore uno sforzo regolatorio specifico per disciplinare questo fenomeno emergente e sempre più pericoloso e dilagante.

2.5 (Segue) Le tre fasi del *cyberlaundering*: la rilevanza del *cyber-placement.*

Se la letteratura nostrana e internazionale riconducono al *cyberlaundering* le tre fasi tipiche del reato di riciclaggio di *placement, layering* e *integration*, è tuttavia opportuno mettere in luce alcuni adattamenti necessari che devono essere apportati a queste tre fasi, in particolare alla prima. Infatti, non si può trascurare come sia proprio la fase del *placement* a riflettere maggiormente l'impatto che le nuove tecnologie e tutte le loro potenzialità hanno sulla realizzazione di attività criminose, quali il riciclaggio *online.*

La prima fase del *cyberlaundering*, e anche la più delicata, si identifica come c.d. *cyberplacement*. Come si è cercato di spiegare nel capitolo precedente, nella disciplina tradizionale del riciclaggio, il *placement* del denaro di provenienza delittuosa si realizza fisicamente: si assiste, infatti, ad una movimentazione fisica o materiale del denaro contante, che ad esempio può essere depositato presso una banca.

Per quanto concerne, invece, il *cyberlaundering* e la rispettiva fase di *placement* bisogna premettere una distinzione utile tra riciclaggio digitale strumentale e riciclaggio digitale integrale. Nel riciclaggio del primo tipo, il denaro è inizialmente presente in forma materiale – contante – e viene convertito in moneta digitale solo in un momento successivo. In tal caso è dunque necessario ricorrere ad un'operazione di

cambio del denaro circolante per moneta elettronica o direttamente per criptomoneta. Più nello specifico, nel caso di cambio di denaro contante in moneta digitale basterà semplicemente depositare il denaro sui conti correnti o sulle carte prepagate. Nell'ipotesi, invece, di cambio di denaro contante direttamente in criptomoneta, il procedimento è senza dubbio più macchinoso, perché bisognerà avvalersi di appositi ATM che accettino rimesse in contante e forniscano chiavi crittografiche in Bitcoin o che emettano criptovalute convertibili.

Nel riciclaggio digitale integrale, invece, i proventi illeciti destinati alla ripulitura si trovano sin dal principio in stato digitale. In questo modo, può dirsi che la fase di *placement* spinga ad individuare due processi criminosi differenti: se da un lato, il *cyberlaundering* strumentale consente di facilitare l'esecuzione solo di qualche passaggio del procedimento riciclatorio, dall'altro il *cyberlaundering* integrale si fonda interamente su una sola operazione finanziaria che avviene *tout court online*.

Il *cyberplacement*, se realizzato integralmente nella dimensione virtuale, permette quindi di eliminare *tout court* la movimentazione fisica del denaro, venendo meno, in questo modo, uno dei rischi potenzialmente più alti di riciclaggio, ossia lo spostamento fisico di ingenti somme di denaro.[140]

In dottrina si registrano sul punto orientamenti opposti, dei quali sembra opportuno dare breve riscontro in questa sede. Il primo si spinge a considerare che la fase di *placement* verrebbe in qualche modo elisa quando il provento da reato risulti già disponibile in valuta virtuale[141]. In tal caso, per l'appunto

[140] A questo proposito, sembra efficace la definizione di *cyberlaundering* come "riciclaggio del terzo millennio" formulata da U. RAPETTO, *Il riciclaggio del terzo millennio,* in *Gnosis*, *Rivista italiana di intelligence*, 1999, reperibile al sito www.sicurezzanazionale.gov.it

[141] Sul punto si veda opinione a favore di M. CROCE., *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy,* in Sistema Penale 4/2021, p. 139, dove il *placement* viene definito come fase "non necessaria" in caso di riciclaggio digitale integrale. A favore di questo orientamento, si veda anche W. FILIPKOWSKI, *Cyberlaundering: An Analysis of Typology and Techniques*, in *International Journal of Criminal Justice Sciences*, vol. 3, 2008, p. 20

di riciclaggio interamente virtuale, risulterebbe dunque estremamente difficile intervenire in ottica repressiva, in quanto, non essendo *ab initio* individuabili gli intermediari, è assai arduo che emergano i capitali illeciti e i rispettivi responsabili delle operazioni

La seconda voce dottrinale[142], sostiene invece, al contrario, che per il *cyberlaundering* integrale potrebbe, dunque, dirsi che la fase del *placement* assorba anche le altre due, avviando e concludendo il procedimento di ripulitura interamente *online*. A chi scrive, sembra più calzante sostenere la prima soluzione proposta, in quanto nelle ipotesi in cui la valuta virtuale sia già disponibile *online*, non vi sarebbe alcuna utilità nell'individuare una vera e propria fase di "collocamento". Inoltre, contrariamente a quanto sostenuto dal secondo filone dottrinale, si ritiene invece che le altre due fasi – di cui si parlerà nell'immediato prosieguo della trattazione – rivestano una loro autonomia e funzione essenziale nel procedimento di riciclaggio *online*. Si precisa, infine, che è indiscussa la necessità della fase di *cyberplacement* qualora il denaro sia inizialmente presente in moneta fisica o elettronica e necessiti, dunque, di essere convertito in valute virtuali[143].

La seconda fase di *cyber-layering* si sostanzia nell'attuazione di processi e tecniche idonee a disperdere quanto più possibile le tracce dell'origine criminose del denaro. A questo riguardo, si ricorre facilmente al trasferimento di fondi in *shell companies* ovvero all'acquisto di beni *online* che vengono poi rivenduti. Tra tutti però, si è registrata una prevalenza del ricorso all'*online banking* al fine di ripulire

[142] J. ALCINI, "*Mondi paralleli, bitcoin e reati virtuali",* in *La giustizia penale*, 2, 2018, pp. 438-448

[143] Sul punto, v. M. CROCE., *op. ult. cit.*, p. 139. L'Autrice esplicita come, in questo fase, la fase di collocamento sia "particolarmente delicata, poiché i potenziali riciclatori debbono entrare in contatto con gli intermediari professionisti al fine di ottenere la conversione del provento delittuoso in circolante virtuale." Sul punto, si veda al Capitolo III, parr. 3.11 e 3.12 in punto di responsabilità di *exchangers* e *wallet providers*, in qualità di intermediari nella conversione del denaro in criptovalute.

il denaro sporco[144]. Più precisamente, tale tecnica è risultata assai favorevole al

perseguimento di scopi criminosi, in quanto un conto bancario può essere aperto senza un contatto diretto tra il cliente e la banca, potendo dunque il soggetto criminale permanere in una condizione di anonimato.[145]

Da ultimo, per quanto concerne l'ultima fase di *cyberintegration* può dirsi che sia necessitata dall'esigenza di conferire un'apparenza di legittimità al denaro ripulito. Di regola, questo obiettivo viene perseguito immettendo il denaro ripulito nel mercato, ma devono essere messe in luce le differenze rispetto al riciclaggio fisico o materiale.

Le tecniche di *integration* risultano, infatti, di natura differente. Se nel riciclaggio materiale si assiste, in via esemplificativa, alla creazione di false ricevute per beni e servizi, nella c.d. *cyberintegration* sono proprio le *shell companies*, menzionate anche per la fase di *cyberlayering*, che giocano un ruolo significativo. Accade, dunque, che creando conti in nome di esistenti società, i proventi illeciti vengano "uniti" a quelli legittimi, dandovi una parvenza di liceità. Inoltre, a rendere agevole queste operazioni di riciclaggio contribuisce la circostanza che queste *shell companies* abbiano sede in Stati in cui le leggi finanziarie e i controlli delle Autorità siano estremamente deboli, per questo conosciuti come paradisi fiscali[146].

Questi ultimi presentano una notevole quantità di aspetti assai ambigui e opachi. In primo luogo, la gestione fiscale si caratterizza spesso per una tassazione sul patrimonio e sul reddito estremamente bassa o, addirittura inesistente. Ancora, si tratta di aree ove, ad esempio, il segreto bancario viene

[144] A. LESLIE, *op. ult. cit.*, 2014, p. 74

[145] L'*online banking* rientra, dunque, tra le tecniche di riciclaggio *online* maggiormente utilizzate, ma non è la sola. Per un quadro più completo sulle tecniche di riciclaggio si rinvia a A. LESLIE, *op. ult. cit*., 2014.

Nella presente trattazione, si veda, invece, il paragrafo successivo.

[146] V. PLANTAMURA*, Il cybericiclaggio*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, 2019, pp. 859 e ss.

garantito con un grado così elevato da risultare impermeabile alle Autorità[147]; oppure ove la responsabilità penale per evasione fiscale, riciclaggio e altri reati finanziari è debole o inesistente.

2.6 (Segue) Le principali tecniche di *cyberlaundering.*

Menzionate nel capitolo precedente alcune tra le tecniche più frequenti di riciclaggio di denaro, il *cyberlaundering* conosce tuttavia un catalogo di attività criminose di gran lunga più esteso ed in crescente espansione. In via puramente esemplificativa, può citarsi in questa sede la falsificazione di carte di pagamento (sia di credito, che di debito), il furto di identità, il gioco d'azzardo online (c.d. *gambling)* e altre operazioni realizzate nel *web*.[148]

Più nel dettaglio, si pensi all'utilizzo di una c.d. *smart card,* i.e. carta di pagamento ricaricabile, la quale permette di acquistare beni o servizi attraverso l'utilizzo di proventi illeciti che potrebbero tuttavia apparire "ripuliti" grazie all'impiego della carta stessa.

Ancora, rientrano tra le tecniche più ricorrenti di riciclaggio, l'utilizzo indebito di piattaforme come PayPal o la presentazione *online* di offerte di lavoro fittizie al fine di fungere solo da "intermediario" per ricevere e successivamente ritrasferire somme di denaro o beni previo pagamento di un compenso. Anche l'utilizzo improprio delle SIM telefoniche prepagate potrebbe risultare strumento utile per veicolare somme consistenti di denaro. Ancora, molto comune è la tecnica del c.d. "man in the middle" (MITM)[149]. Essa comporta un'attività di

[147] Si segnala, però, che questo non vale per tutti quei Paesi che hanno firmato gli Accordi sullo scambio automatico delle informazioni finanziarie (SAI), incentivati dall'OCSE. Italia e Svizzera ne siglarono uno nel 2017.

[148] L. PICOTTI, *op. ult. cit.*, p. 593

[149] C. PARODI, V. SELLAROLI, *op. ult. cit*., 2020, p. 455. Le due tecniche maggiormente diffuse sono BEC, i.e., *business e-mail compromise* e CEO Fraud, i.e. *Chairman Executive Officer*. Secondo questa seconda tecnica, ordini a contenuto patrimoniale vengono impartiti da soggetti terzi che fingono di essere – tramite falsa identità telematica – uno degli organi di vertice di importanti società. Tuttavia, la prassi più comune pare essere la prima, di più

interferenza nella connessione tra due utenti o tra due dispositivi al fine di deviare su un determinato conto bancario delle somme di denaro versate a titolo di corrispettivo. Altra tecnica assai diffusa è quella dell'*online banking*[150]: ad oggi l'*online banking* costituisce una tra le più evidenti manifestazioni del progresso tecnologico: ai clienti è concesso, infatti, di compiere semplici operazioni bancarie senza la necessità di recarsi fisicamente in banca.

Se da un lato tale opportunità risulta fortemente semplificativa nella gestione di ogni genere di attività economica, dall'altro si deve dare conto dei motivi per cui risulti di frequente una sorta di "paradiso" per i riciclatori di denaro. In primo luogo, il denaro tenuto dalle c.d. *internet-based banks*, trattasi nello specifico di *e-cash*, non è soggetto alla regolamentazione e al controllo del denaro contante. Risulta in tal caso ostica l'applicabilità del principio "*know your customer*" (KYC), il quale richiede alle banche fisiche di registrare operazioni e transazioni sospette alle autorità. Inoltre, aprire un conto *online* risulta di gran lunga più agevole, poiché la reale identità del cliente non è verificata né autenticata, contrariamente a quanto accade quando ci si reca fisicamente in banca per l'apertura di un conto.

Sempre per quanto concerne l'*online banking* come tecnica per svolgere attività di riciclaggio, una importante notazione riguarda, in questo caso, la realizzazione della prima fase di *layering*: infatti, il deposito di *e-cash* è facilmente realizzabile ricorrendo alla tecnica dello *smurfing* al fine di disperdere le tracce dell'origine criminosa del denaro, distribuendolo in una pluralità di conti aperti presso una o più *internet-based banks*. Da ultimo, giocano un ruolo fondamentale anche le *smart cards*, in particolare quelle "*open looped*" come VISA, Mastercard, American Express che possono essere utilizzate ovunque il *brand* della carta stessa sia accettato.

---

agile attuazione qualora vengano versati o ricevuti dei bonifici da parte di soggetti commerciali.

[150] D. A. LESLIE, *op. ult.cit*., p. 76. In argomento, W. FILIPKOWSKI, *op. ult. cit.*, p. 233.

Inoltre, vale mettere in evidenza come il *cyberlaundering* sia strettamente connesso anche all'ascesa dei casi di furto di identità: gli hackers tendenzialmente utilizzano metodi crittografici che rendono possibile l'accesso ai conti *online* senza lasciare alcuna traccia, trasferendo somme di denaro da un conto ad un altro, addirittura rubando i numeri delle carte di credito.

Il panorama delle tecniche di riciclaggio si estende, poi, anche alle aste *online*. Queste vengono soprattutto utilizzate, nella fase di *cyberlayering* del processo riciclatorio, appunto per il "lavaggio" di denaro proveniente da attività illecite. Di regola, il soggetto criminale si iscrive a siti – legali – di aste online e, d'accordo con un soggetto terzo collaboratore parimenti registrato, mettono all'asta un oggetto di valore. Dopo aver acquistato una *smart card* e dopo averla ricaricata con denaro sporco, gli estremi crittografici della carta vengono inviati al collaboratore, il quale estrae il denaro e lo utilizza per acquistare – d'accordo con l'individuo criminale - il bene messo in vendita, versando i soldi nel conto del sito di aste *online*.

Una volta svolti i controlli, dal sito di aste *online* il denaro viene (ri)trasferito nel conto del soggetto riciclatore, venendo così reimmesso nel mercato, una volta ripulito.

Seppur non sia la sola mancante, per ragioni espositive imposte dalla presente trattazione, a chi scrive sembra opportuno menzionare la rilevanza di un'ultima modalità di *cyberlaundering*, pur con la consapevolezza della vastità dell'argomento. Trattasi, nello specifico, del c.d. *online gambling*[151].

[151] L'Italia ha il maggior mercato di gioco *online* in Europa, il cui profitto è in costante ascesa. Nel 2017, si è registrato che gli Italiani abbiano perso infatti nelle giocate alle slot machine o con le scommesse sportive sul web 1,38 miliardi di euro. Cfr. l'articolo del Sole24ore al link: https://www.ilsole24ore.com/art/gambling-online-italiani-bruciano-13-miliardi-euro-l-anno-AEMKwWgE

Non può, inoltre, trascurarsi la sussistenza di un forte legame tra il *gambling*, il riciclaggio di denaro e le attività svolte da associazioni mafiose. Si veda ad esempio, la gestione di

Il gioco *online* è una delle attività ad oggi maggiormente diffuse. I casinò *online* paiono, infatti, molto più accattivanti di quelli fisici: senza dubbio più convenienti di questi ultimi, essi sono accessibili da ogni luogo e a basso costo, talvolta a costo zero. La connessione con il *cyberlaundering* si innesta quando l'individuo riciclatore utilizzi servizi di gioco *online* legittimi o ne crei appositamente di nuovi per finalità di "lavaggio" di denaro sporco. Si noti però come la creazione *ex novo* di un apposito sito di giochi *online* potrebbe talvolta risultare maggiormente problematica, alla luce della necessità di *compliance* alle leggi e ai regolamenti in materia e come, per questo, tendenzialmente si ricorra ad infiltrazioni illecite in piattaforme regolarmente attive *online.*

La trattazione delle tecniche di *cyberlaundering* è volta a fornire non solo un quadro quanto più chiaro possibile del vasto panorama criminoso che permea il nostro attuale contesto economico-sociale, ma soprattutto la consapevolezza della varietà di tecniche utilizzabili. Al capitolo successivo, verrà dedicato spazio ad una tecnica ad oggi dilagante che comporta l'utilizzo illecito di un emergente strumento di pagamento, le criptovalute, che in quanto scarsamente regolate si prestano a perseguire finalità criminose, permettendo agli utenti di movimentare ingenti quantità di denaro virtuale.

Continuando, al momento, l'esposizione su una linea più criminologica, si ritiene di seguito opportuno soffermarsi brevemente su come il *cyberlaundering* permanga, ad oggi, strettamente connesso alle attività realizzate dalla criminalità organizzata.

---

scommesse sportive su siti illeciti oppure la prassi secondo la quale le associazioni criminali acquistano biglietti, in complicità con i concessionari, versando un sovrapprezzo che dovrà poi essere riciclato. Per una vasta casistica in materia, si veda anche COMMISSIONE PARLAMENTARE DI INCHIESTA SUL FENOMENO DELLE MAFIE E SULLE ALTRE ASSOCIAZIONI CRIMINALI, ANCHE STRANIERE, *Relazione sulle infiltrazioni mafiose e criminali nel gioco lecito e illecito*, 2017 (consultabile sul sito www.camera.it/temiap/allegati/2017/01/12/OCD177-2634.pdf), pp. 20 e ss.

2.7 La stretta connessione tra *cyberlaundering* e criminalità organizzata.

Come rilevato anche nel precedente capitolo, la criminalità organizzata – nella sua forma più pericolosa, ossia quella mafiosa - ha subito negli ultimi decenni una forte trasformazione: se, originariamente, la principale attività che occupava le organizzazioni criminali era il traffico di stupefacenti, ad oggi, a fronte del vertiginoso sviluppo economico e sociale e del mutamento della fisionomia dei mercati, il campo prediletto di azione delle associazioni criminali è divenuto l'imprenditoria, le attività finanziarie e dei servizi pubblici.[152]

In altre parole, la criminalità organizzata, seppur mantenendo uno dei suoi tratti più tipici, il c.d. *power syndicate*, ossia il profondo legame con il territorio in cui si insedia – quasi in veste di "protettrice" delle realtà locali – ha contemporaneamente assunto una dimensione transnazionale, di natura imprenditoriale, il c.d. *enterprise syndicate*[153].

È proprio in seno alla criminalità organizzata di stampo mafioso che si assiste ad un'alta domanda di riciclaggio, in quanto tali organizzazioni costituiscono terreno fertile di attività criminose che realizzano un'elevata quantità di denaro[154]. *A fortiori*, si registra una crescente determinazione ad

[152] Cass. pen., sez. VI, 29 ottobre 2015, n. 563 afferma che "l'elemento che caratterizza l'associazione di tipo mafioso rispetto all'associazione dedita al narcotraffico, in presenza del quale può configurarsi il concorso tra i due delitti, è costituito non tanto dal fine di commettere altri reati, quanto dal profilo programmatico dell'utilizzo del metodo, che nell'associazione di cui all'art 416-bis c.p., ha una portata non limitata al traffico di sostanze stupefacenti, ma si proietta sull'imposizione di una sfera di dominio in cui si inseriscono la commissione di delitti, l'acquisizione della gestione di attività economiche, di concessioni, appalti e servizi pubblici, l'impedimento o l'ostacolo al libero esercizio di voto, il procacciamento del voto in consultazioni elettorali". Per approfondimenti sull'art. 416 *bis* c.p., si v. R. BARTOLI, M. PELISSERO, S. SEMINARA, *op. ult. cit*., pp. 792 e ss.

[153] R. PATALANO, *Riciclaggio e flussi finanziari illeciti nel capitalismo contemporaneo*, 10 marzo 2022, in *economiaepolitica, Riv. online della politica economica, reperibile al link: https://www.economiaepolitica.it/lavoro-e-diritti/distribuzione-e-poverta/riciclaggio-e-flussi-finanziari-illeciti-nel-capitalismo-contemporaneo/

[154] Come sottolineato da A. BALSAMO E A. MATTARELLA, *Criminalità organizzata: le nuove prospettive della normativa europea*, in Sistema Penale, 3/2021, p. 35 "Vi è stato quindi un clima di generale sottovalutazione delle mafie, considerate come un fenomeno essenzialmente italiano, ignorando le tracce della loro espansione all'estero. Proprio questo

inserirsi in modo capillare sia nei mercati leciti che illeciti, al fine di acquisire principalmente il controllo di attività economiche ed imprenditoriali.

Sul punto, in una stima globale il Fondo Monetario Internazionale ha stimato che il riciclaggio assommi il 5% del PIL[155].

Come osservato da autorevole dottrina[156], la crescente necessità di ridurre il c.d. *law enforcement risk,* ossia il rischio di essere individuati e incriminati dalle Autorità, induce i soggetti criminali a migliorare le tecniche di riciclaggio, dirigendosi verso una costante sofisticazione degli strumenti utilizzati.

Più in particolare, non sorprende che la criminalità organizzata di stampo non solo nazionale ma anche transfrontaliero, si sia rivolta con successo all'applicazione di vie alternative rispetto a quelle tradizionali per riciclare denaro. Infatti, anche alla luce delle ragioni sopra esposte, sono di certo determinanti i vantaggi di Internet quali rapidità e basso costo delle operazioni e la possibilità di non essere rintracciati ha naturalmente incentivato le criminalità.[157]

A stretta riprova del nesso intercorrente tra riciclaggio, nella sua più attuale forma di *cyberlaundering*, e criminalità organizzata, a livello europeo, si è assistito all'istituzione nel 2012 di un apposito organismo sovranazionale. Trattasi, nello specifico della Commissione speciale sul crimine organizzato, la corruzione e il riciclaggio di denaro (CRIM)[158].

---

clima ha permesso alle mafie di prosperare in maniera invisibile, ma inarrestabile, nei Paesi del Centro e Nord Europa, trovando nuovi canali per il riciclaggio (…)."

[155] Sul punto, v. contributo del Vicedirettore Generale di Banca d'Italia, A. M. TARANTOLA, *La prevenzione del riciclaggio nel settore finanziario. Il ruolo della Banca d'Italia*, in https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2011/Tarantola_100511.pdf, 2011

[156] Sul punto vedi E. U. SAVONA, *Criminalità organizzata*, in Enciclopedia del Novecento, 1998, pp. 422 e ss.; A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *op. ult. cit*.

[157] In argomento, G. PILLER, E. ZACCARIOTTO, *Cyber-Laundering: The Union Between New Electronic Payment Systems and Criminal Organizations*, in Transition Study Review, 2009, pp. 65 e ss.

[158] L'istituzione del presente organo è avvenuta in seguito all'approvazione della risoluzione del Parlamento europeo del 25 ottobre 2011. Si ritiene che sia di particolare

Sul piano internazionale, invece, non può non menzionarsi la Convenzione di Palermo sul crimine organizzato transnazionale (UNTOC) del 2000[159], volta a combattere la criminalità organizzata internazionale. In particolare, l'art. 6 della Convenzione stessa, rubricato "Penalizzazione del riciclaggio dei proventi da reato", ha previsto un obbligo di criminalizzazione di ogni attività di riciclaggio di proventi illeciti nei confronti degli Stati. Nella Convenzione emerge con chiarezza come l'attività di riciclaggio sia caratteristica delle organizzazioni criminali. Questa deduzione è confortata dal dato positivo dell'articolo 7 della Convenzione stessa, il quale recita al paragrafo b) che "Ogni Stato Parte assicura, senza pregiudizio per gli articoli 18 e 27 della presente Convenzione, che le autorità amministrative, di regolamentazione e di applicazione delle leggi e le altre autorità impegnate nella lotta al riciclaggio di denaro (comprese, laddove previsto dal diritto interno, le autorità giudiziarie) siano in grado di cooperare e scambiare informazioni a livello nazionale ed internazionale alle condizioni previste dal suo diritto interno, e prende in considerazione a tal fine la creazione di un servizio di informazione finanziaria che operi come centro nazionale per la raccolta, analisi e diffusione di informazioni riguardanti potenziali operazioni di riciclaggio di denaro".

---

rilievo il paragrafo 15 della risoluzione in discorso, il quale recita "*Il Parlamento europeo intende istituire, entro tre mesi dall'approvazione della presente risoluzione, una commissione speciale sulla diffusione delle organizzazioni criminali che agiscono a livello transnazionale, tra cui le mafie, ponendo tra le sue finalità l'approfondimento della dimensione del fenomeno e degli impatti negativi a livello socio-economico su scala UE, ivi compresa la questione della distrazione dei fondi pubblici da parte delle organizzazioni criminali e delle mafie e delle loro infiltrazioni nel settore pubblico nonché della contaminazione dell'economia legale e della finanza, e l'individuazione di una serie di misure legislative che possano far fronte a questa tangibile e riconosciuta minaccia per l'Unione europea e i suoi cittadini; chiede pertanto alla Conferenza dei presidenti di articolare la proposta, ai sensi dell'articolo 184 del regolamento*".

[159] Ad oggi, ratificata da parte di 117 Paesi. In argomento si veda CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *op. ult. cit*., p. 876. Per un approfondimento sulla Convenzione di Palermo e sui suoi Protocolli si v. MCCLEAN D., *Transnational Organized Crime. A Commentary on the UN Convention and its Protocols*, 2007; MATTARELLA A., *La Convenzione di Palermo: il futuro della lotta alla criminalità organizzata transnazionale*, 2020.

Si è venuto così a delineare un progresso tecnologico che corre a due velocità: da un lato la criminalità organizzata in ogni sua forma è pronta e reattiva all'adozione di nuove tecniche criminogene, dall'altro, il legislatore è estremamente lento ed inefficiente nell'adozione di misure di contrasto. Si vedrà nel prosieguo che gli interventi più significativi in materia di antiriciclaggio sono stati assunti solo nell'arco degli ultimi cinque anni, talora risultando comunque incompleti e bisognosi di essere rafforzati.[160]

2.8 Il *cyberlaundering* nell'ordinamento italiano: analogie e differenze rispetto al riciclaggio "materiale".

Se prestando attenzione alle possibili definizioni rinvenibili in dottrina, come sopra menzionate, la conclusione a cui si è giunti è che il *cyberlaundering* si configuri come forma ibrida tra riciclaggio e *cybercrime* tale fenomeno rimane tuttavia sfuggente e i contorni di disciplina assai sfumati, a causa di una riscontrata riluttanza dei legislatori, sia nazionali che sovranazionali, di prendere posizione in materia, nonostante l'allarmante esigenza di fronteggiare il problema.

Sembra dunque utile in questa sede, vagliare l'effettiva compatibilità tra elementi costitutivi del riciclaggio e *cyberlaundering*, al fine di non lasciare alcun vuoto di tutela.

Alla luce della sua natura, essenzialmente digitale, il *cyberlaundering* si realizza senz'altro attraverso condotte molto diverse rispetto a quelle "dello spallone che porti la valigia di denaro contante oltre confine"[161].

La formulazione ex artt. 648 *bis* c.p. è estremamente ampia, come *supra* esplicato; pertanto, può affermarsi che sia senz'altro idonea ad abbracciare la molteplicità di condotte svolgentesi *online* destinate al riciclaggio di denaro.

---

[160] Efficace è la metafora utilizzata da E. SAVONA E M. MIGNONE, *op. ult. cit.*, 2004 "*the scenario outlined above demonstrates that the impact of ICTs has produced relevant changes to crime and consequently to the law enforcement for detecting it. It is like a fox hunting where the fox (criminals) are frequently better-off than hunters (law enforcement).*"

[161] L. PICOTTI, *op. ult. cit.*, 2018, cit. p. 610

Non sembra, quindi, necessaria l'apposita previsione di elementi tecnici descritti nella disposizione normativa che richiamino in via esplicita l'utilizzo delle nuove tecnologie informatiche.[162] Tuttavia, trattasi pur sempre di due fenomeni distinti, che richiedono pertanto le dovute precisazioni.

Prendendo avvio dalla sussistenza dei tratti in comune, è pacifico come il bene giuridico leso dal *cyberlaundering* sia il medesimo leso nel caso di riciclaggio tradizionale. Anche se la movimentazione del denaro avviene *online*, in ogni caso ad essere lesi sono l'ordine economico e l'amministrazione della giustizia, alla luce delle perdite erariali in termini di tasse e della circolazione di denaro non tracciabile che ogni Stato silenziosamente ospita.

Per quanto concerne ancora i tratti in comune, devono poi considerarsi, parimenti a quanto richiamato nel capitolo I in tema di riciclaggio, la condotta tipica e l'elemento soggettivo. Non sono riscontrabili sul punto sostanziali differenze: infatti, anche nel caso del *cyberlaundering*, sembra appropriato recuperare la configurabilità dell'elemento soggettivo del dolo generico[163] e dell'idoneità della condotta a dissimulare la provenienza illecita del bene. In primo luogo, si richiede che il *cyberlaunderer* sia a conoscenza o abbia il sospetto che i fondi in suo possesso sono illeciti e che, per questo, agisca al fine di: (i) nascondere i proventi illeciti dalle Autorità; (ii) dissimulare la natura, il luogo o la fonte dell'origine criminosa; (iii) aggirare l'obbligo di legge di dichiarare il compimento dell'operazione.

In via di primo inquadramento, può dunque concludersi che la struttura generale del *cyberlaundering* sia speculare a quella del riciclaggio "materiale" nella sua forma più tradizionale.

---

[162] Questa argomentazione non sarebbe possibile per i reati informatici in senso stretto tipo la frode informatica, che invece richiedono necessari riferimenti alle TIC.

[163] Cfr. A. LESLIE, *op. ult. cit.*, p. 211 ove si utilizza l'espressione "*mens rea*" per indicare "*the state of mind of the accused – the so called internal or subjective element – which tends to justify the conduct, or act, or, omission of the accused*".

Tuttavia, è doverosa qualche specificazione. A rendere il *cyberlaundering* un fenomeno *sui generis*, oltre a quanto sopra descritto riguardo alla dimensione del *Cyberspace*, è, in primo luogo, l'utilizzo di un *computer*[164]. Ma, a parte questa osservazione, non assai rilevante, sembra più opportuno invece focalizzarsi sui c.d. reati-presupposto[165]. Non rinvenendosi in letteratura, in punto di reati-presupposto, elencazioni tassative, si ritiene vi siano ricomprese tutte quelle condotte offensive idonee a generare denaro o utilità illecite.[166]

In relazione al *cyberlaundering*, deve tenersi conto di tutti i reati informatici, come il *phishing*[167] e la frode informatica. Per quanto concerne il *phishing*, trattasi dell'utilizzo abusivo di tecniche informatiche, i.e. di *social engineering* – al fine di indurre la vittima a fornire i propri dati personali digitali necessari per accedere a servizi di *home banking*, di regola, a scopo di truffa ex art. 640 c.p. o di frodi informatiche, aggravate di norma dal furto di identità digitale.[168] Ancora, si pensi all'acquisizione illecita di password o altre forme di accessi abusivi a sistemi informatici.

In punto di *phishing* come reato presupposto si può menzionare, a titolo esemplificativo, il caso di un *phisher*, il quale reperiva illecitamente denaro, agendo per mezzo di un c.d. *financial manager*, il quale a sua volta tratteneva provvigioni per operazioni di trasferimento di somme di denaro versandole poi a favore del *phisher*, di regola in conti correnti accesi all'estero. Si è

---

[164] In argomento, si veda A. REYES, A. BRITTSON, K. O'SHEA, J. STEELE, *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors*, 2007; D.S. WALL, *Cybercrime: The transformation of crime in the information age* (*PCSS-Polity Crime and Society*), 2007.

[165] Si segnala la differenza tra reati-presupposto e reati strumentali. I reati strumentali sono stati definiti autonomamente punibili ex art. 81 c.p. nella pronuncia di Cass. Pen. sez. II, n. 47147, 2013

[166] Sul punto, si veda la Raccomandazione 3, FATF, 2012, p. 12

[167] In argomento, R. FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in Riv. it. dir. proc. pen., 2007, n. 1-3, p. 899

[168] Cfr. L. PICOTTI, *Profili penali del Cyberlaundering: Le nuove tecniche di riciclaggio*, cit. p. 610 e ss.

ritenuta pacifica la configurabilità del reato di riciclaggio in capo al *financial manager*, in quanto consapevole della provenienza illecita del denaro[169].

Accanto all'espansione dei reati presupposto, assistiamo anche ad una corrispondente emersione di reati strumentali al delitto di riciclaggio. Tale categorizzazione è frutto della più recente elaborazione giurisprudenziale, la quale ne ha affermato l'autonoma punibilità[170]. L'occasione pratica su cui la Suprema Corte ha avuto modo di elaborare tale ulteriore categoria risale ad un caso di utilizzo indebito, da parte di un rappresentante di una società, di carte clonate per movimentare proventi illeciti.

Si trattava, in particolare, di carte di credito che erano già state clonate da soggetti terzi ignoti, utilizzate dal rappresentante di una società per movimentare denaro di provenienza illecita – in questo caso proprio il frutto della falsificazione delle carte stesse – su alcuni conti della società. Trattasi, dunque, di delitti che potenzialmente possono costituire reati presupposto idonei a produrre proventi illeciti, destinati poi ad essere ripuliti. La giurisprudenza ha ritenuto, dunque, di separare la clonazione delle carte – reato strumentale – dall'utilizzazione vera e propria delle stesse a fini di riciclaggio.

2.9 Prospettive interne *de iure condendo* di contrasto al *cyberlaundering*: è necessaria la creazione di una fattispecie autonoma?

In considerazione dell'analisi della disciplina del reato di riciclaggio e dei profili emergenti del fenomeno del *cyberlaundering*, all'esito del percorso

[169] Si veda in proposito la sent. Trib. Milano, 10 dicembre 2007. In argomento, v. DI PAOLO E., *Cyber crime. Il Phishing: prospettive di un delitto*, in Archivio penale Web, 2017, n.2, p. 18. L'Autore, in punto di elemento soggettivo del *financial manager*, rileva come "Il dolo di ricettazione o riciclaggio può dirsi sussistente in capo al financial manager solo allorquando, in forza di precisi elementi di fatto, si possa affermare che questi si sia seriamente rappresentato l'eventualità della provenienza delittuosa del denaro e, nondimeno, si sia comunque determinato a riceverlo e, se del caso, trasferirlo all'estero con le modalità indicate dal phisher. In termini soggettivi, occorre qualcosa di più del mero sospetto della provenienza illecita del denaro: un atteggiamento della psiche inequivoco, un impulso cosciente della volontà che implica una scelta consapevole tra l'agire, rappresentandosi la concreta possibilità della provenienza della cosa da delitto, e il non agire."

[170] Si fa riferimento alla pronuncia Cass. Pen., sez. II, 24 ottobre 2013, n. 47147

argomentativo appena svolto, sembra pacifico poter affermare che sotto un profilo repressivo-sanzionatorio sia possibile contrastare *il cyberlaundering* facendo ricorso alla disciplina codicistica *ex* artt. 648 *bis* e 648.1 *ter* c.p.

Tale applicazione, seppur priva di forzature interpretative e di violazioni del divieto di analogia, necessita tuttavia di un'implementazione regolamentare da parte del legislatore, al fine di dipingere una più efficace tutela del "*cybericiclaggio*". In questo senso, sono ipotizzabili diverse soluzioni di disciplina.

In primo luogo, potrebbe configurarsi la creazione di una fattispecie autonoma che sanzioni la sostituzione, il trasferimento e il compimento di altre operazioni – e dunque, la condotta tipica del reato di riciclaggio ex art. 648 *bis* c.p. – poste in essere specificamente nel *web*. I reati presupposto, produttivi dei proventi illeciti da riciclare, sarebbero sia quelli realizzati *online*, come *phishing* o frode informatica, sia quelli realizzati fisicamente i cui proventi sarebbero poi trasferiti *online* e ripuliti e reinvestiti tramite il *web*.

Tuttavia, poiché, al pari del delitto di riciclaggio, tale possibile fattispecie autonoma si configurerebbe come reato comune, tutelerebbe il medesimo bene giuridico protetto dalla disposizione ex art 648 *bis* c.p. e sarebbe proponibile sempre il dolo generico come elemento soggettivo, parrebbe forse una scelta più efficiente, anche per evitare inutili duplicazioni di fattispecie criminose, per il Legislatore ricorrere ad una soluzione sanzionatoria diversa.

Sul punto, in alternativa, come messo in luce da autorevole dottrina[171], potrebbe proporsi l'introduzione di un'aggravante speciale[172] alla fattispecie

[171] V. PLANTAMURA, *Il cybericiclaggio*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *op. ult. cit*., pp. 859 e ss.

[172] Sul punto, si veda F. POMES, *op. ult. cit.*, p. 173. L'Autrice compara l'ipotesi in discorso con quanto realizzato dal legislatore in contrasto al terrorismo internazionale, introducendo la disposizione ex art 270-*quinquies* c.p., la quale fa espressa menzione di strumenti telematici o informatici utilizzati a fini terroristici. Per un'analisi più approfondita del finanziamento di gruppi terroristici o di cellule o lupi solitari ricorrendo alle criptovalute, si rinvia al contributo di L. STURZO, *Bitcoin e Riciclaggio 2.0*, in *Dir. pen. contemp*., 2/2018, pp. 31 e ss.

ex art. 648 *bis* c.p., onnicomprensiva di ogni condotta riciclatoria realizzata *online*. A chi scrive sembrerebbe più consono optare per questa seconda opzione, che risponderebbe contestualmente sia a nuove esigenze regolatorie senza al contempo comportare un ulteriore aggravamento della normativa nazionale.

Oltre alla disciplina sanzionatoria, in una prospettiva *de iure condendo*, non può trascurarsi la rilevanza della disciplina preventiva, i.e. disciplina antiriciclaggio, che ha fatto il suo ingresso a livello sovranazionale con la Quinta Direttiva 2018/843/UE. Tale Direttiva, se da un lato ha rafforzato i poteri delle Financial Intelligence Units (FIUs), promuovendo maggiore collaborazione tra esse e imponendo più consistenti obblighi di trasparenza fiscale, si è incentrata in particolare nel rafforzamento di obblighi di verifica della clientela di *exchangers* e *wallet providers.* Nell'ordinamento interno, il Legislatore ha recepito la Quinta Direttiva con il D.Lgs. 4 ottobre 2019, n. 125 perseguendo l'obiettivo di riformare i reati di riciclaggio, autoriciclaggio e reimpiego.

Per un'analisi approfondita in argomento, si rinvia al capitolo III.

2.10 Prospettive sovranazionali *de iure condendo* di contrasto al *cyber-laundering*: la futura convenzione ONU sul *cybercrime.*

Considerato il *cyberlaundering* sussumibile nella categoria dei *cybercrime*, seppur in via non esclusiva, in una prospettiva *de iure condendo*, sembra utile guardare ai provvedimenti sovranazionali pensati in materia per esercitare un'azione repressiva incisiva contro ogni crimine commesso *online*.

Con la Risoluzione 74/247 del 27 dicembre 2019[173], l'Assemblea generale delle Nazioni Unite ha istituito un Comitato *ad hoc* al fine di

[173] Dal titolo "*Countering the use of information and communications technologies for criminal purposes"*

elaborare una Convenzione sulla lotta all'uso delle nuove tecnologie a fini illeciti. In accordo con la Risoluzione, il Comitato neocostituito aveva convocato una sessione di tipo organizzativo per agosto 2020 a New York, poi posticipata a maggio 2021 per motivi legati alla pandemia da Covid-19.

In questa sede, è stata assunta un'ulteriore risoluzione[174] la quale prevede la pianificazione di almeno sei sessioni di lavoro durante le quali formulare una bozza di Convenzione da sottoporre all'Assemblea Generale. La prima sessione si è svolta a New York tra febbraio e marzo 2022.

Alla luce della necessità di un nuovo strumento di contrasto ai crimini informatici, si darà breve conto in questa sede delle proposte avanzate dai principali paesi. Per iniziare, il governo degli U.S.A. ha messo in luce come la pandemia abbia incrementato l'utilizzo di strumenti informatici per scopi criminali.

A suffragio di questa osservazione, è riscontrabile un aumento percentuale di attacchi *hacker* e reati informatici in generale nel periodo intercorso tra il 2020 e il 2022. La principale proposta sul fronte americano riguarda una valorizzazione della disciplina di ricerca delle prove rilevanti (*e-evidence*) ed un'implementazione dell'apparato assistenziale e di cooperazione tra Stati per i paesi dotati di minori risorse.[175] Si segnala in questa sede che il governo americano ha anche evidenziato da un lato l'esigenza di contrastare i crimini cyber-dipendenti, ossia tutti gli illeciti passibili di essere realizzati completamente nel mondo digitale e che dunque non potevano configurarsi prima della diffusione dei sistemi informatici.

D'altro canto, è stato parimenti messo in rilievo il rischio di estendere la disciplina dei reati tradizionali a tutti i *cybercrimes*, solamente perché realizzati tramite un dispositivo informatico, evidenziando l'esistenza di

[174] Risoluzione 75/282 dell'Assemblea Generale ONU, 26 maggio 2021, dal titolo "*Lotta all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali*".

[175] A. MATTARELLA, *La futura convenzione ONU sul Cybercrime e il contrasto alle nuove forme di criminalità informatica*, in Sistema Penale, Fasc. 3/2022, p. 60.

categorie di reati che non possono essere assimilati *tout court* ai reati tradizionali e che necessitano di ulteriori tutele perché connotati da una maggiore offensività se realizzati attraverso il computer, da una lesione che si realizza molto più velocemente e anche un pregiudizio ancor più grave.

Sul punto, per quanto riguarda la posizione dell'Unione Europea, giova innanzitutto premettere che, con l'entrata in vigore del Trattato di Lisbona nel 2007, la criminalità informatica è stata riconosciuta, ex art. 83 TFUE, come un fenomeno criminoso di natura grave e di portata transnazionale[176] e che, alla luce di ciò, nonostante l'Unione europea non detenga competenza diretta in materia penale, bensì solo indiretta, attraverso l'emanazione di direttive volte ad armonizzare i sistemi penali degli Stati membri, il Legislatore eurounitario non rimane in ogni caso esente dall'elaborare norme necessarie al contrasto di crimini connotati da seria gravità su scala transnazionale[177]. Procedendo in questo senso, il Legislatore potrebbe, dunque, avanzare proposte in vista della c.d. "europeizzazione" della lotta alla criminalità organizzata, a fondamento della quale i principali obiettivi da raggiungere dovrebbero essere, in primo luogo, la previsione di misure sovranazionali integrative di quelle nazionali e regionali per contrastare – non solo la criminalità organizzata – ma anche la c.d. *cybercriminalità*.

A seguito di questa puntualizzazione sulla posizione dell'Unione europea, tornando a volgere lo sguardo alle disposizioni della futura Convenzione ONU dovrebbero concentrarsi maggiormente sulle fattispecie penali sostanziali da reprimere e sui meccanismi procedurali e di cooperazione. Altra corrispondente esigenza a cui rispondere riguarda il

[176] Cfr. A. MATTARELLA, *op. ult. cit.*, p. 64

[177] In questo processo di armonizzazione e sviluppo della normativa europea, potrebbe darsi sostanziale rilievo alla Procura Europea (EPPO), nata nel 2017. Le sue competenze sono principalmente circoscritte alla repressione di frodi lesive degli interessi finanziari dell'Unione. Tuttavia, ex artt. 83 e 86 TFUE, è possibile estendere il raggio d'intervento ai "*serious crimes having a cross border dimension*". In generale, sulla competenza penale dell'Unione europea v., di recente, i vari contributi contenuti in C. GRANDI (a cura di), *I volti attuali del diritto penale europeo*, Pisa, 2021.

mantenimento della tutela dei dati personali e il mantenimento di garanzie di libertà di espressione.[178]

Con riguardo alla Convenzione ONU, gli Stati hanno enfatizzato il ruolo chiave e la necessità di implementazione della c.d. sorveglianza elettronica[179]. In via generale può dirsi che nella categoria della c.d. "sorveglianza elettronica" sono compresi tutti gli strumenti investigativi, come ad esempio anche il captatore informatico, che attraverso l'utilizzo delle nuove tecnologie perseguono gli stessi risultati dei mezzi di ricerca della prova tipici e atipici, seppur superando le difficoltà fisiologiche insite nella natura delle intercettazioni tradizionali.

Alla luce di queste non trascurabili necessità, si delineano esigenze di armonizzazione tra ordinamenti al fine di creare una rete di tutela sovranazionale che non costringa a rimettere la regolamentazione dell'attività investigativa ad ogni singolo Stato, il che comporta una normativa puntellata e disomogenea.[180]

---

[178] A tal proposito, imprescindibile risulta il rispetto dei principi di proporzionalità e necessità. Il primo di questi, inteso in senso formale, è scolpito nell'art. 49, co. 3, della Carta dei diritti di Nizza, il quale dispone che «L'intensità delle pene non deve essere sproporzionata rispetto al reato.» Il principio di proporzionalità in senso materiale deve essere, invece, inteso come sussistenza della proporzionalità tra i mezzi impiegati, dunque la sanzione inflitta, e gli scopi perseguiti, ossia la rieducazione del reo. In altre parole, questa seconda accezione, richiede che l'individuo colpevole non sia punito più di quanto sia utile. Il secondo principio, c.d. di necessità o di indispensabilità della pena, è posto all'art. 83 2° comma TFUE dove si dispone che «Allorché il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri in materia penale si rivela indispensabile per garantire l'attuazione efficace di una politica dell'Unione (...), norme minime relative alla definizione dei reati e delle sanzioni nel settore in questione possono essere stabilite tramite direttive». Per ulteriori approfondimenti si veda C. SOTIS, *I principi di necessità e proporzionalità della pena nel diritto dell'Unione europea dopo Lisbona*, in Riv. Dir. Pen. Contemp., 1/2012, p. 111 e ss.

[179] Per una definizione di questo strumento si rinvia agli articoli 20 della Convenzione di Palermo e 50 della Convenzione di Merida. Le tecniche di sorveglianza elettronica sono molteplici, in via esemplificativa si riportano di seguito alcune tra le più importanti: audiosorveglianza attraverso intercettazioni telefoniche (phone trapping); intercettazioni ambientali attraverso microspie (room bugging); videosorveglianza, termografia o rilevazione delle radiazioni infrarosse. Vi rientrano anche gli *spyware* e i *cookies* utilizzati sul computer e su internet.

[180] A. MATTARELLA, *op. ult. cit.*, p. 72

Così come ogni forma più recente di *cybercrime*, le nuove frontiere di contrasto ai reati informatici, così come anche al *cyberlaundering*, secondo queste nuove prospettive sembra risiedere nella strutturazione di un programma di cooperazione d'indagine di tipo transnazionale, basato su un rafforzamento nella circolazione di informazioni, di assistenza tecnica e di cooperazione giudiziaria e di polizia.

Sotto il profilo del diritto penale sostanziale, si ritiene senz'altro necessaria una maggiore chiarezza e riorganizzazione delle categorie di studio, quali ad esempio reati informatici e reati cibernetici, in vista di uno snellimento e di una semplificazione dell'attività del Legislatore per la configurazione di forme di tutela omogenee che non lascino adito a dubbi esegetici. Si è visto, infatti, come non sia immediato collocare *tout court* il *cyberlaundering* all'interno di una delle già menzionate categorie, configurandosi esso come fenomeno assai sfaccettato e poliforme. Si ritiene, che solo da una classificazione che sia *ab origine* cristallina, possa conseguirne un tentativo regolatorio più chiaro e deciso, idoneo anche ad abbracciare la molteplicità di ipotesi in cui il *cyberlaundering* può manifestarsi.

Il prosieguo della trattazione si focalizzerà da ora sull'analisi dello strumento finanziario delle criptovalute, evidenziandone i maggiori profili di rischio di riciclaggio, anche alla luce dei pareri emessi dalle Autorità di Vigilanza.

CAPITOLO III

LE CRIPTOVALUTE E LA LORO FORZA ATTRATTIVA PER LE ATTIVITÀ DI RICICLAGGIO

3.1 Le criptovalute: un fenomeno di rilevanza globale

Come sopra accennato, ad oggi la potenzialità offensiva del *cyberlaundering* si manifesta principalmente in riferimento ad operazioni che hanno ad oggetto valute virtuali[181].

La rivoluzione tecnologica, *i.e.* la digitalizzazione, dei sistemi economici ha introdotto cambiamenti epocali anche nel settore finanziario. In particolare, con la diffusione delle valute virtuali, la fisionomia dei mercati è ininterrottamente sottoposta a molteplici mutamenti e, dunque, richiede costantemente l'adeguamento delle legislazioni nazionali e sovranazionali al fine di fronteggiare le nuove esigenze di tutela che si manifestano.

Inquadrabili come frutto della c.d. democratizzazione dei mercati[182], le valute virtuali costituiscono ad oggi uno strumento assai accattivante nel

[181] F. POMES, *op. ult. cit.*, p. 165

[182] F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti, in Dir. pen. contemp*., 10/2018, p. 22

panorama finanziario: costituendo un ecosistema autonomo, svincolato dai molteplici controlli delle Autorità di vigilanza, figurano ad oggi come strumenti in mano ai privati che permettono di operare sul mercato in uno stato di minacciosa "libertà".

Il loro quadro di disciplina ad oggi risulta tutt'altro che univoco ed omogeneo, richiedendo una difficile armonizzazione tra diverse ma complementari branche del diritto, quali la disciplina antiriciclaggio, la normativa finanziaria e tributaria, la tutela dei consumatori.[183]

Ad oggi, un alto numero di giurisdizioni si è dedicato ad approntare una disciplina – o ad impegnarsi *pro-futuro* a declinare una normativa regolamentare – sulle valute virtuali[184].

Facendo in primo luogo menzione della legislazione domestica, il legislatore italiano, recependo la V Direttiva UE antiriciclaggio[185], si è apprestato ad enucleare una prima impronta di disciplina con il d.lgs. n. 125/2019[186] novellando l'art. 1, comma 2, lett. qq) del d.lgs. 231/2007[187], il

[183] Sul punto, si vedano le riflessioni di D. MAJORANA, *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in Corriere Tributario, 8, 2018, p. 630. "*Fino a quando non sarà possibile istituire regole che presiedano la rete dall'interno, sarà necessario costituire una "cinta daziaria" dotata di alcune "porte" per individuare chi e che cosa passa dal mondo reale a quello virtuale e viceversa. Solo alle transazioni compliant sarà garantito l'accesso al mondo reale, mentre le altre saranno destinate ad essere isolate in quello virtuale*". Sempre in argomento, cfr. F. DI VIZIO, *op. ult. cit*., p. 23.

[184] Per tutti, cfr. E. FRANZA, *Le valute virtuali e prodotti finanziari con sottostanti valute virtuali. Una prima indagine sugli interventi*, in *Foroeuropa*, 2018.

[185] V. *infra*, par. 3.11

[186] Decreto delegato, adottato con la l. 12 agosto 2016, n. 170 intitolato "*Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847*".

Si segnala che con lo stesso d. lgs. 90/2017 sono stati ricompresi nella categoria degli operatori non finanziari destinatari della normativa antiriciclaggio tutti i prestatori di servizi relativi all'utilizzo di valute virtuali, anche se "*limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso*". Il riferimento è diretto ai c.d. *exchanges* che operano delle conversioni con valute che hanno corso legale. In argomento si veda E. CORAPI, R. LENER (a cura di), *I diversi settori del Fintech*, 2019

[187] Il presente decreto è attuativo della Direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo

quale ha introdotto la definizione di 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*".[188] Tale definizione sembra efficacemente riassumibile ricorrendo all'espressione "contante digitale"[189], che racchiude il significato di valuta virtuale in veste di figura ibrida tra moneta fisica ed elettronica[190].

In altre parole, questa definizione nostrana di valuta virtuale ha introdotto una rilevante novità riguardo la funzione delle criptovalute: dall'essere considerati meri strumenti di scambio, il Legislatore le ha annoverate nella categoria degli strumenti di investimento e finanziamento.[191]

Volgendo, poi, l'attenzione sul piano globale, gli U.S.A., su recente impulso dell'attuale Presidente Biden[192], si apprestano a configurare una regolamentazione auspicabilmente completa delle valute virtuali. In particolare, nell'ordine esecutivo emesso dal Presidente a marzo 2022, si legge come le misure prossime ad essere adottate, siano specificamente

---

[188] Per un'analisi sulla natura giuridica delle criptovalute e le definizioni fornite dalle principali Autorità, si rinvia *infra* al par. 3.2

[189] N. PASSERELLI, *Bitcoin e antiriciclaggio*, in *Gnosis*, Rivista italiana di intelligence, reperibile al sito: www.sicurezzanazionale.gov.it , 2016

[190] Cfr. F. POMES, *op. ult. cit.,* p. 161. L'Autrice definisce la moneta virtuale come "*tertium genus*" tra moneta fisica e quella elettronica.

[191] In argomento, cfr. R.M. VADALÀ, *Criptovalute e cyberlaundering: novità antiriciclaggio della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in Sistema Penale, 2020.

[192] Come riportato in https://finanza.lastampa.it/News/2022/03/09/criptovalute-la-mossa-di-biden-firma-ordine-esecutivo/MTMxXzIwMjItMDMtMDlfVExC "*Nel dettaglio, l'ordine esecutivo solleciterà le autorità di regolamentazione federali a rivedere i rischi per i consumatori, gli investitori ed il mercato di un mercato cripto da circa 1.750 miliardi di dollari. Inoltre stabilirà una politica nazionale "sulla stabilità finanziaria; sulla finanza illecita; sulla leadership statunitense nel sistema finanziario globale, sulla competitività economica; sull'inclusione finanziaria e sull'innovazione responsabile" (...) In particolare, l'ordine esecutivo chiede di esaminare come le criptovalute possano minare gli sforzi statunitensi per combattere il riciclaggio di denaro, preoccupazioni particolarmente pressanti dopo che gli Stati Uniti hanno imposto sanzioni alla Russia in risposta alla sua invasione dell'Ucraina*."

mirate a: (i) proteggere i consumatori; (ii) garantire stabilità finanziaria; (iii) contrastare attività illecite.[193]

Estendendo poi lo sguardo anche alla posizione di altre giurisdizioni, la Germania, ad esempio, ha definito le criptovalute come unità di conto, ricomprendendole all'interno della categoria degli strumenti finanziari[194]. Ancora, la Francia è attualmente impegnata nella stesura di un'apposita disciplina di vigilanza sulle valute virtuali al fine di evitare ogni tipo di speculazione o manipolazione finanziaria. Un primo passo, sempre in territorio francese, nel mese di maggio 2022, è rappresentato dalla registrazione di "*Binance*" in qualità di *digital asset service provider* (DASP) da parte del regolatore dei mercati finanziari, in seguito al *nulla osta* fornito da parte dell'Autorité de contrôle prudentiel et de résolution (ACPR). "*Binance*" costituisce un mercato di scambio di criptovalute, in costante e crescente espansione e la Francia, in questa occasione, si è configurata come il primo mercato eurounitario ad approvare una vera e propria "borsa dell'Unione Europea"[195].

Ancora, la Cina ha, in tempi recenti, dedicato maggiore attenzione alla regolamentazione e al controllo delle criptovalute.[196] Essa vanta nel suo

---

[193] Secondo quanto emerso dai dati stimati dalla Casa Bianca, circa il 16% degli americani adulti – 40 milioni di persone circa – ha investito, scambiato o utilizzato criptovalute. Inoltre, nell'ordine esecutivo in discorso, il Presidente Biden ha ufficialmente proposto di valutare la creazione di un dollaro digitale controllato dalla Banca Centrale Americana, ovvero la Federal Reserve.
Cfr. sul punto l'articolo datato 10 marzo 2022, in *Rivista online* "*Dealflower | Financial and Legal News*" al link https://dealflower.it/biden-ha-firmato-un-ordine-esecutivo-sulle-criptovalute/

[194] Si fa riferimento alla legge entrata in vigore in Germania il 1° luglio 2020, il quale concede ai fondi speciali tedeschi (c.d. *Spezialfonds*) di investire fino al 20% dei loro portafogli in Bitcoin e altri cripto-asset.

[195] In argomento, si veda l'articolo di Borsa Italiana, reperibile al link: https://www.borsaitaliana.it/borsa/notizie/radiocor/finance/dettaglio/binance-obtains-regulator-clearance-in-france-nRC_05052022_1923_759145265.html?lang=en?lang=en

[196] Cfr. E. FRANZA, *op. ult. cit*., 2018 "*Da ricordare che la Cina è diventato il più grande mercato di produzione e di scambio di Bitcoin al mondo. (...) Nel gennaio 2018, le autorità di Seul hanno annunciato che le banche locali non potranno dare corso alle operazioni provenienti da conti anonimi per il trading in cripto valute e ciò al fine dichiarato di poter*

territorio, la circolazione di una criptovaluta *sui generis*, lo Yuan digitale (e-CNY), ossia una valuta digitale che funge da mezzo di pagamento e, facendo riferimento alla Banca Centrale Cinese, presenta la peculiarità per cui il suo valore equivale al denaro fisico, venendo dunque meno la volatilità che caratterizza di norma le criptovalute in generale.[197]

Vi sono, tuttavia, alcuni Paesi in cui la criptovaluta costituisce un vero e proprio nemico: si veda, ad esempio, la Russia. Nelle prime settimane del 2022, la Banca Centrale russa ha abbozzato una proposta di divieto di emissione e di investimento nei confronti di tutte le banche russe, nel tentativo di fermare ogni potenziale scambio di cripto con la valuta tradizionale[198].

3.2 La controversa natura giuridica delle criptovalute.

Avendo inquadrato le criptovalute alla stregua di un'innovazione radicale di risonanza globale, che sta gradualmente modificando l'assetto del mercato mondiale, ai fini delle nostre riflessioni sui risvolti penalistici delle stesse, sembra opportuno procedere in primo luogo con un loro inquadramento giuridico.

Ad oggi, la natura giuridica delle criptovalute è assai discussa e controversa: i legislatori nazionali e le istituzioni europee da anni perseguono il tormentato tentativo definitorio delle stesse, con l'obiettivo di porre ordine all'interno di un ecosistema in costante cambiamento e di difficile perimetrazione.

---

rendere tracciabili e trasparenti le transazioni e mettere un freno al riciclaggio ed alle attività criminali, oltre che alla speculazione e all'evasione fiscale".

[197] Cfr. in argomento l'articolo di R. FATIGUSO, 18 marzo 2022, in Sole24Ore, reperibile al link: https://www.ilsole24ore.com/art/cosi-yuan-digitale-puo-circolare-tutta-cina-AElPD7KB

[198] Cfr. l'articolo di R. SAVOJARDO, in MilanoFinanza, 20 gennaio 2022, reperibile al link: https://www.milanofinanza.it/news/la-banca-centrale-russa-propone-il-divieto-di-trading-e-mining-di-criptovalute-202201201643203829

Giova premettere alcuni tentativi definitori proposti dalle maggiori Autorità di Vigilanza e controllo, per poi calarsi nei tentativi di inquadramento avanzati da giurisprudenza e dottrina.

La Banca Centrale Europea (BCE) nel 2012 ha fornito, per prima, una definizione di valuta virtuale come "*moneta virtuale non regolata che è controllata e gestita solo dal proprio inventore e utilizzata dagli appartenenti ad una comunità virtuale*"[199]. Pochi anni dopo, la Banca d'Italia ha anch'essa improntato una definizione di valute virtuali come "*rappresentazione digitale di valore, utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente*"[200]. Successivamente, nel 2014, la definizione – forse più completa – è stata enucleata in un *report* dell'European Banking Authority, il quale ha definito le valute virtuali come "*rappresentazioni digitali di valore che non sono emesse da una banca centrale o autorità pubblica né sono necessariamente collegate a una valuta avente corso legale, ma che vengono utilizzate da una persona fisica o giuridica come mezzo di scambio e che possono essere trasferite, archiviate e negoziate elettronicamente*"[201].

Tali definizioni proposte dalle maggiori Autorità di Vigilanza e controllo devono senz'altro essere integrate con i contributi giurisprudenziali che si sono pronunciati sul tema, ma che tuttavia risultano numericamente scarsi, e le opinioni dottrinali, invece numerose.

Prendendo avvio dalla giurisprudenza, è possibile menzionare poche pronunce che hanno approntato una possibile categorizzazione

[199] EBA, *Virtual Currency Schemes,* 2012

[200] Cit. da Documento Banca d'Italia, *Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*, 30 gennaio 2015. Si veda anche la definizione fornita dall'ESMA, la quale si riferisce alle criptovalute come "*rappresentazioni digitali di valore che non sono né promosse né garantite da una banca centrale o da un'autorità pubblica e che non hanno corso legale*".

[201] EBA, *Opinion on virtual currencies*, 2014.

definitoria di valuta virtuale, con la precisazione che non si è trattato di definizioni generali ed universali, ma strettamente legate alla funzione da essa svolta.

La prima sentenza considerata è nostrana ed è ritenuta meritevole di menzione in quanto l'organo giudicante definisce la valuta virtuale come "strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni *online*" [202]. A conforto di questa perifrasi, la stessa pronuncia richiama la risoluzione n.72/E, datata 2 settembre 2016, emessa dall'Agenzia delle Entrate[203], dove viene sancita la soggezione ad imposizione fiscale del reddito derivato dall'attività di intermediazione nella compravendita di criptovaluta. Tale assoggettamento fiscale viene riconosciuto in forza dell'argomentazione per cui tale attività di intermediazione costituisce una prestazione di servizi finanziari. La stessa risoluzione richiama a sua volta una pronuncia del 2015 della Corte di Giustizia Europea[204], che affronta il tema delle criptovalute sotto il profilo fiscale, in particolare assimilando un'operazione di cambio di valuta

[202] Si fa riferimento all'isolata pronuncia del Trib. Verona, sent. 195 del 2017.Si veda sul punto anche la nota a sentenza di C. TATOZZI, *Bitcoin: natura giuridica e disciplina applicabile al contratto di cambio in valuta avente corso legale*, reperibile in Banca Dati *online* al sito www.Ridare.it, in fascicolo datato 9 agosto 2017. L'Autore rileva come la soluzione definitoria proposta dal Tribunale di Verona sia "ondivaga" e che "se da un lato sembra riecheggiare la tesi dottrinale che classifica il bitcoin alla stregua di moneta privata e/o complementare, dall'altro lato, non chiude la porta ad un possibile inquadramento di tale entità in termini di vero e proprio *strumento* ovvero *prodotto finanziario*". Per approfondimenti ulteriori si veda anche E. CORAPI, R. LENER (a cura di), *I diversi settori del Fintech*, 2019 e M. CIAN, C. SANDEI, *Diritto del Fintech*, 2020.

[203] AGENZIA DELLE ENTRATE, *Trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali*, 2016. Si segnala che, più recentemente, sempre l'Agenzia delle Entrate, rispondendo a un'istanza dell'interpello 956-39/2018 reperibile in www.webeconomia.it , ha ribadito il suo precedente orientamento, somministrando informazioni specifiche sulla tassazione del reddito da cessione di criptovalute in capo al percipiente.

[204] C.G.U.E., sez. V, n. 264, 2015. In argomento, vedi anche M. DA ROLD, *Innovazione tecnologica ed implicazioni penalistiche. Le monete virtuali*., in Giurisprudenza Penale Web, 2, 2019, p. 6

tradizionale con criptovalute e viceversa ad una prestazione a titolo oneroso, per questo soggetta all'Imposta sul Valore Aggiunto (IVA)[205].

È così che il Tribunale di Verona, nella vicenda oggetto di pronuncia, assumendo che la compravendita di valute virtuali abbia una natura contrattuale, afferma che questa è giuridicamente inquadrabile alternativamente come "attività professionale di prestazioni di servizi a titolo oneroso, svolta in favore di consumatori" oppure di "offerta al pubblico di prodotti finanziari" o, ancora, di "servizi e attività di investimento in valori immobiliari". Il passaggio logico successivo, dunque, induce ad identificare le criptovalute come strumenti finanziari, assoggettabili alla normativa del T.U.F.

Sempre in giurisprudenza, l'anno successivo rispetto alla pronuncia del Tribunale di Verona, il Tribunale di Brescia – e successivamente, con lo stesso orientamento, anche la Corte d'Appello di Brescia – si è pronunciata sulla natura delle criptovalute, negando che possano essere assimilate a beni in natura, definendoli incapaci di essere soggetti ad una valutazione economica attendibile, essendo il loro sviluppo e la loro diffusione ancora "*in fase sostanzialmente embrionale*"[206].

A suffragio di questa impostazione, ricorre anche una recentissima pronuncia della Cassazione Penale[207] in tema di Bitcoin, la quale ha affermato che "Ove la vendita di bitcoin venga reclamizzata come una vera e propria proposta di investimento, si ha una attività soggetta agli adempimenti di cui agli artt. 91 e ss. (…) la cui omissione integra la

[205] La sentenza appena citata della C.G.U.E. ha disposto, sul punto, che *"costituiscono prestazioni di servizi effettuate a titolo oneroso (...) operazioni (...) che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale (...) e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti*".

[206] Cfr. Trib. di Brescia, 25/07/2018, n.7556, in *Rivista del Notariato*, 2018, 6, II, 1283 e Corte d'Appello di Brescia, sez. I, 30 ottobre 2018, in *Rivista dei Dottori Commercialisti*, 2019, 1, 52.

[207] Cass. Pen., sez. II, 10 ottobre 2021, n.44337

sussistenza del reato di cui all'art. 166, comma 1, lett. c), t.u.f. (…); *pertanto, allo stato, può ritenersi il bitcoin un prodotto finanziario qualora acquistato con finalità d'investimento*: la valuta virtuale, quando assume la funzione, e cioè la causa concreta, di strumento d'investimento e, quindi, di prodotto finanziario, va disciplinato con le norme in tema di intermediazione finanziaria (art. 94 ss. t.u.f.), le quali garantiscono attraverso una disciplina unitaria di diritto speciale la tutela dell'investimento."[208] Può concludersi, quindi, che secondo giurisprudenza, le criptovalute rientrino nel *genus* degli strumenti finanziari.

Contrariamente ai pochi riscontri giurisprudenziali, si deve invece segnalare che la dottrina ha proposto una notevole varietà di opzioni definitorie di criptovalute. Di tale ventaglio si darà breve conto di seguito, scorrendo i più rilevanti tentativi menzionati dagli esperti e, tentando di formulare una nuova proposta definitoria[209].

Una prima ricostruzione di criptovaluta riprende il concetto di "*new properties*"[210] o, altrimenti, beni immateriali, ossia beni *nuovi* sussumibili nella definizione civilistica di bene ex art. 810 cod. civ., seppur prive del requisito della materialità.[211]

---

[208] La massima della sentenza, datata 1° dicembre 2021, è rinvenibile nella banca dati *Diritto & Giustizia*, menzionata in *Banca Dati DeJure.*

[209] In argomento, per tutti, si veda V. DE STASIO, *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca, borsa, tit. cred.*, 2018, I, p. 747 ss.; G. RINALDI, *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contr. e impr.*, 2019, p. 257 ss

[210] Cfr. il contributo di C. REICH, *The New Property,* in *The Yale Law Journal*, Vol. 73, No. 5, 1964, pp. 733-787. L'autore evidenzia l'accezione del termine "*property*" non tanto come rapporto esclusivo di appartenenza di un bene ad un soggetto, quanto più il novero dei diritti che consentono il godimento o l'utilizzo di un bene e tutti i diritti, anche su beni immateriali, di cui il proprietario dispone.

[211] S. CAPACCIOLI, *Criptovalute e bitcoin*, 2015 p. 142. Sembra calzante l'analogia menzionata dall'autore il quale richiama le pronunce di Cass. Civ. sez I, 26 maggio 2000, n. 6957; Cass. Civ. sez III, 12 dicembre 1986, n. 7409; Cass. Civ. sez. I, 30 gennaio 1997, n. 934, le quali hanno riconosciuto il requisito della materialità del bene come non essenziale ai fini definitori ex art. 810 c.c., attribuendo alle quote di società a responsabilità limitata e alle quote di società di persone la natura di bene giuridico.

Tuttavia, come sostenuto da dottrina autorevole[212], definire la criptovaluta come *res* immateriale potrebbe collidere con l'impronta più caratteristica dell'ordinamento italiano, fortemente legata al concetto di cosa e di bene materiali. *A fortiori,* poiché la norma di riferimento, ossia l'art. 810 cod. civ., dispone che "*sono beni le cose che possono formare oggetto di diritti*" e che ancora non è rinvenibile una norma che attribuisca un diritto sulle criptovalute ad un relativo titolare, potrebbe concludersi che, ad oggi, il mercato delle criptovalute sia solo fattuale[213] e che l'identificazione delle stesse come beni non sia, per questo, del tutto corretta.

Percorrendo, quindi, una seconda ipotesi definitoria, ad oggi la più utilizzata ma criticabile, le criptovalute si configurerebbero come "monete", anche se virtuali. Da un lato, sembra difficile sussumere le criptovalute nella definizione di moneta: infatti, in accordo con la teoria statalista, nessuno Stato le ha ancora riconosciute come aventi corso legale nel proprio ordinamento[214].

Diversamente, secondo la teoria economica, parrebbe invece possibile strutturare una definizione di criptovaluta in chiave causale, focalizzandosi sulla sua idoneità ad assolvere, nel medesimo tempo, le funzioni di: (i) mezzo di scambio; (ii) riserva di valore; (iii) unità di pagamento.[215] Tale posizione presta il fianco, però, ad una critica che fa

---

[212] Cfr. 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 (II), fasc. 1, 2017, p. 27.

[213] E. CORAPI, R. LENER (a cura di), *op. ult. cit.*, 2019

[214] Cfr. R. BOCCHINI, *op. ult. cit.,* 2017. Sempre in argomento, e più di preciso, sull'impossibilità di adempiere obbligazioni pecuniarie tramite criptovalute, si veda E. CORAPI, R. LENER (a cura di), *op. ult. cit.*, 2019.

[215] BANCA D'ITALIA, *Le funzioni della moneta e le proposte di "moneta fiscale",* 2017. Reperibile al link: https://www.bancaditalia.it/media/views/2017/moneta-fiscale/index.html. Ciascuna funzione della moneta è così precisata: (i) mezzo di scambio: la moneta può essere utilizzata per l'acquisto di beni e servizi; (ii) riserva di valore: la moneta permette di spostare nel tempo la quota di reddito che non viene utilizzata immediatamente per consumare beni e servizi. In altri termini, consente di conservare (risparmiare) una quota del reddito corrente per spenderlo in futuro; (iii) unità di conto: La moneta si usa per confrontare in maniera omogenea il valore di prodotti e servizi molto diversi tra loro, agevolando così le decisioni economiche e gli accordi contrattuali.

leva sulla inidoneità delle criptovalute ad assolvere questo tipo di funzioni[216]: la funzione di mezzo di scambio, infatti, anche se molto diffusa nelle definizioni in materia, non convince alla luce della considerazione che le criptovalute basano il loro funzionamento su accordi tra soggetti privati e che in larga parte non sono ancora accettate dalla maggioranza del pubblico. Ancora, la loro alta volatilità dei tassi di cambio non le rende utilizzabili come "riserva di valore", anche volendo considerare di operare in un arco temporale di breve periodo.

Infine, la combinazione di una scarsa popolarità tra il pubblico e dell'alta volatilità renderebbero le valute virtuali non adatte ad essere utilizzate come unità di conto, in quanto il loro potere d'acquisto sarebbe non affidabile[217].

Per completezza si segnala, che alcune voci dottrinali, hanno tratto un diverso risultato argomentativo, attribuendo alle criptovalute natura di moneta, pur non avendo corso legale.[218]

Al vaglio delle opzioni appena considerate, se da un lato alcuni[219] sostengono che ricorrere alle categorie definitorie tradizionali appena considerate non consenta di inquadrare esattamente il fenomeno, la soluzione auspicabile potrebbe essere l'adozione di un approccio "a-sistematico" che tenga da un lato come riferimento le categorie tradizionali, ma che ogni volta dia rilievo alla funzione svolta in concreto dalla criptovaluta. Sul punto, anche la BCE ha spesso evidenziato come la definizione di Bitcoin sia variabile a seconda del contesto e del caso di specie.

Ritenendo questa conclusione pur soddisfacente, sembra contestualmente appropriato condividere anche – in via generale – quanto

[216] E. CORAPI, R. LENER (a cura di), *op. ult. cit.*, 2019

[217] E. CORAPI, R. LENER (a cura di), *op. ult. cit.*, 2019

[218] Cfr. M. PASSERETTA, *Bitcoin: il leading case italiano*, in Banca Borsa Titoli di credito, fasc. 4, 2014, p. 472. L'Autore fa riferimento alla "teoria sociale", ai sensi della quale la moneta è definibile come fenomeno sociale, in quanto dipende dalla volontà delle parti, che restano sempre libere di decidere come regolare e svolgere le proprie transazioni.

[219] C. TATOZZI, *op. ult. cit.*, 2017

sostenuto dalla giurisprudenza, nel tentativo di strutturare una disciplina organica sul punto. In altre parole, a chi scrive sembra più calzante la definizione per cui le criptovalute siano identificabili come strumento finanziario[220] e dunque, sottostanti alla disciplina del T.U.I.F.

Contro questa interpretazione potrebbe richiamarsi la formulazione dell'art. 1, comma 2, T.U.I.F., che elenca il novero degli strumenti finanziari – in cui, ad oggi, naturalmente non figurano le criptovalute – poiché sembrerebbe trattarsi di un'elencazione tassativa che dunque non permetterebbe di ricomprendervi anche le criptovalute.

Tuttavia, alla luce dei riscontri giurisprudenziali sopra citati, sia del Tribunale di Verona, che della Suprema Corte di Cassazione, che hanno riconosciuto la natura di strumento finanziario, a suffragio di questa ipotesi esegetica possono essere richiamati ulteriori elementi. Infatti, secondo la Corte di Cassazione, un investimento di natura finanziaria comprende ogni conferimento di una somma di denaro da parte di un soggetto risparmiatore che vanti un'aspettativa di profitto o di remunerazione, pur sempre in presenza di un margine di rischio[221]. La stessa posizione è stata peraltro condivisa da una parte della dottrina[222], secondo la quale all'interno della voce "prodotto finanziario" è possibile ricomprendere ogni strumento utile al risparmio, a condizione che rappresenti un impiego di capitale[223].

Dunque, essendo l'investimento finanziario connotato da tre elementi principali: (i) impiego di capitali; (ii) aspettativa di rendimento; (iii) fattore di rischio correlato all'impiego dei capitali stessi, sembra possibile rinvenire il medesimo schema strutturale anche nel funzionamento delle criptovalute. Infatti, "*il soggetto interessato*

[220] Sul punto, cfr. M. DA ROLD, *op. ult. cit*., 2019

[221] Cfr. Cass. civ., sez. II, 5 febbraio 2013, n. 2736. *Ex multis* Cass. civ., sez. II, 15 aprile 2009.

[222] M. PASSARETTA, *Bitcoin: il Leading Case italiano*, in *Banca borsa tit. cred.*, 4/2017.

[223] F. DI VIZIO, *op. ult. cit*., p. 50

all'investimento, per ottenere bitcoin ha sborsato a) una somma di danaro b') nell'aspettativa di ottenere un rendimento, non necessariamente corrispondente ad una somma di danaro maggiorata rispetto a quella investita c') assumendo su di sé un rischio connesso al capitale investito"[224].

3.3 (Segue) Brevi cenni al sistema *blockchain*

Ai fini della presente trattazione, per una migliore comprensione delle criptovalute e dei rischi ad esse connessi, conviene accennare brevemente alla definizione di *blockchain*[225], ad oggi espressione massima del mondo *Fintech*. Come si vedrà in seguito, la *blockchain* è strettamente legata al funzionamento criptovalute e, come queste, presenta alcune criticità che non possono essere trascurate né dal Legislatore né dalle Autorità al fine di contrastare il fenomeno del riciclaggio in qualsiasi sua forma.

La *blockchain* costituisce uno strumento di validazione, manifestazione della c.d. *distributed ledger technology* (DLT)[226]. Il DLT costituisce a sua volta una modalità di registrazione e condivisione di dati attraverso più archivi – di dati – noti anche come *ledger*, che contengono e sono

---

[224] Cass. Civ., sez. II, 5 febbraio 2013, n. 2736. In argomento F. DI VIZIO, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, in Discrimen.it, 2019

[225] Segue una definizione di "blockchain" contenuta in *Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser*, reperibile al sito https://www.gov.uk. "*A blockchain is a type of database that takes a number of records and puts them in a block (rather like collating them on to a single sheet of paper). Each block is then "chained" to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and corroborated by anyone with the appropriate permissions."*

[226] R. HOUBEN, A. SNYERS, *Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion,* Study requested by the TAX3 committee of the EU Parliament, July 2018, p. 15.

Nell'ordinamento italiano, è rinvenibile la definizione di DLT ex art. 8-*ter* del D.L. 14 dicembre 2018, n. 135, convertito in legge con L. 11 febbraio 2019, n. 12 (Decreto Semplificazioni) come *"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".*

collettivamente mantenuti e controllati da una rete distribuita di *server* informatici, che sono chiamati nodi.[227]

In altre parole, trattasi di un *database* che prevede l'utilizzo di un sistema crittografico, all'interno del quale, con algoritmi matematici destinati a creare e verificare i dati registrati, viene a crearsi una "catena di blocchi"[228] in grado di registrare e contenere al loro interno le transazioni compiute dagli utenti. Tali blocchi sono connessi in rete grazie al c.d. *peer-to-peer system*[229], tramite il quale è possibile che ogni transazione sia registrata e validata dai membri del *network*, senza il controllo di un soggetto terzo e permettendo agli utenti di operare in situazione di parità, affinché la transazione stessa sia immutabile e permanente. In questo modo, la fiducia negli enti fisici, più precisamente, viene rimpiazzata da complessi algoritmi e *network* decentralizzati di utenti, permettendo agli stessi di compiere scambi di denaro direttamente tra di loro[230].

La dottrina ha individuato due categorie principali di *blockchain*: la prima, c.d. aperta – *permissionless* – permette a chiunque di partecipare o abbandonare il *network*, senza che vi sia la necessità dell'approvazione di un ente centrale. Manca, infatti, un titolare centrale del *network* e copie identiche del registro dei dati sono distribuite in ogni suo nodo. La maggior parte delle

---

[227] Cfr. anche World Bank Group, H. NATARAJAN, S. KRAUSE, H. GRADSTEIN, "*Distributed Ledger Technology (DLT) and blockchain*", 2017, reperibile al link http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf.
In argomento, si veda anche G. CASSANO, F. DI CIOMMO, M. RUBINO DE RITIS, *Banche, Intermediari e Fintech. Nuovi strumenti digitali in ambito finanziario,* 2021.

[228] Altrimenti definibile come "consecuzione di unità collegate indissolubilmente e indelebilmente l'una all'altra", cfr. E. GIRINO, *Criptovalute: un problema di legalità funzionante*, in *Rivista di Diritto Bancario*, fasc. IV, 2018, p. 741.

[229] F.A. BIONDI, *How Block- chain technology and its regulation could promote the Capital Markets Union: focus on ICO*, 2019, p. 19 ss.

[230] In argomento, si veda il contributo M. CROCE, *op. ult. cit.*, p. 137. L'autrice rileva come "*la criptomoneta è la valuta della rete per eccellenza, condividendo con essa la ratio e alcune caratteristiche di fondo. Infatti, come la rete Internet è il risultato del movimento di democratizzazione informativa, le valute virtuali sono il prodotto dell'esigenza di democratizzazione finanziaria (...) i valori virtuali agevolano il coinvolgimento dei soggetti più deboli nelle attività commerciali e finanziarie*."

valute virtuali, come Bitcoin, Litecoin, Bitcoin Cash, si basa su queste c.d. *permissionless blockchains.*

La seconda categoria ricomprende, invece, le *blockchains* "chiuse" – *permissioned blockchains* – all'interno delle quali i validatori delle transazioni devono essere selezionati e controllati in una fase preliminare dall'amministratore del *network*. In questi casi, contrariamente a quanto accade con il primo tipo, è molto più semplice verificare l'identità degli utenti, in quanto è la stessa autorità centrale a determinare le regole per decidere chi possa accedervi.

Ai fini della trattazione conviene senz'altro focalizzarsi sul sistema di *blockchain permissionless*, in relazione al quale, connotandosi per la sua natura pubblica, si sottolinea come il ruolo chiave è giocato dal meccanismo del consenso distribuito[231], in forza del quale tutti gli utenti sono legittimati e controllare la validità delle transazioni, venendo dunque meno la necessità di un ente controllore centrale.

Alla luce del breve inquadramento di contesto qui fornito, si ritiene ora opportuno approfondire i tratti più caratteristici delle criptovalute, ponendone in luce rischi e debolezze, che espongono tali strumenti a condotte abusive e distorsive da parte di individui criminali.

3.4 I profili di rischio di riciclaggio nell'utilizzo delle criptovalute.

Tratta la conclusione di cui *supra*, ai sensi della quale le criptovalute sono inquadrabili come strumenti finanziari e avendole inserite all'interno del loro naturale sistema di funzionamento di *blockchain permissionless*, si può ora procedere nell'analisi dei risvolti che le monete virtuali producono nell'ordinamento penale.

[231] Esistono diverse categorie di consenso distribuito, i principali sono: *Proof-of-Work* e *Proof-of-Stake*. Per ulteriori approfondimenti si veda G. CASSANO, F. DI CIOMMO, M. RUBINO DE RITIS, *op. ult. cit.,* 2021

Molteplici sono le riflessioni e le discussioni aperte in tema di criptovalute e, per la maggior parte, di una tra quelle più note, i Bitcoin: se da un lato stanno rivoluzionando l'ordinamento economico, dall'altro si prestano, però, ad essere estremamente accattivanti ed attrattivi per il mondo criminale, pronto a sfruttarli per movimentare, trasferire, nascondere e reinserire nel mondo legale i proventi di attività illecite.

Ai fini di vagliare la forza criminogena delle criptovalute, con preciso riferimento al Bitcoin, conviene accennare brevemente alla sua natura e struttura, riconducibile al modello di *blockchain permissionless*, a cui si accennava *supra*. Il Bitcoin rientra nella categoria delle monete virtuali bidirezionali[232]: trattasi, per esteso, di una moneta virtuale integralmente convertibile[233], acquistabile con valute reali sulla base di tassi di cambio ufficiali ed utilizzabili per acquistare beni o servizi virtuali o reali.

Il Bitcoin (BTC) è stata la prima criptovaluta rilasciata nel 2008, basata su un sistema di tenuta dei conti decentralizzato: per la validazione delle transazioni, quindi, non si richiede l'intervento di un ente centrale o istituto di credito, ma si fa forza sul sistema *peer-to-peer*, il quale – come sopra accennato – si serve della crittografia per la validazione delle transazioni, rimpiazzando l'elemento fiduciario tradizionalmente indirizzato verso gli enti centralizzati[234].

---

[232] In base al loro rapporto con l'economia reale e quindi con le monete aventi corso legale, si segnalano altre due categorie di criptovalute: (i) moneta virtuale chiusa; (ii) moneta virtuale unidirezionale. La prima, altrimenti detta "pura", non è convertibile in denaro reale: è acquistabile unicamente tramite operazioni online e utilizzabile per compiere acquisti di beni digitali o di servizi virtuali. La seconda, invece, può essere acquistata anche con denaro reale ad un tasso di cambio fissato e può essere utilizzata per acquistare beni o servizi sia virtuali che reali, pur non potendo essere riconvertita in moneta reale. In argomento, si veda F. DI VIZIO, *op. ult. cit.,* p. 34 e ss.; R. BOCCHINI, *op. ult. cit*.

[233] Come spiegato anche da CONSOB in https://www.consob.it/web/investor-education/criptovalute: "Il bitcoin, ad esempio, è una moneta virtuale bidirezionale in quanto può essere facilmente convertita con le principali valute ufficiali e viceversa."

[234] S. NAKAMOTO, *Bitcoin*: *A peer-to-peer electronic cash system*, 2008. Infatti, come dichiarato dell'"ideatore" del Bitcoin, conosciuto con lo pseudonimo Satoshi Nakamoto, nel 2008, si tratta di un metodo di pagamento elettronico basato su una prova crittografica invece

Se da un lato, dunque, l'intero sistema *blockchain* nasce perseguendo obiettivi di maggiore trasparenza, agilità operativa e affidabilità ricorrendo *in primis* all'utilizzo di metodi crittografici e algoritmi matematici, che si pongono in sostituzione della tradizionale fiducia[235] riposta in intermediari fisici, non si possono tuttavia trascurare i rischi e le implicazioni di natura criminosa che possono scaturire da un utilizzo abusivo e distorto dell'intero sistema, in particolare con riguardo all'attività di riciclaggio.

In primo luogo, nel tentativo di fugare qualsiasi dubbio, conviene premettere che le valute virtuali non devono essere confuse con la moneta elettronica[236] utilizzata con i normali strumenti di pagamento elettronici, quali i bonifici bancari, le carte prepagate o di credito o debito.

La circolazione della moneta elettronica comporta pur sempre l'esercizio di una sfaccettata attività di controllo da parte di una Banca, dedicata a verificare che i fondi siano concretamente disponibili nel conto bancario di chi opera, che sia compiuto l'ordine di pagamento e che vi sia un rispettivo addebito – in capo all'acquirente – e accredito – in capo al venditore. Trattasi, dunque, di una tenuta dei conti "centralizzata"[237].

Tale caratteristica tipica delle monete elettroniche, infatti, confligge nettamente con il tratto tipico dei Bitcoin – e di tutte le altre criptovalute convertibili – che invece si configura per la sua natura "decentralizzata".

---

che sulla fiducia – tradizionalmente riposta in istituti quali banche e autorità regolatrici – che permette a due parti di negoziare direttamente tra loro senza la necessità di un intermediario

[235] Come affermato da E. GIRINO, *op. ult. cit*., p. 748 "*sulla fiducia, ma riposta in un'autorità centrale, si basa lo scambio della valuta tradizionale altrimenti detta fiat currency*." Sempre in tema di fiducia, si veda anche quanto statuito in Banca Centrale Europea, *Virtual currencies schemes*, 2012, p. 9: "*Trust is therefore a crucial element of any fiat money system*".

[236] Giunge utile ed intuitiva la definizione di moneta elettronica come "*una disponibilità di potere d'acquisto registrata su un conto corrente acceso presso una Banca*" data da G. P. ACCINNI, *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017*), in Archivio Penale, 2018, n. 1, p. 2,

[237] G. P. ACCINNI, *op. ult. cit*., p. 2. L'Autore spiega come risulti "indispensabile l'intervento di un ente terzo (una Banca) che, grazie ai dati custoditi nei propri *server* centralizzati e protetti, verifichi e confermi l'identità dell'ordinante, la disponibilità dei fondi, la correttezza dei codici di sicurezza; esegua l'operazione e la trascriva sui propri libri contabili".

Infatti, come sopra richiamato, la circolazione delle valute virtuali, non facendo perno su un solo organo terzo e centrale (o, altrimenti, su un solo gestore), in aderenza a quello che è il sistema DLT, la gestione delle operazioni è distribuita tra tutti gli utenti del *network*[238] e ciascuno vi può accedere dal proprio dispositivo.[239]

In altre parole, dunque, soggetti privati e non dipendenti tra loro operano e compiono transazioni, agendo in una situazione di parità[240]: in forza di questo meccanismo, viene a crearsi una sorta di "memoria condivisa"[241] tra utenti.

Per mezzo di questa decentralizzazione[242], essendo permessa l'operatività direttamente tra operatori privati, il sistema *blockchain* rimpiazza la fiducia degli intermediari, come le banche, che svolgono un ruolo centrale nelle politiche antiriciclaggio. Sul punto, si noti come le attività di contrasto ad operazioni illecite, prendano generalmente avvio in forza di segnalazioni, denunce e controlli di operazioni sospette da parte di Autorità centrali, che in questo caso, a causa della natura

[238] Cfr. anche G.W. PETERS, "*Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective*", 2015 ove si chiarisce come le criptovalute, per loro natura, permettono la realizzazione di transazioni "*peer to peer*" ed eliminano la necessità di una banca o di un intermediario per facilitare la transazione finanziaria.

[239] Si segnala che in dottrina si è registrato un orientamento secondo il quale tale "decentralizzazione" e il conseguente venir meno di un soggetto terzo intermediario sia, in verità, solo apparente. Secondo tale corrente, infatti, ad indossare le vesti di intermediario rimane l'algoritmo del sistema che è pur sempre controllato da operatori umani. In argomento, cfr. E. GIRINO, *op. ult. cit.*, p. 740

[240] Tale metodo operativo è stato ricondotto da alcuni studiosi ad una ideologia di stampo anarchico, che fa capo alla tesi, promossa dalla scuola economica austriaca, della "denazionalizzazione della moneta", secondo la quale l'emissione di valute non subordinate al controllo di un'autorità nazionale o sovranazionale centrale perseguirebbe il tormentato obiettivo di rifuggire "l'oligopolio dell'intermediazione bancaria e finanziaria autorizzata". In argomento, si veda E. GIRINO, *op. ult. cit*., p. 740.

[241] F. CONSULICH, *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*, in Diritto penale e processo 2/2022, p. 153

[242] M. CAMPBELL-VERDUYN, *Bitcoin and beyond: cryptocurrencies, blockchains and global governance*, 2018, p. 74. In argomento ricorre utile la definizione di "dematerializzazione" fornita da F. CONSULICH, *op. ult. cit.,* p. 153 come "collocazione delle transazioni in un ecosistema in cui i servizi (dai prestiti, ai pagamenti fino agli investimenti) vengono forniti senza la supervisione e regolazione di un'autorità pubblica".

decentralizzata del sistema, non potrebbero invece aver luogo[243]. Sempre sul punto, si pensi anche allo svolgimento di controlli ed ispezioni, sempre nei confronti di intermediari e operatori finanziari, destinatari della normativa antiriciclaggio.

Ulteriore rilevante caratteristica delle valute virtuali è la loro impossibilità di essere possedute fisicamente dall'utente e dunque di essere difficilmente riconducibili ad un soggetto determinato. Infatti, vengono movimentate solo grazie al c.d. *e-wallet*, un servizio di portafoglio elettronico, il quale mette a disposizione un *wallet* che può essere installato nel proprio *computer* o *smartphone* e che è sempre accessibile via internet al fine di movimentare le valute virtuali.

Tali portafogli elettronici di regola sono *software*, realizzati e forniti dai c.d. *wallet providers*, società che tramite appositi programmi permettono agli utenti di detenere e trasferire Bitcoin o altre specie di criptovalute. Inoltre, le criptovalute possono essere anche acquistate con moneta tradizionale su una piattaforma di scambio o possono essere ricevute *online* da qualcuno che le detiene, per poi essere trattenute in un "portafoglio elettronico".

Problematica è, peraltro, sia la condizione dei detentori dei portafogli elettronici sia di tutti coloro che operano nelle transazioni in condizione di anonimato. Le monete virtuali, infatti, sono per la maggior parte vendute privatamente, senza la supervisione di un'autorità di vigilanza, lasciando dunque ampi margini di libertà per chi volesse compiere attività di ripulitura del denaro proveniente da reato.[244]

Tale difficoltà nell'identificare i soggetti che si nascondono dietro alle operazioni in criptovalute induce a non trascurare la loro più ambigua

[243] N. PASSARELLI, *op.ult. cit.*, p. 12
[244] In argomento, M. DA ROLD, *op. ult. cit.*, p. 11

caratteristica della pseudonimità[245] delle transazioni garantita agli utenti. Sembra invero condivisibile abbracciare la tesi della corrente dottrinale che sostiene che sarebbe forse più appropriato parlare di "pseudonimato"[246] e non di anonimato.

Infatti, con questa espressione si fa riferimento allo *status* che si crea per chi opera in criptovalute in forza della commistione di due fattori opposti: da un lato, la libera accessibilità al registro contabile digitale presente sulla *blockchain,* che permette di tracciare gli *accounts* di coloro che hanno compiuto l'operazione; dall'altro, l'incertezza permanente sulla vera identità fisica di coloro che hanno compiuto le operazioni[247].

Si segnala, che per alcuni rimane più appropriato parlare di anonimità[248], in quanto l'indirizzo di Bitcoin composto da una sequenza di lettere e numeri, una volta individuato dalle Autorità in ogni caso non consente di svolgere indagini ulteriori identificando l'identità fisica del titolare dell'*account* individuato.[249]

Ad ogni modo, è senz'altro indubbio che l'anonimato venga in gioco quando sia possibile eseguire un finanziamento del sistema criptovalutario in forma anonima (c.d. *funding* anonimo)[250]. Ciò accade quando alcuni detentori di monete virtuali le mettono in vendita in forma privata, sfruttando la potenzialità di "innocui" annunci *online*, non necessitando di un soggetto che funga da intermediario, come

---

[245] Come segnalato dal direttore di Deloitte, Fred Curry, "regulators can't monitor transactions if they don't know who the parties are".

[246] G.J. SICIGNANO, *op. ult. cit*., p. 11; G.P. ACCINNI, *op. ult. cit*., pp. 5-6

[247] In argomento, cfr. F. POMES, *op. ult. cit.*, p. 164

[248] S. CAPACCIOLI, *Criptovalute e bitcoin: un'analisi giuridica*, 2015, p. 254, in punto di sistema peer-to-peer parla di una potenzialità per qualsiasi utente di "*trasferire soldi a velocità quasi istantanea a bassissimo o senza alcun costo, con basse barriere all'ingresso nell'anonimato virtuale in assenza di una tracciabilità*".

[249] Come posto in luce in L. STURZO, *op. ult. cit.*, p. 31: "(…) *come se non bastasse, un unico soggetto persona fisica può addirittura divenire contestualmente proprietario di più accounts, operando così più transazioni illecite, ciascuna riconducibile ad un account diverso*".

[250] G.P. ACCINNI, *Profili di rilevanza penale delle criptovalut*e, in Archivio penale 2018, p. 13.

l'exchanger, oppure di siti che siano raggiungibili e controllabili dalle Autorità di Vigilanza[251].

Rimane d'altronde inconfutabile, che seppur sia di certo più preciso parlare di "pseudonimato", il livello di anonimato garantito è di gran lunga superiore rispetto a quello previsto per le transazioni bancarie. Infatti, non si richiede che i detentori dei portafogli elettronici siano fisicamente identificati e inoltre sono accessibili una molteplicità di strumenti che massimizzano la *privacy* degli utenti[252]. La certezza dell'anonimato permette dunque la realizzazione di trasferimenti ingenti di capitale sia a livello interno che sovranazionale senza essere sottoposti ad alcuna regolamentazione.

In prima battuta, può dunque considerarsi, come la forza attrattiva verso i soggetti criminali sia data soprattutto dall'anonimato e pseudonimato e dall'assenza di un soggetto controllore *super partes*[253]: attraverso questo sistema, in linea potenziale qualunque utente è in grado di trasferire denaro in tempistiche immediate e a basso costo – o addirittura a costo nullo – in una condizione di anonimato virtuale. In questo modo le criptovalute potrebbero incentivare i riciclatori di denaro a spostare fondi illeciti in maniera molto più rapida.[254]

Proseguendo il vaglio dei rischi connessi all'utilizzo delle criptovalute, così come anche ribadito dalla Banca d'Italia[255], non trascurabile è poi la volatilità[256] a cui è soggetto il processo di formazione dei valori delle

[251] Può essere ad esempio il caso dei siti: www.bitboat.net e www.localbitcoins.com.

[252] Basti pensare anche allo svolgimento di operazioni tramite i *privacy coins*, come Monero, o il ricorso a programmi nel *deep web* che consentono di oscurare gli indirizzi IP tramite cui si naviga.

[253] È proprio l'idea di costituire un'economia di mercato libero *tout court,* regolato solamente dagli utenti del sistema a rendere l'universo dei Bitcoin fortemente accattivante.

[254] S. CAPACCIOLI, *op. ult. cit.*, p. 254

[255] Documento 30 gennaio 2015. *Ex multis*, cfr. A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, 2019, p. 882-883.

[256] E. GIRINO, *op. ult. cit.,* p. 55 secondo il quale "la volatilità, che di norma non è un fattore della più o meno accentuata rischiosità di un investimento, diviene invece elemento attributivo di natura e funzionalità finanziaria alla criptovaluta. E lo diviene perché siffatta

criptovalute e l'assenza di metodi di stabilizzazione, i quali sono le principali cause della creazione di altalenanti bolle speculative. Da ultimo, non può non menzionarsi la passibilità ad attacchi informatici, nel tentativo di rubare i dati di utenti che genuinamente cercano di operare nel sistema, senza alcuna finalità illecita.

Dunque, condividendo pacificamente quanto sostenuto da attenta dottrina[257], secondo cui configurandosi il reato di riciclaggio come reato di pericolo concreto, non si richiede il concreto compimento dell'azione riciclatoria per la configurazione dell'attività delittuosa, bastando puramente l'idoneità della condotta ad ostacolare la provenienza criminosa del bene, è allora tanto più probabile che il sistema Bitcoin divenga un ecosistema criminogeno volto a ripulire proventi illeciti, quanto più la sua struttura e le sue peculiarità impediscano *tout court* o ostacolino l'accertamento della provenienza delle criptovalute.

In nota di chiusura si riporta inoltre una statistica aggiornata che testimonia la concretezza dei pericoli sopra esposti: in un recente *report* pubblicato dalla compagnia Chainalysis[258], è emerso che nel 2021 il riciclaggio di denaro tramite criptovalute è aumentato di circa il 30% rispetto al 2020.

Può dunque concludersi, in considerazione di quanto appena messo in luce in tema di valute virtuali e, nella specie, dei Bitcoin, che è in continua emersione un allarmante pericolo che il mercato digitale si trasformi in un "*cyber-heaven*"[259] per ogni individuo o persona giuridica che voglia realizzare attività di riciclaggio.

---

volatilità è particolarmente pronunciata e quest'ultima tale è proprio in ragione della natura alegale della moneta virtuale e della struttura alternativa che la governa."

[257] Cfr. L. STURZO, *op. ult. cit*, p. 22; In argomento, si veda anche E. MEZZETTI, *op. ult. cit. e*, in *Trattato di diritto penale, Parte speciale*, diretto da GROSSO-PADOVANI-PAGLIARO, 2013, p. 658; A.R. CASTALDO, M. NADDEO, *op. ult. cit.*, 2010, p. 11

[258] Chainalysis, *Crypto Crime Report,* 2022

[259] L. D'AGOSTINO, *op. ult. cit*., p. 5

Riprendendo una constatazione condivisa da autorevole dottrina[260], infatti, il Bitcoin racchiude gli aspetti più vantaggiosi della moneta elettronica e del contante. Infatti, "come una banconota, è anonimo: non richiede che siano rese note le identità delle controparti né la causale di pagamento; ma, essendo digitale, ossia un puro numero, divisibile e moltiplicabile a piacere, consente trasferimenti per qualunque importo, dai micropagamenti di pochi centesimi al regolamento di traffici commerciali internazionali"[261]. Alla luce di questa sua natura "ibrida" necessita con urgenza la subordinazione a norme di funzionamento puntuali, che non lascino spazio a lacune di disciplina, aggirabili per interessi economici più spregevoli.

3.5 Nuovi soggetti partecipi del "cripto-riciclaggio".

In riferimento a quanto sopra descritto in tema di riciclaggio e *cyberlaundering*, può qui richiamarsi la suddivisione del processo di ripulitura del denaro in tre fasi tipiche: *(cyber)placement*, *(cyber)layering*, *(cyber)integration*. Tuttavia, ritenendo sufficiente la spiegazione fornita *supra*[262], sembra qui opportuno focalizzarsi sulle caratteristiche di ciascuna di queste tre fasi in relazione all'utilizzo delle criptovalute, che comporta il coinvolgimento di figure "nuove", non presenti nello svolgimento del riciclaggio in forma tradizionale.

Non sfugge, infatti, che una molteplicità di soggetti con funzioni diverse intervenga nel procedimento trifasico in oggetto, vedendosi di regola assegnata una funzione tipica e non sostituibile.

---

[260] G. P. ACCINNI, *op. ult. cit.*, p. 2

[261] L. AMATO, M. FANTACCI, *Per un pugno di Bitcoin*, 2016, p. 3. Sul punto si veda anche il contributo di M. CROCE, *op. ult. cit*., p. 129. L'Autrice scrive in proposito che la valuta virtuale "*come la moneta fisica, essa è accessibile a chiunque, ha carattere anonimo ed è agevolmente trasferibile; come la moneta elettronica, consente di effettuare agevolmente pagamenti a distanza e garantisce transazioni rapide e a basso costo*".

[262] V. *supra*, cap. II, par. 2.5

Prendendo avvio dalla fase di *cyberplacement*, qualora si tratti di riciclaggio digitale strumentale, assumono un ruolo essenziale gli *exchangers* e i *wallet providers.* Con il termine *exchanger*[263], si fa riferimento alla persona fisica o giuridica che, dietro pagamento di una commissione, mette a disposizione degli utenti un servizio di cambio di moneta con corso legale – o, in alternativa, di metalli preziosi[264] – con criptomonete.[265]

Accanto all'*exchanger*, gioca un ruolo preminente in questa prima fase anche il *wallet provider*[266], che detiene la gestione del denaro virtuale, in una sorta di portafoglio elettronico. Entrambi, sia l'*exchanger* che il *wallet provider* devono attenersi a quanto disposto nel d.lgs. 90/2017, il quale ha recepito nell'ordinamento interno la Direttiva UE 2015/849 ai sensi della quale tali soggetti devono rispettare le norme antiriciclaggio, rispondendo ad obblighi di segnalazione e identificazione della propria clientela.

La seconda fase, c.d. *cyber-layering,* si sostanzia nella movimentazione di valuta virtuale tra più indirizzi appartenenti allo stesso soggetto o a prestanome virtuali, i c.d. *money mules*.[267] Il *money mule* è definito come "una

---

[263] Si riporta di seguito la definizione fornita dalla BCE, in *Virtual currency schemes*. *A further analysis,* 2015, p. 8: "*Exchangers offer trading services to users by quoting the exchange rates by which the exchange will buy/sell virtual currency against the main currencies (US dollar, renmibi, yen, euro) or against other virtual currencies. These actors, most of them non-financial companies, can be either issuer-affiliated or a third party. They generally accept a wide range of payment options including cash, credit transfers and payments with other virtual currencies. Moreover, some exchanges also provide statistics (e.g. volumes traded and volatility), act as wallet providers and offer (immediate) conversion services for merchants who accepts VCS as an alternative payment method".*

[264] In argomento, si veda A. PARBONETTI, *Caratteristiche e modalità di gestione delle aziende criminali*, in R. BORSARI (a cura di), *Itinerari di diritto penale dell'economia*, 2017, pp. 469 e ss.

[265] Cfr. sul punto ACCINNI, *op. ult. cit.,* p. 4 e M. DA ROLD, *op. ult. cit.*, p. 13

[266] Si riporta di seguito la definizione fornita dalla BCE, in *Virtual currency schemes*. *A further analysis,* 2015, p. 8: "*Wallet providers offer a digital wallet to users for storing their virtual currency cryptographic keys and transaction authentication codes, initiating transactions and providing an overview of their transaction history. There are basically two types of wallet, which differs as regards their immediate usability versus their safety from cyber crime: online wallets (hot storage) and offline wallets (cold storage). From a functional perspective, these services for desktop PCs, mobile devices and as cloud-based applications. Nevertheless, users can also set up and maintain a wallet themselves without making use of a wallet provider".*

[267] M. CROCE, *op. ult. cit*., p. 139

persona che riceve denaro da una terza persona sul suo conto bancario e poi lo trasferisce ad un'altra persona sotto forma di contanti o di altro tipo dopo aver ottenuto la sua commissione"[268].

In altre parole, il *money mule* permette che il suo conto corrente sia utilizzato dai criminali per ripulire denaro di provenienza illecita[269]. I *money mules* vengono di norma reclutati ricorrendo a tecniche diverse, come ad esempio incontri di persona, annunci *online*, *social networks*. Per quanto riguarda gli annunci *online* di lavoro, questi possono configurarsi in due modalità: la prima comporta la diffusione di richieste di figure come "*financial manager*", "*account manager*" o "*client manager*"; la seconda, invece, implica che il criminale contatti direttamente un individuo offrendo lavoro in privato.[270] Gli individui a cui ci si rivolge più di frequente sono soggetti appena arrivati in un determinato paese, studenti, disoccupati e persone in condizioni economiche precarie, così maggiormente suscettibili di acconsentire alla commissione del crimine[271].

Calandosi ancor più nello specifico, i *money mules* sono soliti trasferire il denaro ricevuto nel proprio conto corrente in paesi lontani dal proprio, in genere oltreoceano, dietro pagamento di una commissione per il servizio prestato.

Volgendo ora lo sguardo ad un'ulteriore categoria di soggetti che partecipano attivamente al procedimento di riciclaggio, *i.e.* i *mixers*, deve richiamarsi quanto analizzato in tema di transazioni criptovalutarie nel sistema *blockchain*. Tali transazioni, infatti, vengono registrate nel *database* e associate all'indirizzo di portafoglio degli utenti, restando così tracciabili. Dunque, proprio per compromettere questa inevitabile tracciabilità, nella fase

[268] EUROPOL, *Public Awareness and Prevention Guides*, 2019.

[269] M. S. RAZA, *Role of money mules in money laundering and financial crimes. A discussion through case studies*, in Journal of financial crime, 2020, p. 912.

[270] F. STALENBERG, *Find out How You Can Start Making a 6487 a Month at Home!* ,2002

[271] M. S. RAZA, *op. ult. cit*., p. 919.

di *layering*, assumono un ruolo importante i c.d. *mixers*[272] i quali hanno il compito di rendere più complessa la ricostruzione del c.d. *digital trial*, ossia la successione dei trasferimenti di valuta virtuale.

L'attività di *mixing* costituisce uno dei tratti più tipici di questa seconda fase e, per completezza, merita di essere brevemente descritta in questa sede. Tale servizio, altrimenti detto anche *mixnet*, permette all'utente di depositare un determinato ammontare in criptovaluta su uno o più conti di ingresso per poi ritirare il denaro (virtuale) su conti di uscita[273] appositamente creati o già esistenti. In altre parole, l'attività del *mixer* si sostanzia in una vera e propria frammentazione del denaro di provenienza illecita, che verrà poi destinato ad una pluralità di conti oppure il denaro di più utenti viene destinato ad un unico conto. L'obiettivo principale per il *mixer* deve essere quello di far sì che la somma di denaro depositata *ab initio* sia diversa da quella ritirata alla fine del procedimento e, per questo, il *mixer* trattiene di regola una percentuale in qualità di corrispettivo per il servizio prestato.[274]

I *mixers* si servono, in genere, di due artifici per perseguire la loro finalità dissimulatoria. Il primo *escamotage* consiste nell'invio consequenziale di moneta proveniente da diversi portafogli, dai quali poi, in un secondo momento, prendono avvio altre transazioni su altri conti, conosciuti come "conti di rimbalzo" (conti *bounce*). La seconda tecnica di frammentazione del *digital trial* fa sì che i fondi di una pluralità di utenti, che si sono rivolti al

[272] Tra i servizi più noti di *mixing*, si ricordino: *Bitlaunder*, *Bitcoin Laundry* e *Easycoin*. In argomento, cfr. L. D'AGOSTINO, *op. ult. cit.,* p. 11, secondo il quale "il mixing è avvolto da un'aura tale di sospetto sull'impiego a fini criminosi (in particolare al fine di ostacolare l'identificazione della provenienza dei flussi di valuta virtuale), da poterla considerare in sé intrinsecamente illecita". Sempre in tema di *mixing*, si segnala l'utilizzo della valuta *Monero*, la quale garantisce un alto grado di anonimato, rendendo le operazioni non tracciabili. Essa, infatti, permette di oscurare i nomi dei soggetti che operano *online* e di nascondere anche l'ammontare delle transazioni compiute. Si segnala anche l'esistenza di altre criptovalute della stessa natura di Monero (*privacy coins*): Dash e Zcash.

[273] Cfr. M. CROCE, *op. ult. cit*., p. 139. Di norma, nei servizi di *mixing*, vengono utilizzati ben quattro tipologie distinte di conti: di ingresso, *bounce*, *pool*, di uscita. In argomento, si veda O. CALZONE, *Servizi di mixing e Monero*, in Gnosis, 2017, p. 5

[274] Cfr. M. CROCE, op. ult. cit., p. 139.

servizio di *mixing*, confluiscano in un unico conto (conto *pool*) e da qui poi vengono diramati a molteplici indirizzi.[275]

La terza fase del *cyberlaundering* permane, invece, perlomeno immutata: la c.d. *cyberintegration* sembra essere qui assimilabile a quanto descritto in punto di riciclaggio "tradizionale".

Infatti, la maggior parte delle valute virtuali sono accettate da un numero di operatori economici sempre più esteso, pertanto il reinserimento nel circuito economico legale pare essere di facile riuscita, tramite l'acquisto di beni o servizi, pur senza conversione in moneta avente corso legale.

3.6 Le più note vicende di "cripto-riciclaggio": i casi *Liberty Reserve* e *Silk Road.*

Non può trascurarsi come tali osservazioni non si limitino ad essere mere congetture teoriche, ma, al contrario, abbiano avuto risonanza concreta negli ultimi anni, interessando le più importanti Autorità e sollecitando notevolmente l'opinione pubblica. Si darà breve conto in questa sede di due colossali vicende di riciclaggio, realizzato tramite l'utilizzo illecito di criptovalute. La prima è conosciuta come il caso "*Liberty Reserve*", ad oggi noto come "il maggior caso di riciclaggio *online* mai verificatosi"[276]. Nel 2013, il US Department of Justice ha condotto una maxioperazione, accusando il fondatore, Arthur Budovsky, e i dipendenti della società Liberty Reserve, un servizio di valuta digitale[277], con sede in Costa Rica, per aver condotto un *business* da 6 miliardi di dollari di provenienza illecita a fini di ripulitura[278]. Secondo quanto emerso dalle indagini, questa società era stata

[275] L. D'AGOSTINO, *op. ult. cit*.

[276] G. P. ACCINNI, *op. ult. cit*., p 14 e ss. L'Autore mette in luce la portata transnazionale di questa indagine, che ha coinvolto ben 18 giurisdizioni.

[277] Washington: Federal Information & News Dispatch, LLC, Notice of Finding That Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern, in The Federal Register, 2013-06-06, Vol.78, p.34169: "*Liberty Reserve is a Web-based money transfer system, or ''virtual currency*"".

[278] Cfr. Aspen Publishers, *Liberty reserve founder pleads guilty to laundering more than $250m*, in The computer & Internet lawyer, 2016-05-01, Vol.33 (5), p.24: "*Budovsky specifi*

fondata con il preciso intento di aiutare le associazioni criminali e contribuire al riciclo di proventi illeciti, derivanti nello specifico da furti di identità, clonazioni di carte di credito, reati informatici. Le transazioni compiute avvenivano in forma anonima e non rintracciabile; inoltre, dietro pagamento di una tassa aggiuntiva, poteva essere garantita un'anonimità ancora più forte[279]. Secondo i dati emersi, la società avrebbe gestito 55 milioni di transazioni illecite[280].

La *Liberty Reserve*, al fine di conseguire il proprio oggetto sociale, emetteva una propria valuta, il *Liberty Dollar*, che per essere utilizzato richiedeva che ogni utente aprisse il proprio *e-wallet* tramite il sito della società. Naturalmente, la società non effettuava controlli di alcun tipo sulla bontà dei dati inseriti dagli utenti, che spesso erano manifestamente falsi. È così che, una volta aperto il proprio conto, ogni utente poteva liberamente compiere ogni tipo di operazione, servendosi di *online markets* che accettassero pagamenti in *Liberty Dollar*.

Questa vicenda di "cripto-riciclaggio" si è realizzata seguendo un modello operativo per cui criminali "comuni" convertivano il denaro di provenienza illecita in criptovalute, operando transazioni e movimentazioni di denaro per offuscare l'origine delittuosa dei proventi. A questo *modus operandi,* tuttavia, non è riconducibile anche la seconda vicenda di cui si darà conto di seguito.

Trattasi, in particolare, della nota vicenda "*Silk Road*", altra maxioperazione americana che ha impegnato un importante numero di

cally designed Liberty Reserve, which billed itself as the Internet's "largest payment processor and money transfer system," to help users conduct anonymous and untraceable illegal transactions and launder the proceeds of their crimes".

[279] Washington: Federal Information & News Dispatch, LLC, Notice of Finding That Liberty Reserve S.A. Is a Financial Institution of Primary Money Laundering Concern, in The Federal Register, 2013-06-06, Vol.78, p. 34170.

[280] FATF, *Virtual currencies: key definition and potential aml/cft risks*, 2014, pp. 10.

Autorità[281]. Tale caso è riconducibile ad una matrice operativa secondo la quale un criminale informatico vendeva merce di natura illecita verso pagamento in criptovaluta, che veniva successivamente convertita in moneta avente corso legale utilizzata per operare sul mercato al solo fine di nascondere l'origine illecita del denaro[282].

Guardando più da vicino la vicenda, in via di sintesi, *Silk Road* consisteva in una piattaforma *e-commerce* anonima che operava nel *dark web* tramite il TOR *network*[283] e che accettava solamente Bitcoin per i pagamenti relativi all'acquisto *online* di stupefacenti, dati personali rubati, armi e altri beni illeciti.

Questo sito veniva utilizzato, quindi, come *black market* per la vendita e distribuzione di prodotti illeciti, con un ricavo complessivo registrato di circa 1.2 miliardi di dollari[284]. Previo collegamento del portafoglio virtuale dell'utente con un portafoglio gestito dalla piattaforma *Silk Road*, al momento del compimento dell'acquisto da parte dell'utente i Bitcoin da esso detenuti venivano trasferiti nel portafoglio presente nel sito. I Bitcoin rimanevano depositati in quello stesso portafoglio, fino ad avvenuta conferma del perfezionamento della vendita. Quando questa si fosse perfezionata, i Bitcoin depositati nel portafoglio virtuale gestito da *Silk Road* venivano trasferiti al venditore. Infine, non può trascurarsi come *Silk Road* si curasse di mettere a disposizione dei propri utenti degli appositi servizi di *mixing*, in modo tale da

[281] Le indagini su *Silk Road* hanno comportato il coinvolgimento, come per il caso *Liberty Reserve,* di molteplici autorità americane, tra cui i FBI's New York Special Opeations and Cyber Division, DEA's New York Organized Crime Drug Enforcement Strike Force, NY Department of Taxation con il supporto del French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

[282] G.P. ACCINI, *op. ult. cit.*, p. 15; Royal United Services Institute for Defence and Security Study, *Occasional paper, virtual currencies and financial crime: challenges and opportunities*, in www.rusi.org.pdf

[283] TOR è l'abbreviazione di *The Onion Router,* definibile come un *privacy network* di tipo *open-source* che consente di navigare in condizione di anonimato. Definizione presa dal sito www.investopedia.it

[284] Cfr. FATF, *Report Virtual currencies: Key Definition and Potential AML/CFT Risks*, 2014, pp. 11.

rendere non tracciabili le operazioni compiute e, di conseguenza, rendendo impossibile l'identificazione dei soggetti acquirenti e venditori.

Considerato il riscontro pratico qui riassunto, che si sottolinea non essere isolato, data la molteplicità di vicende che ad oggi impegnano le maggiori Autorità e attraggono l'interesse della pubblica opinione, è possibile escludere pacificamente la mera astrattezza o la rilevanza puramente teorica delle riflessioni qui riportate. I rischi che si profilano dietro l'utilizzo delle criptovalute a fini di riciclaggio sono concreti e minacciosi per l'ordine economico, data la possibilità di movimentare somme di denaro assai significative.

Alla luce della evidente pericolosità del fenomeno in discorso, le maggiori Autorità, da una decina d'anni ad oggi, si sono espresse con fermezza riguardo alla potenzialità offensiva nell'utilizzo delle criptovalute, al fine non solo di salvaguardare i cittadini da operazioni azzardate, ma *in primis* di sollecitare il Legislatore a provvedere quanto prima. Di tali autorevoli voci si darà riscontro nel paragrafo immediatamente successivo.

3.7 Le determinazioni delle Autorità sui rischi di riciclaggio connessi alle criptovalute: il Financial Action Task Force (FATF) nel 2014.

A seguito delle considerazioni appena svolte sui rischi annessi all'utilizzo di criptovalute per compiere attività di riciclaggio, si ritiene opportuno suffragarle ulteriormente dando conto dei molteplici pareri forniti sul punto dalle principali Autorità di Vigilanza.

Tra queste, merita di essere menzionato in prima battuta il Gruppo di Azione Finanziaria (GAFI/FATF). Nel 2014, il FATF, dopo aver fornito una prima definizione di criptovaluta, da intendersi come "*rappresentazione digitale di valore che può essere ceduta/scambiata*

digitalmente e funzionare come mezzo di scambio, unità di conto e riserva di valore, che tuttavia non ha corso legale in alcuna giurisdizione; non è emessa o garantita da alcuna giurisdizione, riuscendo a soddisfare le predette condizioni solo attraverso l'accordo che intercorre tra la comunità degli utilizzatori della valuta virtuale" [285], ha messo in luce nel proprio *report* alcuni rischi eclatanti intrinseci all'utilizzo delle criptovalute.

La prima criticità evidenziata dal GAFI concerne l'anonimato[286] legato al funzionamento delle criptovalute, rischio che invece non sussisterebbe – o quantomeno sussisterebbe in via certamente inferiore – rispetto ai mezzi tradizionali di pagamento non basati sui contanti, come i bonifici bancari e le carte di pagamento. Infatti, il rapporto sussistente tra i soggetti operatori si insatura integralmente *online* e, dunque, in assenza del cliente (c.d. *non-face-to-face customer relationship*), rendendo in tal modo agevole la realizzazione di finanziamenti in forma anonima o finanziamenti da parte di terzi che, operando tramite gli *exchangers*, non permettono di risalire alla fonte del finanziamento stesso. Su questo punto, torna utile ricordare che un *e-wallet* di Bitcoin non è riconducibile immediatamente ad una persona fisica o giuridica. Ancora, il sistema non è provvisto di un *software* centrale volto a identificare e monitorare transazioni potenzialmente sospette.

Altro fattore di rischio per il GAFI è dato dalla decentralizzazione tipica del sistema *blockchain*. Infatti, l'assenza di un ente controllore o di un apposito *software* antiriciclaggio volto ad indentificare e verificare l'identità di chi agisce *online* o capace di costruire uno "storico" delle transazioni associate a soggetti determinati, ostacola e talvolta impedisce ogni tipo di indagine ricostruttiva.

[285] FATF, *Report,Virtual Currencies, Key Definitions and Potential AML/CFT Risks*, June 2014

[286] In FATF, *Report,Virtual Currencies, Key Definitions and Potential AML/CFT Risks*, June 2014, si parla di "greater anonymity than traditional noncash payment methods".

Ancora, secondo il FATF, altro incentivo offerto alla platea di criminali è dato dalla possibilità di effettuare pagamenti su scala transnazionale, superando il limite delle giurisdizioni di ogni Stato. Sempre sul punto, deve inoltre tenersi conto che le criptovalute sono spesso basate su una pluralità di strutture informatiche localizzate anche in Paesi esteri: questa frammentazione comporta naturalmente forti incertezze di tutela, risultando assai ostico avere accesso alle informazioni sulle transazioni, in particolare alla luce del fatto che il tracciamento delle transazioni potrebbe essere conservato da enti diversi – spesso in giurisdizioni diverse – ostacolando in modo consistente l'attività investigativa delle Autorità. Si assiste, in altre parole, ad uno scambio di valore che non passa ufficialmente per alcuna giurisdizione e che, al contrario, si svolge in una c.d. quarta dimensione, del tutto dematerializzata ed impercettibile.

Nel 2020, sempre la Financial Action Task Force ha pubblicato un *report* illustrativo delle manifestazioni più allarmanti di riciclaggio di denaro in tema di criptovalute[287]. Nel report, si parla di preciso di "*red flag indicators*" relativamente ad attività sospette nell'utilizzo di *assets* virtuali o di elusione della normativa antiriciclaggio.

Di norma, sarebbe proprio la presenza simultanea di una pluralità tra questi indicatori a dover allarmare le Autorità in merito al potenziale svolgimento di attività criminali. *In primis*, l'attenzione degli Organi di Vigilanza ricade sull'ammontare e sulla frequenza delle transazioni. Più precisamente, secondo il FATF sono sospette tutte quelle movimentazioni di denaro compiute in somme di modesto rilievo, in sequenza temporale assai ravvicinata (ad esempio, nell'arco di ventiquattro ore) ed indirizzate verso un conto appena acceso o, al contrario, da lungo tempo non utilizzato. Ancora, altri motivi di sospetto

[287] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, September 2020.

potrebbero, secondo il FATF, scaturire da quelle transazioni realizzate in un determinato periodo di tempo, da una pluralità di soggetti e riguardanti ingenti somme di denaro.

Da ultimo, è senz'altro di particolare interesse, dare rilievo a tutti i possibili indicatori di transazioni sospette relativi alla condizione di anonimato in cui si trovano i soggetti criminali che operano *online.* In particolare, trattasi principalmente di transazioni compiute con criptovalute ad alto tasso di anonimità[288] o con i c.d. *privacy coins*. Ancora, parimenti sospetta potrebbe risultare la pratica di ricevere fondi da o inviare fondi dove i controlli *know-your-costumer* (KYC) sono molto deboli o inesistenti. In via di nuovo esemplificativa e senza alcuna pretesa di esaustività ad attirare l'attenzione delle Autorità di controllo potrebbero, infine esservi tutte le transazioni realizzate attraverso servizi di *mixing*, rendendo palese l'intenzione di voler offuscare la provenienza illecita dei proventi.

3.8 (Segue) L'European Banking Authority (EBA).

L'European Bank Authority si è a più riprese pronunciata in tema di criptovalute percorrendo il tentativo di aumentare la consapevolezza della platea di operatori finanziari sui rischi connessi all'utilizzo delle monete virtuali[289]. Infatti, dal 2013 fino ai giorni più recenti, si sono registrati sul punto molteplici allerte da parte dell'Autorità[290].

---

[288] Si veda, ad esempio, la criptovaluta Monero. Ad oggi è conosciuto come uno tra gli "altcoins" più oscuri. Afferisce, infatti, alla categoria dei c.d. *privacy coins* e, secondo le più recenti statistiche, costituisce la moneta virtuale maggiormente utilizzata dai criminali. Cfr. Trendmicro, *Evasive threats, pervasive effects*, 2019. Reperibile al link: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat reports/roundup/evasive-threats-pervasive-effects

[289] All'EBA compete, ex art. 9 del Regolamento (UE) n. 1093 del 24 novembre 2010, "monitorare le attività finanziarie nuove ed esistenti e adottare orientamenti e raccomandazioni volti a promuovere la sicurezza e la solidità dei mercati e la convergenza delle prassi di regolamentazione". In argomento, cfr. M. MANCINI, *Valute virtuali e Bitcoin*, in *Analisi Giuridica dell'Economia*, 1/2015.

[290] Più di preciso si segnalano gli interventi del 2013, 2014, 2016, 2019

Giova menzionare in questa sede, il Report EBA del 2014[291], il quale ha inquadrato il rischio di riciclaggio sotteso all'utilizzo di criptovalute nella macrocategoria dei "*Risks to financial integrity*".[292]

In particolare, secondo l'EBA il rischio maggiore – e per questo contrassegnato a priorità alta – si configura poiché gli operatori, potendo agire in un rapporto "*peer to peer*", non sono personalmente identificati: infatti, il portafoglio di ogni utente è privo di qualsiasi informazione sull'identità reale delle persone fisiche o giuridiche che ne sono titolari.

In secondo luogo, ulteriori rischi sono dati dalla possibilità per i criminali di procedere al lavaggio di denaro sporco potendo depositare e trasferire le criptovalute da uno Stato all'altro, in modo rapido e irreversibile. In altre parole, poiché le valute virtuali non sono legate a confini territoriali e giurisdizionali ed essendo solamente sufficiente una connessione *internet* risulta assai arduo intercettare le transazioni.

Secondo l'Autorità, è dunque elevato il rischio per cui i soggetti criminali si apprestino ad utilizzare gli *account* virtuali per finanziare attività criminose o di stampo terroristico, offuscando la provenienza del capitale impiegato e dunque impedendo alle Autorità di ottenere prove delle operazioni illecite compiute.

Ulteriore e non trascurabile rischio evidenziato dall'EBA riguarda l'attività di controllo che i soggetti criminali sono poi in grado di esercitare sugli operatori di mercato. Tale rischio emerge dalla condizione per cui gli operatori di mercato sono spesso guidati da individui non qualificati.

Alla luce dei rischi sopra evidenziati, è opportuno precisare come il parere dell'European Banking Authority in discorso sia stato emanato a scopi armonizzativi e di coordinamento tra le varie normative

[291] Immediatamente successivo al Report GAFI, di cui si è detto più sopra, si tratta del Report dell'EBA, *Opinion on Virtual Currencies*, 2014

[292] Report dell'EBA, *Opinion on Virtual Currencies*, 2014, p. 32 e ss.

nazionali. Infatti, secondo l'EBA, i rischi connessi all'utilizzo delle criptovalute sono superiori ai vantaggi che queste potrebbero apportare ai propri utenti, alla luce dei costi e delle tempistiche relate all'esecuzione di ogni transazione.[293] Se da un lato, l'EBA, in una prospettiva di breve periodo, ha sollecitato le Autorità nazionali di vigilanza a scoraggiare il compimento di qualsiasi operazione di acquisto o vendita delle monete virtuali, dall'altro, in un'ottica di lungo termine ha messo in luce la necessità che le istituzioni europee configurino una rete normativa armonizzata che affidi le operazioni in valute virtuali a soggetti centrali autorizzati.

Più di recente, il 17 marzo 2022, l'EBA, unitamente alle altre Autorità di vigilanza europee (ESMA ed EIOPA)[294] con un comunicato congiunto hanno catalizzato l'attenzione dei consumatori sugli elevati profili di rischio e di speculazione connessi alle criptovalute[295].

A questo proposito, le suddette Autorità hanno elaborato delle linee guida che i consumatori sono invitati a seguire al fine di operare sul mercato virtuale disponendo di tutte le informazioni necessarie.

---

[293] F. DI VIZIO, *op. ult. cit.*, p. 27 e ss.

[294] Trattasi di due Autorità indipendenti dell'Unione Europea. In particolare, in riferimento all'ESMA, si tratta dell'Autorità europea degli strumenti finanziari e dei mercati, istituita nel 2011, che svolge la funzione di garantire un migliore soddisfacimento delle esigenze finanziarie dei consumatori e rafforzare i loro diritti in qualità di investitori; garantire il corretto funzionamento dei mercati finanziari e promuovere la stabilità finanziaria. L'ESMA, inoltre, coordina le misure prese da autorità di vigilanza sui valori mobiliari e ha il compito di adottare misure di emergenza in caso di crisi. Cfr. anche il sito ufficiale dell'Unione Europea: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/esma_it
EIOPA è la sigla con cui si indica l'Autorità di vigilanza delle assicurazioni e delle pensioni aziendali o professionali. Anch'essa fu istituita nel 2011, fornisce pareri alla Commissione europea, al Parlamento europeo e al Consiglio dell'UE. Le sue funzioni principali possono essere così enucleate: (i) contribuire alla stabilità del sistema finanziario; (ii) garantire la trasparenza dei mercati e dei prodotti finanziari; (iii) contribuire alla protezione degli assicurati e degli iscritti e beneficiari dei sistemi pensionistici. Cfr. anche il sito ufficiale dell'Unione Europea: https://european-union.europa.eu/institutions-law-budget/institutions-and bodies/institutions-and-bodies-profiles/eiopa_it

[295] EBA, ESMA, EIOPA, EU *financial regulators warn consumers on the risks of crypto-assets,* marzo 2022.

In particolare, secondo le Autorità, i consumatori, prima di operare, dovrebbero sempre valutare la permanente possibilità di perdere tutto il denaro investito. Infatti, il primo alto profilo di rischio segnalato riguarda l'estrema volatilità[296] e la potenziale creazione di una bolla speculativa.

In *secundis*, le Autorità hanno rivolto l'invito ai consumatori ad essere consapevoli dell'assenza di strumenti di tutela, essendo le criptovalute attualmente esenti dalle norme europee sui servizi finanziari, nonostante l'emanazione delle più recenti direttive antiriciclaggio[297]. Pertanto, chiunque acquisti o venda valute virtuali non gode delle garanzie e delle tutele connesse ai servizi regolamentati. Altri profili critici riguardano l'assenza di opzioni di uscita, che dunque non permettono a chi acquista le valute virtuali di scambiarle con quelle tradizionali per un periodo di tempo lungo, rischiando quindi di subire gravi perdite.

Manca poi un principio di trasparenza a permeare l'andamento dei prezzi: la formazione di questi è assai variabile e poco accessibile, con esposizione al rischio di non vedersi corrisposto un prezzo adeguato a fronte di un acquisto o una vendita in cripto.

Ancora, alcune piattaforme di negoziazione non sempre sono risultate effettivamente funzionanti con i loro sistemi operativi, essendosi di frequente registrate interruzioni del sistema che hanno causato perdite ingenti in capo ad alcuni consumatori, impossibilitati ad operare nel momento in cui lo desideravano e dovendo successivamente fronteggiare fluttuazioni di prezzi ad essi sfavorevoli.

---

[296] F. CONSULICH, *op. ult. cit*., p. 154 secondo il quale la volatilità delle criptovalute è "drammatica" e "ciò ne impedisce sia la funzione di unità di conto che di riserva di valore (ciò peraltro espone a gravi rischi coloro che la impieghino proprio a tale ultimo scopo)".

[297] Vedi capitolo I, par.1.5, per un breve inquadramento sulle Direttive Antiriciclaggio. Si veda *infra*, al par. 3.11 del presente capitolo per un approfondimento sulla Direttiva (UE) 2018/843.

Le Autorità si sono anche pronunciate sul rischio di pubblicità ingannevoli in vertiginosa ascesa negli ultimi tempi[298]: di frequente, infatti, le informazioni fornite ai consumatori sono tendenzialmente incomplete, protese per lo più a promuovere questo nuovo strumento di pagamento e pertanto affatto esaustive nell'inquadramento dei rischi ad esso connessi.

3.9 (Segue) I provvedimenti delle Autorità italiane: Banca d'Italia e CONSOB

Sul piano interno, la Banca d'Italia, nel 2015, in piena condivisione di quanto statuito dall'European Banking Authority, ha scoraggiato banche e altri intermediari ad operare – detenendo, acquistando, vendendo – con le valute virtuali.[299] In particolare, essa ha posto in luce come in assenza di adeguata regolamentazione e di un consolidato reticolato normativo che disciplini natura e funzionamento delle valute virtuali, i rischi evidenziati dall'EBA siano suscettibili di concretizzarsi e provocare ingenti perdite patrimoniali, minacciando gravemente la stabilità degli intermediari finanziari. Inoltre, l'Autorità di vigilanza italiana ha specificato come "le concrete modalità di funzionamento degli schemi di VV (n.d.r. valute virtuali) possono integrare, 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

[298] In punto di pubblicità fuorvianti, cfr. anche A. MAURUSHAT, DAN HALPIN, *Investigation of Cryptocurrency Enabled and Dependent Crimes*, 2022, p. 236 ove si afferma "*Cryptocurrencies are heavily marketed on social media through hyped language, and false promotion through celebrity status with no links for business plans, details of products, but all with high claims of profitability*".

[299] Cfr. Banca d'Italia, sez. II, *Comunicazione sulle valute virtuali*, 30 gennaio 2015, in Bollettino di Vigilanza n. 1/2015.

investimento"[300]. Da ultimo, nell'avvertimento si richiede espressamente a banche ed intermediari vigilati dalla Banca d'Italia di fornire piena conoscenza alla propria clientela – sia che si tratti di persone fisiche che giuridiche – di tutti i rischi connessi all'esercizio di attività nel settore delle valute virtuali.

Di recente, precisamente il 28 aprile 2021, Banca d'Italia e la Commissione Nazionale per le Società e la Borsa (CONSOB) hanno di concerto diffuso un avvertimento, rivolto in particolare ai piccoli risparmiatori, sui rischi insiti nelle cripto-attività[301]. Tale intervento è stato ritenuto urgente, alla luce dell'attuale assenza di una omogenea normativa di regolamentazione sulle criptovalute nel panorama legislativo europeo. In particolare, l'avvertimento in discorso elenca tra i principali rischi rispetto alle operazioni in criptovalute la scarsa disponibilità di conoscenza e informazioni sulle modalità di determinazione dei prezzi; la volatilità delle quotazioni; la complessità delle tecnologie utilizzate; il pericolo di perdite a causa di malfunzionamenti dei sistemi, attacchi *hacker*, smarrimento delle credenziali per accedere ai portafogli elettronici.

Nell'avvertimento in analisi, inoltre, emerge come tutti i potenziali rischi appena menzionati abbiano un'importanza ancor più accentuata di fronte alla vertiginosa diffusione di offerte *online* di acquisto di criptovalute tendenziose e fuorvianti. Proprio su questo punto, è senz'altro meritevole di menzione una deliberazione emessa da CONSOB nel 2017[302] che ha sospeso in via cautelare per un periodo di

[300] Banca d'Italia, sez. II, *Comunicazione sulle valute virtuali*, 30 gennaio 2015, in Bollettino di Vigilanza n. 1/2015.

[301] Banca d'Italia e CONSOB, Comunicato Stampa, Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle cripto-attività, 18 aprile 2021. Reperibile al link: https://www.bancaditalia.it/media/comunicati/documenti/202101/CS_Congiunto_BI_CONSOB_cryptoasset.pdf

[302] Deliberazione CONSOB, n. 19866, *Sospensione, ai sensi dell'art. 101, comma 4, lett. b), del D.lgs. n. 58/1998, dell'attività pubblicitaria effettuata tramite il sito internet www.coinspace1.com relativa all'offerta al pubblico promossa dalla Coinspace Ltd. avente*

90 giorni la campagna pubblicitaria ingannevole compiuta da Coinspace Ltd, una società straniera che offriva possibilità d'acquisto di "pacchetti di estrazione" comprensivi di un certo ammontare di monete, con promesse di guadagno pari al 50% entro il termine di un anno. A fondamento della delibera la CONSOB ha posto, principalmente, due rilievi. In primo luogo, la violazione dell'articolo 101, comma 4, lett. b) T.U.F. il quale vieta la pubblicazione di qualsiasi annuncio pubblicitario di offerte al pubblico di prodotti finanziari diversi dagli strumenti finanziari comunitari".

In secondo luogo, tale sito non risultava riconducibile ad alcun soggetto determinato: nell'avvertimento si legge infatti che "il sito www.coinspace1.com risulta registrato da un soggetto la cui identità è celata da un fornitore di servizi di *privacy*".

3.10 (Segue) Il Report di EUROPOL ed EUROJUST.

A giugno 2019, le due Autorità europee nate per combattere ogni forma di criminalità nell'ambito della cooperazione giudiziaria e di polizia hanno presentato un Report[303] di analisi dei rischi legati all'uso delle monete virtuali. In particolare, le Autorità si sono pronunciate sui rischi di dispersione di dati, delocalizzazione, minacce per gli ordinamenti interni, frammentazione del quadro normativo sul piano di cooperazione internazionale e nuove sfide e prospettive con enti pubblici e privati.

Per quanto concerne la delocalizzazione, nel Report in discorso si evidenzia come l'abuso della crittografia a fini illeciti e di strumenti di anonimato – in particolare nella dimensione del *dark web* – abbiano ad oggi condotto a situazioni in cui non è più possibile identificare il territorio di azione del criminale e, dunque, non è possibile individuarne la giurisdizione

ad oggetto "pacchetti di estrazione di criptovalute", 1° febbraio 2017. Reperibile al link: https://www.consob.it/web/areapubblica/bollettino/documenti/hide/cautelari/soll/d19866.htm

[303] Report EUROPOL-EUROJUST, *Common challenges in combating cybercrime*, June 2019, pp. 11 e ss.

e il panorama legale di riferimento. Ancora, l'utilizzo crescente di strumenti *cloud* comporta che i dati in esso conservati siano localizzabili in giurisdizioni diverse.[304]

Un'altra problematica messa in luce nel Report EUROPOL - EUROJUST concerne le notevoli differenze intercorrenti tra i vari ordinamenti domestici nel sanzionare condotte criminose e nella disciplina investigativa e di raccolta di prove connesse ai *cybercrimes*.

Spesso, infatti, le opere di allineamento e coordinamento tra Paesi risultano assai complesse alla luce della rapida e costante evoluzione del panorama criminoso digitale.

Se da un lato le pronunce giurisprudenziali possono essere lette al fine di colmare lacune di normativa specifica, dall'altro però ad oggi non è rinvenibile un numero adeguato di pronunce che affronti direttamente le tematiche in discorso, come ad esempio l'uso distorto delle criptovalute a scopi criminosi. Allo stesso tempo, un'adeguata armonizzazione normativa consentirebbe un netto miglioramento anche sotto il profilo investigativo e di raccolta delle prove.

Nel 2022, l'EUROPOL ha pubblicato un altro Report[305] dedicato ad un'analisi aggiornata sull'utilizzo delle criptovalute a fini illeciti. Nel documento, si legge che il riciclaggio è l'attività principale associata all'utilizzo illecito di criptovalute[306]. In particolare, vengono richiamati i principali rischi connessi alla pseudanonimità, alla volatilità e alla struttura decentralizzata del sistema Bitcoin. Ancora, si fa menzione del

[304] Report EUROPOL-EUROJUST, *Common challenges in combating cybercrime*, June 2019, pp. 13

[305] EUROPOL Spotlight, Cryptocurrencies: tracing the evolution of criminal finances, 2022. Reperibile al link: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

[306] EUROPOL Spotlight, Cryptocurrencies: tracing the evolution of criminal finances, 2022. Reperibile al link: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances. A pag. 11 del Report viene dichiarato che "*Money laundering is the main criminal activity associated with the illicit use of cryptocurrencies*".

basso costo e della rapidità delle transazioni che attirano i criminali, lasciando loro ampio raggio d'azione manipolando i vuoti normativi sussistenti tra le giurisdizioni di vari Stati. Viene, inoltre, evidenziato come l'utilizzo di criptovalute ai fini di riciclaggio sia brutalmente aumentato con la pandemia da COVID-19[307].

Alla luce di quanto appena riportato in relazione ai pareri espressi dalle Autorità di vigilanza e controllo nazionali ed eurounitarie, può notarsi come le stesse condividano posizioni comuni e suffragate da simili argomentazioni.

Può dirsi, dunque, che il Legislatore sembri senz'altro munito di ogni strumento utile per prevenire e contravvenire ogni rischio individuato dai maggiori organi centrali. Infatti, nonostante debba considerarsi che il fenomeno criptovalutario sia tuttora in evoluzione e costante mutamento, ciò non toglie che siano ormai chiari i pilastri strutturali del suo funzionamento.

Pertanto, in una prospettiva *de iure condendo* di regolamentazione in materia di criptovalute, se da un lato il Legislatore dovrebbe certamente trattenersi dal regolamentare con precocità questo ecosistema emergente, rischiando altrimenti di incorrere in una produzione normativa non applicabile, dall'altro potrebbe tuttavia dedicarsi quantomeno ad un'implementazione dei sistemi di controllo, alla luce delle debolezze sistemiche appena considerate. Si ritiene, dunque, che l'obiettivo ultimo dovrebbe essere la tutela del progresso e di ogni realtà Fintech sino ad ora raggiunto grazie allo sviluppo delle nuove tecnologie, con l'accortezza di ricucire quelle crepe normative che fornirebbero alla platea criminale uno spazio di manovra estremamente dannoso per l'intero ordine economico globale.

[307] EUROPOL, *European Union Serious and Organised Crime Threat Assessment 2021 - A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime*, 2021. Reperibile al link: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organisedcrime-threat-assessment

3.11 La risposta del Legislatore europeo all'utilizzo criminogeno delle criptovalute: la V Direttiva Antiriciclaggio, il suo recepimento interno e altri interventi preventivi.

Come sinteticamente riportato nel capitolo I[308], accennando all'evoluzione della normativa antiriciclaggio sul piano eurounitario, dai primi anni '90 si è assistito ad un crescente impegno del Legislatore sovranazionale nell'imposizione agli Stati membri dell'Unione Europea del raggiungimento di obiettivi precisi – nel rispetto dell'art. 288, par. 3 TFUE – per combattere e prevenire la realizzazione del delitto di riciclaggio, nelle sue molteplici manifestazioni.

L'intervento più recente si è concretizzato con la Direttiva 2018/843, intervenuta a modifica della precedente Direttiva Antiriciclaggio[309].

Può dirsi che entrambe le Direttive siano volte a rinforzare e potenziare il sistema di prevenzione degli Stati membri, valorizzando l'approccio preventivo basato sul rischio, il c.d. *risk-based approach*. Tale principio è stato scolpito nei considerando della IV Direttiva Antiriciclaggio[310], ove si legge che *"(...) dovrebbe essere adottato un approccio olistico basato sul rischio. Tale approccio basato sul rischio 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 gli Stati membri e per l'Unione per individuare, comprendere e mitigare i rischi di riciclaggio e di finanziamento del terrorismo a cui sono esposti*. (…)".

[308] Cfr. par. 1.5
[309] Direttiva 2015/849
[310] Cfr. considerando 22 e 23 della Direttiva 2015/849.

A fondamento della Quinta Direttiva antiriciclaggio, risiede la necessità di garantire una maggiore trasparenza delle operazioni finanziarie, delle società, dei trust e degli istituti giuridici affini e – in linea più generale – del contesto economico e finanziario eurounitario.

In primo luogo, alla luce del minaccioso rischio dell'anonimato garantito dall'utilizzo delle valute virtuali, la Quinta Direttiva è intervenuta estendendo il novero dei soggetti obbligati a conformarsi agli obblighi antiriciclaggio, che ad oggi ricomprendono anche i prestatori di servizi di cambio valute virtuali e valute legali; i prestatori di servizi di portafoglio digitale; i galleristi; i gestori di case d'asta e gli antiquari.

Proseguendo nell'analisi della Direttiva in discorso, essa ha imposto obblighi più stringenti per la verifica del regolare utilizzo delle carte prepagate. Più precisamente, sono state abbassate le soglie preesistenti per l'utilizzo delle carte prepagate senza dover adempiere l'obbligo di verifica della clientela[311]. Inoltre, con la Direttiva in discorso sono state estese anche le misure di trasparenza della titolarità effettiva di società e trust, prevedendo l'istituzione di registri nazionali accessibili. Sono state poi rafforzate le competenze e i poteri delle Financial Intelligence Units (FIUs) per l'analisi interna dei dati e la collaborazione interstatale. In particolare, si è previsto che le FIU di ciascun Paese possano ottenere informazioni che permettano di ricondurre gli indirizzi della valuta virtuale alla vera identità del proprietario della stessa[312].

È stata poi prevista, all'art. 1, punto 2), lett. d) della Quinta Direttiva, la definizione di valuta virtuale, come "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

[311] La soglia è stata ridotta da euro 250 a euro 150.
[312] Cfr. Considerando nn. 8,9,10,11,16, Direttiva 2018/843.

giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente". Sempre in punto di criptovalute, la Direttiva in discorso specifica anche che "le valute virtuali non dovrebbero essere confuse con la moneta elettronica quale definita dall'articolo 2, punto 2 della Direttiva 2009/110/CE del Parlamento europeo e del Consiglio"[313].

Sul piano interno, il Legislatore nostrano ha recepito la Quinta Direttiva antiriciclaggio con il d. lgs. 125/2019, entrato in vigore l'11 novembre 2019.

Tale decreto legislativo ha modificato e integrato il precedente d.lgs. 231/2007[314], che aveva recepito la Direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Per limiti imposti dalla presente trattazione, si accennerà di seguito brevemente alle sole modifiche intervenute con il d. lgs. n. 125/2019, il quale ha prodotto un forte impatto nella lotta al riciclaggio mediante l'utilizzo di strumenti quali le criptovalute.

Il d. lgs. n.125/2019 ha esteso la definizione di valuta virtuale, comprendendovi anche il loro utilizzo a fini di finanziamento – e non solo di scambio. Inoltre, l'attività di cambiavalute è stata inserita nei servizi di conversione "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"[315]. Ancora, i c.d. *wallet providers* – nonché prestatori di servizi di portafoglio digitale – vengono inclusi nella disciplina dei prestatori di servizi di portafoglio digitale e per questo assoggettati agli obblighi antiriciclaggio.

[313] Cfr. Considerando n. 10), Direttiva 2018/843.

[314] Tale decreto fu modificato anche con il d. lgs. 90/2017, in recepimento della Quarta Direttiva antiriciclaggio.

[315] Art. 1, comma 2, lett. ff), d. lgs. n. 125/2019.

In questo modo, il Legislatore italiano ha colmato molteplici lacune di tutela esistenti dalla previgente disciplina, la quale consentiva solamente un controllo antiriciclaggio durante la fase di conversione delle valute virtuali in moneta fisica, lasciando sprovvisti di alcun controllo i soggetti che permettevano invece la detenzione e la movimentazione delle stesse[316].

La Direttiva 2018/843 non costituisce, tuttavia, l'unica presa di posizione da parte del Legislatore contro il dilagare del reato di riciclaggio. Di notevole rilievo è anche il Regolamento UE 2018/1672.
Tale fonte secondaria ha ampliato le misure destinate al monitoraggio del trasporto transfrontaliero del denaro contante, la condivisione e l'utilizzo delle relative informazioni. In particolare, le Dogane sono obbligate a trasmettere ogni quindici giorni alla FIU del proprio Paese le dichiarazioni[317] sul trasporto di valori pari o maggiori di euro 10.000. Inoltre, sempre le Dogane devono trasmettere alla FIU le informazioni relative a casi di sospetto riciclaggio o finanziamento del terrorismo.

Anche se non finalizzato a combattere il reato di riciclaggio, un altro strumento meritevole di menzione, destinato a combattere l'utilizzo delle criptovalute per finalità illecite, è la Direttiva 2019/713/UE del Parlamento europeo e del Consiglio del 17 aprile 2019 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, sostitutiva della decisione quadro 2001/413/GAI del Consiglio.

Con tale strumento legislativo, il Legislatore eurounitario ha voluto intensificare la lotta contro le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti, come mezzi di finanziamento della criminalità

---

[316] 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*, in Sistema Penale, 6 maggio 2020. In argomento v. NADDEO, *Nuove frontiere del risparmio, Bit Coin Exchange erischio penale*, in Diritto penale e processo, fasc. 1/2019, p. 10, per cui il mancato coinvolgimento dei *wallet provider* sottraeva al monitoraggio le operazioni di riciclaggio aventi ad oggetto valute virtuali provenienti da reati presupposto *on line integrated*.

[317] Tali dichiarazioni riguardano sia il contante tradizionale sia strumenti come carte di pagamento e altri mezzi idonei a prevedere valore liquido.

organizzata e delle relative attività criminose. Dall'altro, la Direttiva vuole promuovere anche il mercato unico digitale, la cui integrità è minacciata da condotte illecite connesse ai mezzi di pagamento come carte di debito e credito, portafogli elettronici e valute virtuali.[318] Si segnala che la Direttiva in discorso è stata recepita nell'ordinamento italiano con d. lgs. 8 novembre 2021, n. 184[319].

3.12 La sussumibilità del "cripto-riciclaggio" nelle fattispecie codicistiche.

Se da un lato le Autorità di Vigilanza e controllo hanno posto in evidenza i rischi di riciclaggio nascosti dietro al funzionamento delle criptovalute, dall'altro la dottrina ha cercato di fornire risposte di tutela, sostenendo la punibilità del "cripto-riciclaggio" ricorrendo alle disposizioni in materia di riciclaggio e autoriciclaggio.

Ammesso, infatti, che il cripto-riciclaggio costituisca una forma di *cyberlaundering*, è opportuno chiedersi come esso possa essere sanzionato e prevenuto all'interno dell'ordinamento italiano. Infatti, alla luce delle molteplici segnalazioni da parte delle principali Autorità, la

[318] S. CARRER, *Lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti: emanata la direttiva (UE) 2019/713*, in Giurisprudenza Penale Web, 2019, pp. 7-8. L'Autrice rileva come "*è stato stimato che nel 2013 le condotte criminose abbiano sottratto 1,44 miliardi di euro mediante frodi con mezzi di pagamento diversi dai contanti e che ogni anno i cittadini europei ricevono circa 36 miliardi di messaggi di phishing*".

[319] Il d. lgs. 8 novembre 2021, n. 184 è titolato "*Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti*". È entrato in vigore il 14 dicembre 2021 ed è intervenuto a modificare la rubrica del reato ex art. 493 *ter* c.p., in il "indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti"; ha poi introdotto la nuova fattispecie ex art. 493 *quater* c.p. di "*detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti*"; ancora, ha provveduto a modificare l'art. 640 *ter* c.p. sul reato di "*frode informatica*", introducendo una circostanza aggravante nel caso in cui la condotta fraudolenta comporti "*un trasferimento di denaro, di valore monetario o di valuta virtuale".* Infine, è stato inserito l'art. 25 *octies*.1 nel d.lgs. n. 231/2001, rubricato "*Delitti in materia di strumenti di pagamento diversi dai contanti*".

dottrina si è dedicata ad individuare una soluzione ad un apparente vuoto di tutela, seppur lasciando aperti spazi di riforma per il legislatore.

Rinviando al precedente capitolo per un inquadramento generale del delitto di riciclaggio, previsto ex art. 648 *bis* c.p., giunti a questo punto della trattazione, sembra opportuno vagliare la fondatezza dell'ipotesi dell'applicabilità della disciplina codicistica anche al riciclaggio realizzato servendosi di monete virtuali, quali i Bitcoin.

L'obiettivo di tale operazione esegetica, alla luce di un'attuale lacuna normativa nell'ordinamento italiano, è naturalmente fondato sull'evitare qualsiasi forma di violazione del principio di divieto di analogia della legge penale, analizzando l'applicabilità dell'art. 648 *bis* c.p. nella sua totalità, oppure considerando l'introduzione di circostanze aggravanti o, se necessario, l'integrale configurazione di una disciplina apposita che sanzioni il riciclaggio realizzato tramite criptovalute.

Prendendo avvio da un'analisi degli elementi costitutivi del reato, non si può non considerare in prima battuta l'identificazione del bene giuridico tutelato. Come affrontato in corso di analisi del reato di riciclaggio "tradizionale", la questione del bene giuridico tutelato si è visto essere assai discussa e complessa. Tuttavia, nonostante l'esistenza di voci non unanimi in dottrina, rifacendosi alla corrente maggioritaria, si è potuto in precedenza concludere che l'art. 648 *bis* c.p. tuteli, *latu sensu*, l'amministrazione della giustizia.

Il primo tratto in comune con il "cripto-riciclaggio" – seppur meritevole di una sottile specificazione – ricorre proprio in tema di bene giuridico. Infatti, come sostenuto da autorevole dottrina[320], si prospetta la necessità di tutelare il bene dell'amministrazione della giustizia, in senso lato, ma prestando attenzione particolare alla tutela della tracciabilità dei flussi finanziari. Come

[320] A. M. DELL'OSSO, *op. ult. cit.,* p. 181. Cfr anche L. STURZO, *op. ult. cit*. A favore, anche G. J. SICIGNANO, *L'acquisto di bitcoin con denaro di provenienza illecita, in* Archivio Penale 2020, 2, p. 9

dichiara l'Autorità Nazionale Anticorruzione (ANAC), la tracciabilità dei flussi finanziari costituisce non tanto "uno strumento di monitoraggio dei flussi finanziari, bensì un mezzo a disposizione degli inquirenti nelle indagini per il contrasto delle infiltrazioni delle mafie nell'economia legale"[321].

A parere di chi scrive, l'individuazione di questo bene giuridico più circoscritto accanto a quello più ampio dell'amministrazione della giustizia parrebbe più idoneo a fornire una tutela più decisa e puntuale, volta a sanzionare e prevenire qualsiasi modalità di dispersione *online* delle tracce delle transazioni realizzate in criptovalute.

Proseguendo l'analisi in discorso, si guarderà ora con attenzione alla condotta tipica tenuta dai criminali nello svolgimento del "cripto-riciclaggio". Sempre mantenendo un'ottica comparativa e di confronto con il riciclaggio tradizionale, come sopra esposto, giova ricordare che il Legislatore italiano ha configurato il delitto di riciclaggio come reato a forma libera e di pericolo concreto[322], ciò significando che la rilevanza penale della condotta emerge ogniqualvolta questa *sia idonea* a ostacolare l'accertamento della provenienza delittuosa di denaro, beni o altre utilità[323] e che, dunque, in altre parole, possa essere sanzionata ogni tipo di condotta dissimulatoria.

La fattispecie ex art. 648 *bis* c.p., come visto nel capitolo I del presente elaborato, si connota per una formulazione di condotte molto ampia – sostituzione, trasferimento, compimento di altre operazioni che

---

[321] Si rinvia, sul punto, al sito ufficiale dell'ANAC per ulteriori approfondimenti: https://www.anticorruzione.it/-/tracciabilit%C3%A0-dei-flussi-finanziari

[322] Cfr. M. CROCE, *op. ult.* cit.. In argomento, A. ZACCHIA, *La natura del reato di riciclaggio*. Nota a Cass. sez. II pen., 13 luglio 2016, n. 29611, in Cass. pen. 2017, 7, 2824 ss.

[323] Sul punto si veda L. STURZO, *op. ult. cit*., ove si rileva che "*la probabilità che il sistema Bitcoin si trasformi in un sistema di ripulitura dei proventi illeciti internazionali sarà direttamente proporzionale all'abilità che lo stesso mostrerà di rendere difficoltoso l'accertamento della provenienza di quel valore*".

ostacolino l'identificazione della provenienza delittuosa di denaro, beni o altre utilità[324].

Alla luce di quanto appena ricapitolato, in ipotesi di "cripto-riciclaggio" è pacifico come sia proprio la frammentazione del c.d. *digital trial*[325] tramite i servizi di *mixing*, ad essere essa stessa idonea, per la sua potenzialità dissimulatoria, ad offuscare l'origine illecita delle monete virtuali.

Dunque, in forza di questa capacità oscurante, pare pacifico per l'elemento della condotta poter ricondurre il *cyberlaundering* tramite criptovalute alla fattispecie ex art. 648 *bis* c.p.[326]

Successivamente, per quanto concerne la definizione di oggetto materiale del reato, è necessario comprendere se le criptovalute siano sussumibili nella voce di "denaro", "beni" o "altre utilità". Il quesito in discorso parrebbe non essere di immediata soluzione, alla luce della controversa natura giuridica delle criptovalute.[327]

Per le ragioni sopra esposte e come concluso poc'anzi, nel presente elaborato sembra opportuno condividere il filone dottrinale secondo il quale le criptovalute hanno natura giuridica di strumento finanziario.

Ripercorrendo, infatti, il tentativo definitorio della natura giuridica delle valute virtuali, si consideri che secondo l'opinione prevalente, la criptovaluta non può considerarsi una moneta in senso proprio, alla luce delle

[324] Cfr. L. PICOTTI, *Profili penali del cyberlaundering,: le nuove tecniche di riciclaggio, in Riv. Trim. Dir. pen. dell'economia*, 3-4, 2018, p. 613

[325] In argomento, cfr. L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio abusivo di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, in *Rivista di Diritto Bancario*, n.5, 2018, p. 4

[326] Cfr. M. CROCE, *op. ult. cit,* p. 137. In argomento, si veda M. NADDEO, *op. ult. cit.*, p. 106.

[327] Si veda il paragrafo 3.2 del presente elaborato. In argomento, cfr. L. SANTONI, *Operazioni in criptovaluta e abusivismo finanziario: nota a Cass. Pen., sez. II, 25 settembre 2020, n. 26807*, in Riv. Dir. Bancario, Fascicolo 2/2021

caratteristiche sopra evidenziate, quali il mancato corso forzoso e legale[328] e l'impossibilità di garantire *tout court* le funzioni di riserva di valore, unità di conto e mezzo di scambio. Infatti, sul punto dottrina maggioritaria[329] - e peraltro più recente – sostiene che le criptovalute non siano assimilabili al denaro, tant'è che se tale assimilazione fosse affermata ai fini dell'applicabilità della disciplina ex art. 648 *bis* c.p., verrebbe violato il divieto di analogia.

Come la criptovaluta non è riconducibile al denaro, nemmeno sembra sussumibile nella categoria dei beni. Infatti, sempre per dottrina maggioritaria[330], le criptovalute non sono sussumibili nella categoria dei beni, in quanto sono beni solamente le *res* tangibili e materiali, passibili di essere oggetto di diritti. Recentemente, tuttavia, deve segnalarsi una presa di posizione contraria della giurisprudenza[331] la quale ha definito i dati informatici come beni mobili.

È così che, dunque, riprendendo l'orientamento condiviso e sostenuto anche dalla giurisprudenza, che identifica le criptovalute come strumento finanziario, se non sembra possibile ricondurre le criptovalute al denaro e nemmeno nella categoria dei "beni", pare calzante la sussumibilità delle stesse nella categoria delle "altre utilità", essendo essa una formula assai ampia, tale da ricomprendere al suo interno qualunque entità che sia economicamente apprezzabile[332].

---

[328] 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, fasc. 3, 2015, p. 415

[329] Per tutti, M. CROCE, *op. ult. cit*., p. 138; D. YERMAK, *Is Bitcoin a real currency? An economic appraisal*, NBER Working Paper No. 19747, 2013, pp. 2 e ss.

[330] Per tutti, FIANDACA-MUSCO, *op. ult. cit.*, p. 23 "è definibile cosa, nel senso del diritto penale, ogni oggetto corporale o fisico: in altri termini, ogni entità fisica del mondo esterno che presenti i caratteri della definitezza spaziale e della esistenza autonoma". Le criptovalute, però, sono dati informatici, dunque prive dei requisiti appena menzionati e quindi, se considerate come beni, comporterebbero una violazione del divieto di analogia e del principio di tassatività.

[331] Cass. Pen., sez. II, 13 aprile 2020, n. 11959.

[332] M. CROCE, *op. ult. cit*., p. 138.

Sembra poi condivisibile, come visto sia per il riciclaggio che per il *cyberlaundering* in generale, la sufficienza del dolo generico come elemento soggettivo.

Questione correlata e parallela alla sussumibilità del *cyberlaundering* tramite cripto-valute nel delitto disciplinato ex art. 648 *bis* c.p. riguarda la sussumibilità dello stesso nella fattispecie ex art. 648 *ter*.1 c.p., venendosi così a configurare il c.d. "*cyber-self laundering*"[333].

Sotto il profilo dell'oggetto materiale del reato, sembra potersi riprendere la riflessione appena compiuta che porta a ricomprendere le criptovalute nella categoria delle "altre utilità"[334]. Infatti, come suffragato da autorevole dottrina, nella categoria delle "altre utilità" non solo può essere ricompresa ogni utilità economicamente apprezzabile, ma anche "tutto ciò che rappresenti il frutto dell'attività criminosa precedente"[335]. Tale sintagma appare estremamente calzante a suffragio del rapporto di immedesimazione che sussiste tra autore del reato presupposto e del reato di riciclaggio.

Per quanto concerne, invece, il profilo soggettivo, in tema di "c*yber-self laundering*" di criptovalute, vi sono alcune problematiche aperte.

Se da un lato è pacifico che il soggetto autore del reato presupposto e del reato di riciclaggio, risponda per autoriciclaggio ex art. 648 *ter*.1 c.p., dubbia è la qualificazione giuridica della condotta realizzata da un soggetto *extraneus* – quale un *exchanger provider* – che abbia contribuito in modo rilevante alla condotta di autoriciclaggio. Il quesito fondamentale riguarda la punibilità di questo soggetto *extraneus* a titolo di concorso in autoriciclaggio o per riciclaggio[336]. Naturalmente, il quesito è di notevole rilevanza ai fini di applicabilità delle sanzioni previste nel codice e delle relative circostanze.

[333] Espressione presa da M. CROCE, *op. ult. cit.,* p. 143.
[334] F. POMES, *op. ult. cit.*, p. 169.
[335] F. POMES, *op. ult. cit*., p. 170. Sul punto si veda anche Cass. Pen., sez. II, 17 gennaio 2012, n. 6061.
[336] F. POMES, *op. ult. cit.*, p. 173

Infatti, non può sfuggire che il profilo sanzionatorio dell'autoriciclaggio sia assai più modesto rispetto a quello del riciclaggio[337].

Restando fedeli alla *littera legis* dell'art. 648 *ter*.1 c.p., il reato di autoriciclaggio si configura come reato proprio, sanzionando solamente l'autore del reato presupposto[338]. Secondo questa impostazione, dunque, per il terzo che non abbia partecipato alla realizzazione del reato potrebbe configurarsi un'ipotesi di concorso nel reato proprio *ex* artt. 110 e 117 c.p. Più precisamente, in tema di reato di autoriciclaggio deve farsi menzione dell'annosa questione – alla quale sembra, come si vedrà in seguito, che la Corte di Cassazione abbia fornito una risposta – sul rapporto tra la fattispecie in discorso con l'istituto penalistico del concorso di persone. Più estensivamente, la questione principale riguarda la possibilità per un soggetto *extraneus* – che nel caso di specie sarebbe il terzo *exchanger* – di concorrere nel reato con l'*intraneus*, ossia l'autore del delitto di autoriciclaggio, nonché autore del reato presupposto, venendosi in tal modo a configurare una condotta tipica plurisoggettiva di un reato proprio.

In particolare, se si abbracciasse l'ipotesi ricostruttiva secondo la quale anche una fattispecie plurisoggettiva debba essere attuata da soggetti qualificati, si avrebbe concorso in autoriciclaggio ogni volta in cui sia l'autore sia il concorrente nel reato presupposto realizzassero la condotta criminosa. Tuttavia, sul punto, come tradizionalmente sostenuto da dottrina maggioritaria, è sempre stato escluso il concorso ai sensi dell'art. 117 c.p. e 110 c.p. relativamente al soggetto che contribuiva nel procedimento di pulitura dei proventi illeciti. Infatti, in questo modo, si assisterebbe ad un ridimensionamento del sistema

[337] A. GULLO, *Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato*, in Dir. Pen. Contemp., 2018, pp. 365 e ss.

[338] Per approfondimenti, v. G. FIANDACA, E. MUSCO, *I delitti contro il patrimonio, Diritto penale, Parte speciale, vol. II*, 2015

sanzionatorio nei confronti del terzo, sfruttando una previsione *ab origine* creata per punire l'autoriciclatore. Sul punto, è d'altronde intervenuta una recente pronuncia della giurisprudenza di legittimità[339] secondo la quale sarebbe, invece, plausibile contestare la commissione del reato proprio nei confronti di un soggetto non qualificato. Sembra, dunque, possibile che il terzo *exchanger* possa essere qualificato come concorrente *extraneus* nel reato proprio, poiché l'autore del reato presupposto non avrebbe potuto realizzare l'operazione di ripulitura delle valute senza il contributo concreto del cambia valute.

Dunque, onde evitare un simile esito argomentativo viziato da oggettiva irragionevolezza, sembra sul punto condivisibile una recente pronuncia della Corte di Cassazione[340], la quale ha sancito la punibilità a titolo di riciclaggio di questi soggetti terzi, che abbiano dato il proprio contributo materiale all'autoriciclatore nella realizzazione della condotta criminosa. La Cassazione ha optato, quindi, in occasione della pronuncia in discorso, per la c.d. differenziazione dei titoli di responsabilità da reato: l'autore o concorrente nel delitto presupposto risponderà di autoriciclaggio; nei confronti del terzo al quale siano affidati i proventi e che li destina allo svolgimento di attività economiche, si applicherà invece l'art. 648 *bis* c.p.

Considerando quanto emerso nello sviluppo del presente capitolo, a parere di chi scrive l'ordinamento italiano è munito di una risposta sanzionatoria contro il reato di riciclaggio *online* che preveda l'impiego delle criptovalute in attività illecite. Potrebbe forse ipotizzarsi, in una prospettiva *de iure condendo*, l'introduzione di circostanze aggravanti che aumentino la risposta edittale qualora siano utilizzate tecniche di "cripto-riciclaggio" assai sofisticate: in via esemplificativa, si pensi al ricorso a *software* utilizzati dolosamente per permanere in una condizione di anonimato.

[339] Cass., sez. II, sent. 14 luglio 2017, n. 42561
[340] Cass. Pen., sez. II, 17 gennaio 2018, n. 17235

L’attenzione del Legislatore interno, appurata la sussumibilità della condotta nelle fattispecie codicistiche, potrebbe dunque focalizzarsi su un’implementazione dei sistemi sanzionatori verso l’utilizzo a scopi criminosi delle nuove tecnologie. Questo tipo di risposta, sul piano domestico, però, deve necessariamente essere appoggiata a livello europeo, dove si auspica la promozione di un quadro regolatorio sulle criptovalute omogeneo e capillare, in grado di prevenire ogni loro forma di utilizzo illecito.

CAPITOLO IV

THE OFFENCE OF MONEY LAUNDERING IN THE DUTCH LEGAL SYSTEM: BETWEEN THE DUTCH CRIMINAL CODE AND THE MOST RECENT CASE LAW

4.1 The Netherlands: towards a new tax heaven

The purpose of this chapter is to provide a general overview of the offence of money laundering as regulated in the Dutch Criminal Code. Accepting this comparative perspective, the latter part of the paper proposes a framework of similarities and differences between the system in question and the Italian one, promoting a wide-ranging study approach. There will also be a brief practical account of the most recent and relevant money laundering incidents, including through the use of cryptocurrencies, that have engaged the Dutch authorities in recent years.

Ab initio to the analysis at hand, it seems of considerable interest to the writer to emphasize how, in the Netherlands too, the regulation against money laundering plays an essential role in the protection of the state economic order.

The Netherlands is globally recognized as a country that has achieved a very high level of development, the symbol of which is the wide range and optimal functioning of public services. Not only an icon of progress in the management of administrative activity, but Holland also stands out for continuous growth in the financial sector. In support of these observations, there is a confirmation provided by the International Monetary Fund in 2010[341] , which ranked the Netherlands seventh in size and interconnectedness with the financial sectors of other jurisdictions. However, this condition of steadily growing prosperity acts as an attractive element for criminal actors wishing to launder money[342]. Indeed, some scholars have described the Netherlands as a 'gateway country for crime[343] .

Specifically, according to recently conducted analyses[344] , as many as 83 market sectors with a high risk of money laundering were found in the Netherlands, among which the casino, betting and gambling sector stands out. In particular, multiple criminal infiltrations, high cash circulation and lack of clarity in the management structure of the various activities have been detected. In addition, the hotel and restaurant sector is heavily contaminated. Criminal infiltration operating in the territory for the purpose of money laundering accounts for as much as 2.88% of

[341] IMF Board Executive Board Paper '*Integrating Stability Assessments Under the Financial Sector Assessment Programme into Article IV Surveillance*' and '*Background Material*', August 2010

[342] FATF, *Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism*, THE NETHERLANDS, 25 February 2011, p. 23.

[343] UNIVERSITY OF UTRECHT AND AUSTRALIAN NATIONAL UNIVERSITY, B. UNGERDRS. M. SIEGEL, *The Amount and Effects of Money Laundering*, 2006.

[344] See for the Netherlands, TRANSCRIME, *Assessing the risk of money laundering in Europe. Final report of project IARM*, 2017, p. 12. See for Italy, TRANSCRIME, *The money laundering risk in Italy. Final report of the IARM project*, 2017, p. 10. In the same analysis, it is highlighted that in Italy the sector with the highest recycling risk is the catering industry, followed by the construction industry, the management of bathing establishments, sports associations and recreational activities.

the companies with registered offices in the Netherlands have stable relationships with risky jurisdictions[345]. While Italian companies are reportedly less connected to *offshore* countries overall, in the Netherlands - and also in the United Kingdom - beneficial owners of companies and businesses are more difficult to trace.

A common trait uniting Italy and the Netherlands is the presence of sectors such as energy, water and waste that are characterized by greater complexity and opacity in the management of their activities[346].

Moreover, considering that according to a recent *ranking* by the *Tax Justice Network* in 2021, the Netherlands was ranked fourth among tax havens, right after the British Virgin Islands, the Cayman Islands, and Bermuda[347]. It is no mere coincidence, in fact, that several multinationals have chosen the Netherlands as their legal seat[348], see for example, among the best known, the transport company Uber or the telecommunications company Mediaset.

The presence of a financial environment unencumbered by strict tax regulations[349], which leaves ample room for manipulating operations by

[345] See S. LATINI, *Anti-Money Laundering*: *EU updates list of high-risk third countries*, in IPSOA Quotidiano, 11 March 2022. The author reports an updated list, which now amounts to no less than 23 countries: Afghanistan, Barbados, Burkina Faso, Cambodia, Cayman Islands, Haiti, Jamaica, Jordan, Mali, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Philippines, Senegal, South Sudan, Syria, Trinidad and Tobago, Uganda, Vanuatu, Yemen, Zimbabwe.

[346] Transcrime, *The money laundering risk in Italy. Final report of the IARM project*, 2017, p. 10.

[347] The complete ranking can be found *online* at: https://cthi.taxjustice.net/en/

[348] On this topic, please refer to the interview with Prof. Jan Vleggeert, Professor of Tax Law at Leiden University. Please refer to the *online* link: https://www.universiteitleiden.nl/en/news/2021/07/multinationals-in-the-netherlands-have-many-ways-to-lower-tax-burden

[349] On this subject, see D. A. LESLIE, *op. cit.*, p. 25 where he explains how "*In the public sector, money laundering manifests its effects in the form of unpaid taxes or tax evasion. Tax evasion is a problem that is not only typical to developed economies, but to developing and under-developed economies alike. Recent estimates show that in the Netherlands and the United States, tax evasion is the largest part of estimated criminal income, constituting between 4 to 6% and 6 to 15% of the Gross Domestic Products (GDPs) of these countries, respectively*."

market participants, lends itself, however, to an aggressive stance by organised crime in the Netherlands, which - as seen *above* - is, as a rule, closely linked to money laundering activities.

The constant menace of organized crime in the territory is not only 'hidden' among financial and entrepreneurial activities, but also manifests itself in conducts related to a primordial and ancient criminal system. See, for instance, the recent murder in the public streets of Amsterdam of the journalist Peter de Vries, a nationally known crime expert, whose killing is symbolic of a violent takeover of the most heinous criminals within the Dutch territory[350] .

It can, therefore, be considered that in the Netherlands the rampant risk of money laundering activities is becoming more and more imminent and concrete.

Therefore, in the light of the above hints, which are an expression of the controversial relationship between legality and illegality in the Netherlands, a brief description of the regulation of the offence of money laundering under the Dutch Criminal Code will be given below.

The aim of the discussion will be, first and foremost, to try to highlight the similarities and differences with respect to the discipline under the Italian Criminal Code, alongside some of the writer's interpretative proposals. Secondly, an attempt will be made to give an account of the most relevant money laundering events that have most engaged the country's authorities in recent times.

Also on this topic, see AMEDEO A., M. BAGELLA, AND F. BUSATO, *Money laundering in a two sector model: Using theory for measurement*. *CEIS Tor Vergata Research Paper Series* 6 (8): 128, 2008.

[350] See, on this point, the article by R. SAVIANO, in Corriere della Sera, Foreign section, 2 August 2021, available at: https://www.corriere.it/esteri/21_agosto_02/roberto-saviano-olanda-paradiso-narcos-f0668978-f2f8-11eb-9e5d-11e1603bb92c.shtml.

4.2 The offence of money laundering in the Dutch Criminal Code: a comparative analysis with Article 648 *bis* of the Italian Criminal Code.

Under Dutch criminal law, the punishability of the offence of money laundering is laid down in several provisions[351], which lend themselves to penalising different forms of money laundering.

Initially, as in the Italian legal system, money laundering was prosecuted based on provisions penalising the reuse of money and other assets for criminal purposes. However, under the influence of developments in the international landscape[352] and by virtue of a growing global awareness of the danger of the crime of money laundering, in the Dutch legal system towards the end of the 1990s the existing rules were no longer considered sufficient by the legislator for the repression of this phenomenon: thus, in 2001, the crime of money laundering was made an independent offence.

Regarding the *ratio legis* underlying the criminalisation of money laundering, as noted by authoritative doctrine[353], it is interesting to note that this can be enucleated in the '*heler-stelerregel'* rule, according to which the proceeds from the commission of a crime cannot be remedied in any way. Even if no such expression is known in the Italian legal system, which metaphorically summarizes the *ratio of* the provision, its applicability is deemed to be extended to it, as it is certainly also suitable for enucleating the *ratio legis of* Articles 648 *bis* and 648 *ter*.1 of the

[351] See Dutch Criminal Code, Articles 420-bis, 420-ter, 420-quater, introduced into Dutch law by an act dated 14 December 2001. In 2017, the provisions of Articles 420-bis.1 and 420-quater. 1 have been introduced in the Dutch Criminal Code. For these, see *below*.

[352] See Chapter 1, Sections 1.4 and 1.5

[353] L. MENDERA, *De reikwijdte van de witwasartikelen in het Wetboek van Strafrecht*, 2012, p. 8

Italian Criminal Code.

In general, according to Title XXXA of the Dutch Criminal Code, there is a prohibition of any act relating to property whose origin - direct or indirect - is the commission of a crime.

However, while the Italian Criminal Code regulates only one type of money laundering, the Dutch Criminal Code distinguishes as many as three categories of money laundering, which, unlike the Italian regulations, make explicit the subtle differences that may exist about the frequency with which the crime is committed, the context of the criminal acts and the subjective element.

The first of these is so-called 'intentional' money laundering, regulated in Article *420 bis* of the Dutch Criminal Code. According to this case, the money launderer is either aware of the illicit origin of the property from the outset or has become aware of it at a later stage, nevertheless continuing the laundering activity. In this case, the doctrine[354] speaks of 'premeditated intent' (*ingeblikt opzet*).

The express provision of intentionality appears to be similar to the provision in the Italian Criminal Code, which requires as a subjective element the generic intent, and therefore the will and representation to obstruct the criminal origin of money or goods.

In particular, *pursuant to* Article 420 *bis* of the Dutch Criminal Code, the criminalised conduct relates firstly to concealing or disguising the illicit origin of the property, its placement or transfer; concealing or disguising the identity of the owner of the property or its possessor; and lastly, again concealing or disguising the acquisition, possession, transfer or conversion and use of property of criminal origin. Like in the Italian legal system, in the Dutch legal system the offence of money

[354] MR. F. DIEPENMAAT, *op. cit.*

laundering is configured as a multi-offence activity, damaging a multiplicity of legal assets. Dutch literature, on this point, considers that the legislator - by making the offence of money laundering autonomous - has introduced a special instrument to protect the integrity of financial and economic traffic and, more generally, public order and the administration of justice[355].

According to the doctrine, of course, the mere production of proceeds through the exercise of a criminal activity is not sufficient, but the element of concealing the illicit origin of the proceeds of crime is required. Therefore, as considered in the national literature, an individual who immediately squanders the proceeds of crime without any attempt to conceal their origin or who reports to the authorities with his loot[356] cannot be considered punishable for money laundering. With regard to the object of the offence, attention must be paid to the provision under analysis, which distinguishes between concealment of the real nature, origin, location, disposal or transfer of an object and concealment of the identity of the owner or possessor of the object.

By means of this clarification, the provision in the Dutch Criminal Code is concerned in the first case with repressing all actions, directly related to the object itself, aimed at concealing its illicit origin; in the second case, the regulation is concerned with repressing those operations carried out by criminals to conceal transfers of ownership carried out specifically in order to conceal the illicit origin.

In the writer's opinion, this second part of the rule, which aims to directly counteract the concealment of the identity of those who engage in criminal conduct, with reference to money laundering through Bitcoin,

[355] For all, see L. MENDERA, *op. ult. cit*. pp. 10 and ff.

[356] P.C. VAN DUYNE & D. VAN DER LANDEN, *'De kennelijke' oorsprong van sneeuwwtije. De nieuwe witwaswet en het 'goede verhaal*', 1999.

as addressed in the previous chapter, could certainly be suitable to sanction *online* money laundering that uses all those *mixing* operations or recourse to anonymity services that enable the traceability of the flow of Bitcoin to be interrupted and prevent the identification of the real identity of the persons operating *online*.

The national doctrine[357] notes two important clarifications on dissimulative conduct. Firstly, total concealment of the illicit origin of the goods or money is not required: it is sufficient - as is the case in Italian law - for the conduct to be capable of concealing the traces of the criminal origin of the goods or money.

Secondly, it must be borne in mind how, in the interpretation of the offence under Article 420 *bis* of the Dutch Criminal Code, an objective assessment of the conduct of the laundering individuals is relevant. What is most relevant is whether the actions performed, in light of the circumstances of the specific case, create a de facto situation of concealment of the criminal origin of the assets or money. It is also interesting to note how concealment of the illicit origin coincides with the very justification of the laundering process. In fact, the carrying out of money laundering activities is generally considered to be the result of a rational choice[358], those who consciously choose to launder money, before starting the money laundering process, as a rule already know the necessary *ploys to* resort to and into which activity to put the apparently 'clean' money[359].

In the writer's opinion, the configuration of this conduct appears to be entirely comparable to the rules laid down in the Italian Criminal

[357] F. DIEPENMAAT, *De Nederlandse strafbaarstelling van witwassen, Een onderzoek naar de reikwijdte en de toepassing van artikel 420bis Sr*, 2016, p. 66 ff.

[358] See Chapter I, Section 1.1 of this paper.

[359] F. DIEPENMAAT, *op. cit.*

Code. The terminology used is, in fact, wide-ranging, being capable of encompassing a multiplicity of unlawful activities.

On this point, in fact, it is useful to bear in mind the Italian regulation, according to which - as seen *above* - the rule is aimed at repressing precisely any type of dissimulative conduct of criminal provenance, where the meaning of 'dissimulative conduct' must be understood as hostile conduct capable of dispersing the traces of the criminal provenance of the asset.

Proceeding with the current analysis, it is now worthwhile to look at the other types of money laundering that underlie the element of intentionality. This concerns so-called 'habitual' money laundering, which is currently the most serious[360] - and most severely punished - form of the offences under analysis. The provision states that '*anyone who commits money laundering shall be liable to a term of imprisonment not exceeding eight years or to a fifth-category fine. The same penalty applies to anyone who commits money laundering in the exercise of his profession or activity*'. This is therefore a more aggravated variant of intentional money laundering, whereby anyone who repeatedly or over a long period of time engages in money laundering is punished more severely.

Departing from the configuration of the provision just analysed is Article 420 *quater* of the Dutch Criminal Code, which proposes a novelty compared to the Italian Criminal Code: this provision in fact regulates the crime of 'culpable' money laundering.

This is specifically the form of money laundering penalised in the mildest form by the Dutch legislature, which has chosen to expressly

[360] J. RAYMAKERS, *ICLG, The International Comparative Legal Guide to: Anti-Money Laundering 2019, 2nd Edition, chapter 24 'Netherlands'*, 2019, p. 166

regulate the hypothesis that a person takes part in the offence of money laundering not being aware of the unlawfulness of his conduct, but having the means to reasonably become aware of it. More precisely, Article *420 quater* punishes '*anyone who conceals or disguises the true nature, origin, place of discovery, disposal or destination of money; the origin, place of discovery, disposal or disposal of an object; or conceals or disguises the person who holds title to the object or the person in possession of the object while he should reasonably suspect that the object originates - directly or indirectly - from a crime'*. The provision also penalises '*any person who acquires, possesses, disposes of or sells an object, or makes an object, or makes use of an object, while he should reasonably suspect that the object originates - directly or indirectly - from an offence*'. It should also be noted that since 2017, Dutch law has witnessed the introduction of two further provisions. Firstly, the Dutch legislator regulated a new form of money laundering, *pursuant to* articles *420 bis,* co. 1 and 420 *quater*, co. 1: 'simple' money laundering.

This provisions are both aimed at repressing the conduct of acquiring or possessing an object that comes immediately from any of the predicate offences committed by the same person, punishable by imprisonment of not more than six months or a fourth-category fine. It is mandatory to precise that both the intentional and culpable form are criminalized. These new offences fill the gap in criminalization that has developed in case law when someone launders proceed that come directly from their predicate offences by merely acquiring or possessing them.

These are variants that appears when the suspect should reasonably have suspected that the object came from a crime.

4.2.1 Some common discipline points.

It seems appropriate to briefly give some necessary clarifications in the analysis of the Dutch money laundering discipline[361].

It should also be noted that, according to Dutch case law, it is not necessary that the goods originate entirely from the commission of a crime: for example, a good purchased partly with money of illicit origin and for another part with money of lawful origin is in any case considered to be of criminal origin[362].

The literal expression "object" used in the Code means property of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and documents or legal instruments in any form, including electronic or digital, evidencing title to or an interest in such property and any right claimed in respect thereof. More precisely, pursuant to Art. *420 bis* the term "*Voorwerp", which* in Dutch means "object", is used literally, although this expression means all property and property rights[363].

As regards the category of predicate offences, as in the Italian legal system, it includes all offences that have produced the illegal proceeds. In other words, Dutch law does not have an exhaustive list of predicate offences, as it is an open category that includes all types of offences, as well as the tax offence[364].

---

[361] For these clarifications, the writer relied on the recent documentation prepared by FISCAL INFORMATION AND INVESTIGATION SERVICE OF THE NETHERLANDS, TAX AND CUSTOMS ADMINISTRATION, *Indirect Method of Proof. Providing Evidence in stand-alone money laundering investigations*, 15th April 2019.

[362] For all, J. RAYMAKERS, *op. cit*., p. 168

[363] In Dutch law, property rights are described in Art. 3:6 of the Dutch Civil Code. They constitute transferable rights either separately or together with another right, provide material benefits to the assignee or are obtained in exchange for material benefits received or promised.

[364] See Hoge Raad (Dutch Supreme Court), 7 October 2008, 03511/06, LJN: BD2774. According to the Supreme Court of the Netherlands, tax fraud must also be considered as money laundering, because if any person pays too little to the tax authorities the money evaded and used for transactions, purchases or any activity, it will always be illegitimate.

This jurisdictional approach has considerable advantages for the effectiveness of money laundering provisions. Firstly, it is not necessary to be able to prove, based on the available evidence, that the object in question derives from a precisely specified offence. *Secondly, it* is not necessary to prove by whom, at what time and place the offence was committed. To obtain a conviction, it is sufficient to establish that the object originated from any crime. This requirement is fulfilled because it cannot be otherwise that the object - directly or indirectly - originates from a crime[365].

In this respect, Dutch money laundering cases of the last decade have shown that it is possible to fairly convict money laundering suspects without proving a predicate offence. All that is needed is proof that the object does not come from a legal source[366].

The statute of limitations for the predicate offence does not affect criminal liability for money laundering, provided it falls within the period of prosecution for the money laundering offence. This also applies to items that originate from offences committed before the money laundering provisions came into force and that still exist.

It is then interesting to observe some notations concerning the notion of possession used by the Dutch Criminal Code. By this expression is meant an effective control over a good[367]; but on this point one should note an extensive orientation promoted by the Dutch Supreme Court (*Hoge Raad),* which wanted to impose certain restrictions with regard to the mere possession of an object derived from an offence committed by the suspect himself.

In particular, the Supreme Court ruled in a recent judgment[368] that the

[365] See *below for* details on the indirect method of proof.

[366] See *infra*, para. 4.2.1, in particular the reference to Judgment. ECHR, Zschüschen *v.* Belgium, 2 May 2017.

[367] L. MENDERA, *op. cit*.

[368] Hoge Raad, 26th October, 2010, LJN BM4440, NJ 2010, 655

mere possession of the offending property is not sufficient, but the presence of a volitional element is also necessary. In fact, alongside possession, there must be the will and representation on the part of the individual to derive an unlawful advantage.

It is also useful to ask whether self-laundering is also punishable under Dutch law. Whereas prior to 2017, a person could not be found guilty of money laundering by merely acquiring an object from his or her own crime, the so-called 'exclusion motive', with the entry into force of Articles 420a.1 and 420c.1, this type of money laundering is now punishable as 'simple' money laundering with a maximum sentence of six and three months' imprisonment.

4.2.2. The Indirect Test Method

To grasp this peculiarity of the Dutch system, it would seem useful to draw on a ruling of the Dutch Supreme Court from 2005: "*To obtain a conviction for money laundering it is necessary to prove that the object originates from any crime [...], it is not necessary to prove a specific predicate offence.*"

This quote from the Supreme Court can be regarded as the ultimate expression of the autonomy that characterizes money laundering investigations. The predicate offence does not have to be proven, it is sufficient to prove that the object 'comes from any offence'. This means that it will be sufficient to prove that an object does not come from a lawful source, which can then be inferred indirectly that it comes from an unlawful source.

This indirect method of evidence may be used in cases where there is no direct evidence of a predicate offence in relation to the object. This may be due to the absence of a paper trail between the offence and the

object; the data (facts and circumstances) on a predicate offence may have been lost at that time either due to the long period of time or due to the concealing and disguising nature of money laundering.

The indirect method of proof consists of excluding a legal source of origin and concluding that it cannot be anything other than that the object originates from any crime.

The exclusion of a legal source is based on a threefold logical-deductive reasoning. First, it must be ascertained that there is no direct connection between the object and the profit of a predicate offence; then a legal source of origin of the object must be excluded, the so-called exclusion method; finally, it must be established what type of relationship (e.g. recipient, owner, seller, user) exists between the object and the suspect.

The exclusion method follows the principle of '*follow the money*'. Thus, if from known legal sources, no visible connection to the object can be found (*forward tracking)* and, conversely, from the object the money trail is impossible to trace back to a legal source of origin (*backward tracking*), then the illicit origin of the proceeds can be deemed proven.

The European Court of Human Rights (ECHR) has also had occasion to pronounce on the indirect method of proof, to examine its compliance with the European Convention on Human Rights. On 2 May 2017, the ECHR ruled in a money laundering case in Belgium[369]. This ruling clarified some issues regarding the potential violation of the rights of suspects if an indirect method of proof is used in money laundering.

The Dutch man Zschüschen opened a bank account in Belgium in March 2003 and deposited a total amount of EUR 1,000,000. in 5 transactions within 2 months. Zschüschen had a record for drug

[369] ECHR, ZSCHÜSCHEN v. BELGIUM, 2 May 2017, 23572/07

trafficking and no declared income. Proceedings for money laundering were initiated in Belgium. He initially claimed that the money had been earned from untaxed work during a four-year period, not wanting to provide the names of the employers. Throughout the proceedings he claimed the right to remain silent. In 2006, Zschüschen was convicted in Belgium and first invoked Article 6, par. 1) and 2) ECHR, specifically invoking the violation of the right to a *'fair trial'*, the presumption of innocence and the right to remain silent.

According to Zschüschen, the fact that the predicate offence was not specified during the proceedings constitutes a violation of his rights of defence and a violation of his right to be informed of the charges in a timely manner.

However, according to the ECHR, Article 6 par. 1) and 2), Zschüschen gave a vague and unconvincing explanation on the origin of the money and did not want to answer further questions on the matter.

The Belgian court considered this refusal to explain the origin of the money in the conclusion that the money came from a crime.

According to the ECHR, this conclusion is in no way contrary to the European Convention on Human Rights, arguing that in this case the facts and circumstances were such that its silence only confirmed the evidence that already existed.

It was also considered that it would not have been difficult for Zschüschen to substantiate his statement on the origin of the money. The conclusions drawn from his refusal to provide a statement are not unfair or unreasonable but are dictated by common sense. The ECHR states that in line with Belgian law, the suspect was adequately informed of the charges against him, considering the clear and detailed description of the suspicious transactions and the legal explanation on money laundering. On this occasion, the ECHR states that Article 6 par. 3), (a) ECHR does not include the obligation to describe the specific predicate offence in

the charges. After all, the predicate offence by means of which the money was obtained is not the focus of the charges in the case of money laundering. In conclusion, it can therefore be said that this judgment confirms that the Dutch approach to money laundering cases, applying the graduated scheme, is not contrary to the ECHR.

4.3 The most popular money laundering techniques in the Netherlands.

According to a study conducted by the *School of Economics of* the University of Utrecht[370], a collaboration with the Dutch National Bank (DNB) - and specifically, with the *capital balance* department - has revealed the prevalence of some of the most common money laundering techniques in the Dutch economic-financial landscape.

Among these, the *report* first mentions minor banking transactions, i.e. less than EUR 10,000.

Also noteworthy is the spread of so-called *back-to-back loans,* i.e. the purchase of real estate in the Netherlands, being covered by a bank guarantee, usually consisting of money of illicit origin. Also among the most widespread techniques are currency exchange offices. These offices are also allegedly used for tax evasion purposes. In particular, it happens that coupons of securities issued abroad - e.g. bonds, shares and money certificates - mostly issued in Belgium and Luxembourg, would be exchanged at the Dutch border, where the offices would then cash the coupons.

The study, although very significant especially on a local level, is, however, not a recent edition and therefore deserves to be supplemented by a memorandum dated April 2020 from the Anti-Money Laundering

[370] University of Utrecht and Australian National University, '*The Amount and Effects of Money* Laundering', 2006.

Centre reporting to the Dutch government, which also provided some indications with regard to the purchase and sale of virtual currencies[371]. The *report,* referring to the provisions of the Financial Intelligence Unit of the Netherlands[372], provides that the main indicators of the conduct of money laundering activities are as follows: firstly, the fact that Dutch citizens have foreign money in bank accounts opened abroad in order to hide it from the Dutch authorities and/or investigative services; secondly, the authorities have pointed out that a method frequently used in exchange offices is the regular exchange of large sums of foreign currency, divided into small denominations, into euros. This type of activity is carried out by couriers or front men, sometimes accompanied by other persons - apparently those who supervise these transactions.

Those offering the money sometimes accept unusual and very unfavourable terms of exchange. This method particularly concerns the proceeds of drug trafficking. A more refined method involves the use of *off-shore* companies. The person offering the money claims to be acting on behalf of a company, often based abroad. He orders the money to be transferred to a bank account of that company, after which the money is immediately withdrawn from that account or further transferred to another account. The amounts that are transferred to these accounts are often inexplicably large compared to the type of business the front company was supposed to be conducting.

[371] Anti Money Laundering Centre, Money Laundering Indicators, April 2020. The *report in* question can be found at the following link in English: https://www.amlc.eu/wp-content/uploads/2020/05/witwasindicatoren-Engelse-versie.pdf

[372] https://www.fiu-nederland.nl/en/general-legislation/money-laundering-typologies

4.4 The Crime of Money Laundering and the Misuse of Virtual Currencies in Dutch *Case Law.*

Similar to the Italian legal system, Bitcoins in Dutch law[373] are not considered as currency, but as a medium of exchange[374].

Both doctrine[375] and case law devote considerable space to the laundering of Bitcoin. It occurs when Bitcoins of illicit origin, originating from any crime, are converted into electronic money or cash[376]. This last concluding paragraph, maintaining more than ever a comparative perspective that crosses national borders, in view of the fact that the phenomenon of virtual currencies has a global dimension and in the light of their widespread diffusion in state legal systems, seeks to give practical expression to what has been considered on a theoretical level in this paper, by proposing a brief review of the most recent case law produced in the Netherlands.

The first case involving the Rotterdam Court[377] concerns the use of cryptocurrencies - and in this case, bitcoins - for money laundering purposes. The adjudicating body bases its decision on what in Italian law might constitute a maxim of experience, stating that 'it is now a well-known fact that bitcoins are often used in criminal contexts, including drug trafficking'[378].

---

[373] Anti Money Laundering Centre, *The bitcoin trader - a facilitating role in the cash out of criminal proceeds*, August 2017.

[374] District Court Overijssel 14 May 2014, ECLI:NL:RBOVE:2014:2667. The Dutch court ruled that the 'wallet' in which bitcoins are stored does not differ much from a normal bank account. However, the bitcoin wallet is not managed by a bank, for instance, but by the owner himself, and therefore cannot be considered as a currency or scriptural fund.

[375] For further reading, W.M. WARNAARS, *Witwassen van bitcoins. De omgekeerde bewijlast bij het witwassen van bitcoins in het licht van de onschuldpresumptie*, 2019.

[376] A ruling of the District Court of the Netherlands, Rb. Midden-Nederland, 24 januari 2018, ECLI:NL:RBMNE:2018:234. In the case at hand, the suspect traded drugs via the *dark web* and the remuneration received for the drugs was in Bitcoins, which were then exchanged for legal tender, in the amount of EUR 500,000.

[377] ECLI:NL:RBROT:2019:2408

[378] ECLI:NL:RBROT:2019:2408, where it states in paragraph 4.1: '*Het is een feit van algemene bekendheid dat bitcoins dikwijls worden gebruikt in het criminele circuit, onder meer in de drugshandel*'.

In the case in question, the suspect had received in 2015 an amount of EUR 1,027,905, 66 in Bitcoin, in exchange for the crack drug, receiving on a multiplicity of current accounts opened by the subject at different banks, *tranches* of fixed sums of short amounts - EUR 8,999.91 - for each transaction.

In light of the consideration that the receipt of these sums was not related to the subject's wage earnings from work and that they were mainly paid directly by the subject in the form of cash without any apparent need to account for the payments, the Court stated that it considered it highly probable that these sums of money derived from other activities that were not of an illicit nature[379].

In the sentence, the individual was found guilty of habitual money laundering, pursuant to Article 420 *ter* of the Dutch Criminal Code, and is likened to a *money mule, in* that after the sums were credited to his bank accounts, they were transferred to the bank accounts of his relatives and then withdrawn in cash.

At the end of the judgment is a clear statement by the Court that "*money laundering is a serious matter that damages the integrity of financial trade and the confidence that must be placed in it.* "[380]

The second case under analysis concerns the conviction by the District Court of the Netherlands, in the Utrecht Office, of two men, one from Utrecht, the other from Amsterdam, for drug trafficking and money laundering of Bitcoin between 2014 and 2015[381]. The convicts had shipped large quantities of hard drugs to various foreign countries, such

[379] ECLI:NL:RBROT:2019:2408, where it states in paragraph 4.1: '*Galet op het ontbreken van een aannemelijke verklaring voor een legale herkomst van voormelde geldbedragen is de rechtbank van oordeel dat het niet anders kan dan deze geldbedragen onmiddellijk of middellijk uit enig misdrijf afkomstig zijn en dat de verdachte dit heeft geweten*'

[380] ECLI:NL:RBROT:2019:2408, where it states in paragraph 7: "*Witwassen is een ernstig feit dat de integriteit van het financiële handelsverkeer schaadt en het vertrouwen dat daarin moet worden gesteld."*

[381] ECLI:NL:RBMNE:2017:5713

as France, the UK, Spain and Japan. The hard drugs had been sold on the *darknet in* exchange for bitcoins and the criminal origin of these had been disguised through a *mixing* service, called Bitcoin Fog. With this *mixing* system the bitcoins received were remixed and redistributed. In its ruling, on the basis of the evidence brought to trial by the Public Prosecutor, the Court establishes a principle of general application, corroborated by scientific research attached by the defence. In particular, it states that '*It follows from the above-mentioned expert statement (...) that research has shown that illegal goods are traded almost exclusively on darknet markets and that payment in bitcoin is required in such markets. Based on this statement, the court assumes that almost all bitcoins from darknet markets have a criminal origin*".[382]

Lastly, given the notoriety of the incident, although not related to the use of cryptocurrencies, the case that affected one of the largest Dutch banks deserves mention. This is the case that hit ING Bank, which was forced to pay a fine of EUR 775 million in 2018, after the Dutch authorities discovered its non-compliance with anti-money laundering regulations from 2010 to 2016[383]. The Bank was charged with culpable money laundering, for failing to prevent many bank accounts from being used for money laundering purposes.

Specifically, the Bank allegedly failed to perform *due diligence* and report suspicious transactions. As a result of these operational failures, the Bank's customers allegedly used their accounts undisturbed for illicit activities.

---

[382] ECLI:NL:RBMNE:2017:5713, where it states in paragraph 4.3.1 that: "*Uit de hiervoor genoemde verklaring van de deskundige (...) volgt dat uit on derzoek is gebleken dat op darknet markets vrijwel uitsluitend in illegal goederen wordt gehandeld en op die markets een betaling in bitcoins is vereist".*

[383] See the note published on the website of the Public Prosecution Service, Netherlands, available at: https://www.prosecutionservice.nl/latest/news/2018/09/04/ing-pays-775-million-due-to-serious-shortcomings-in-money-laundering-prevention

For example, an international telecommunications provider transferred bribes amounting to tens of millions of dollars through its bank accounts with the Dutch bank ING to a company that was owned by the daughter of the then president of Uzbekistan. ING reported the unusual transactions to the FIU too late. Moreover, ING did not sufficiently investigate the identity of the actual owner of the company.

4.5 Concluding remarks: the current *file rouge* between the Italian and Dutch legal systems.

In the light of the above considerations, it can certainly be concluded that, in general, the same repressive structure of the offence of money laundering can be found in Dutch law. Certainly, as we have attempted to point out, there remain certain differences which - in the opinion of the writer - attribute to the Dutch legislator greater attention and specificity in the configuration of the offence under analysis. On the other hand, however, it cannot be overlooked that also the Italian *littera legis* is in any case capable of covering countless money laundering hypotheses, thanks to its wide-ranging wording.

Referring back to one of the questions addressed in this paper, i.e. the subsumability of money laundering through cryptocurrencies in the existing provisions that penalise traditional money laundering, it therefore seems unquestionable that the phenomenon in question can be included in the various types of money laundering known in the Dutch legal system. Since the subject of cryptocurrencies in the Netherlands also still lacks an effective regulation, as far as its criminal relevance is concerned, *de iure condendo*, also for the Dutch legislator - as for the Italian one - an intervention could be hoped for that would give greater prominence to the use of new technologies for money laundering purposes.

Some might argue for an aggravation of the legislation in question, probably incurring in an excess of protection and normative production. To the writer, however, notwithstanding the deducible subsumption of the phenomenon in existing cases, it seems preferable to take the path of an express regulation on the subject, which would place certain constraints free from any interpretative weaknesses that could increase doubts and open questions on the subject.

OSSERVAZIONI CONCLUSIVE

L'analisi condotta nel presente elaborato ha consentito lo svolgimento di una esegesi dei profili più attuali del delitto di riciclaggio, così come disciplinato dal Legislatore domestico *ex* art. 648 *bis* c.p., alla luce del crescente utilizzo, nelle transazioni *online*, delle criptovalute. Infatti, come pacificamente emerso dall'approfondimento sin qui svolto sul possibile utilizzo delle stesse a fini di ripulitura del denaro, attualmente esse si configurano da un lato come pregevole frutto dell'evoluzione tecnologica con elevate potenzialità senz'altro vantaggiose per lo sviluppo dei mercati, dall'altro risultano puntellate però da molteplici ambiguità le quali, ove abilmente sfruttate da individui criminali, ne consentono agevolmente un impiego illecito.

In primo luogo, prendendo avvio da un'analisi del delitto di riciclaggio nell'ordinamento italiano, è emerso che le condotte espressamente sanzionate dal Legislatore domestico risultano di ampia formulazione. Vengono, infatti, sanzionate le condotte di sostituzione, trasferimento e compimento di altre operazioni in modo da ostacolare l'individuazione della provenienza illecita dei beni o di altre utilità che provengano dalla realizzazione del delitto presupposto. La dicitura di così ampio respiro apre senz'altro vaste possibilità interpretative le quali, volgendo lo sguardo al vertiginoso aumento di nuove condotte criminose realizzate nel *web*, hanno permesso di sussumere, in via generale, tali nuovi fenomeni emergenti all'interno della fattispecie *ex* art. 648 *bis* c.p., seppur necessitando di alcune accortezze interpretative e, in prospettiva di riforma, di disciplina.

Nello specifico, si parta dalla ineludibile premessa secondo la quale è proprio leggendo il delitto di riciclaggio attraverso la lente della categoria dei *cybercrimes*, che è risultata di non trascurabile interesse

un'analisi più approfondita del fenomeno del *cyberlaundering*. Trattasi, nello specifico, della più corretta nomenclatura idonea a ricomprendere tutte quelle ipotesi in cui il reato di riciclaggio sia realizzato *online.* Dall'analisi condotta, è emerso che risulta notevolmente diffuso il ricorso ad alcune tecniche di riciclaggio, ad esempio attraverso il *gambling* e l'*online banking*, le quali, comportano lo sfruttamento della difficoltà ad essere rintracciati o le capacità degli *hacker* più esperti di rubare dati personali e muovere – anche ingenti – somme di denaro *online* per poi reinvestirle in attività apparentemente lecite. Generalmente, può dirsi che tali attività siano rese possibili in particolare ricorrendo alla dimensione "oscura" di Internet, conosciuta con il nome di *deep web*. In questa dimensione, grazie allo sfruttamento di *software* che garantiscono di operare *online* in una condizione di anonimato, la forza attrattiva del *web* per i criminali cresce in via esponenziale. Se, da un lato, come prima si accennava, il percorso argomentativo strutturato nel presente elaborato ha permesso di rispondere positivamente al quesito sulla possibile sussumibilità di tale fenomeno nella fattispecie *ex* art. 648 *bis* c.p. e 648 *ter*.1 c.p., d'altro canto si ritiene necessario che il Legislatore provveda più nello specifico, in una prospettiva sanzionatoria, a disciplinare il fenomeno del *cyberlaundering*. Infatti, constatata la non stretta necessità della configurazione di una fattispecie autonoma, si riterrebbe tuttavia ottimale, in una prospettiva *de iure condendo*, che il Legislatore prevedesse una circostanza aggravante alle disposizioni penali già esistenti, volta a sanzionare qualsiasi condotta di riciclaggio realizzata *online*. In questo modo, si eviterebbe senz'altro un inutile appesantimento della produzione legislativa e si interverrebbe indubbiamente in maniera più mirata, circoscritta ed efficace.

Nell'approfondire il fenomeno del *cyberlaundering*, a chi scrive è parso opportuno dedicare attenzione ad una tra le tecniche di riciclaggio *online* che sta maggiormente preoccupando le principali Autorità di

Vigilanza e di controllo, sia a livello interno che sovranazionale. Essa si sostanzia nell'utilizzo delle valute virtuali al fine di movimentare e reinvestire denaro di provenienza illecita. Tali strumenti, dalla natura giuridica ancora incerta e foriera di accesi dibattiti nel mondo dottrinale, stanno attualmente impegnando i vertici degli Organismi di Vigilanza, i quali si sono più volte espressi con molteplici avvertenze nei confronti di investitori, operatori di mercato e, più in generale, di tutti i consumatori, che vogliano intraprendere operazioni tramite criptovalute. I rischi intrinseci alla loro natura sono numerosi e possono essere così brevemente sintetizzati: in primo luogo, le criptovalute non sono regolate da un ente centrale *super partes*; pertanto, manca a monte un soggetto terzo che ne controlli l'emissione e la circolazione. *In secundis*, non potendo essere detenute fisicamente, ma solo in via virtuale, esse ostacolano l'identificazione di coloro che operano con le stesse, garantendo la c.d. pseudonimità. Sono inoltre soggette ad un alto tasso di volatilità, soprattutto a causa dell'assenza di parametri di calcolo idonei a prevedere le modalità di formazione dei prezzi. Si aggiunga anche che le operazioni in criptovalute permettono di operare tra Stati diversi, scavalcando le barriere giurisdizionali di ciascuno e rendendo le operazioni compiute difficilmente rintracciabili.

Condivisa l'opinione secondo la quale le criptovalute siano riconducibili nella categoria degli strumenti finanziari, alla luce di queste loro caratteristiche appena elencate, può affermarsi che esse presentino dei tratti tipici che le rendono degli strumenti finanziari *sui generis*, sulla cui regolazione e disciplina si vede necessaria una ferma presa di posizione da parte del Legislatore. Per quanto riguarda i profili penali, in particolare, si tenga conto che con il suo ultimo intervento in materia, il Legislatore italiano, peccando di carenza di zelo, nel dare attuazione alla Direttiva (UE) 2018/1673 sulla lotta al riciclaggio tramite il diritto penale, con il d.lgs. 195/2021 non ha espressamente previsto che oggetto

del reato di riciclaggio e autoriciclaggio possano essere anche le criptovalute. Si ritiene che tale previsione sarebbe stata senz'altro necessaria per raggiungere una maggiore chiarezza, perché se da un lato le valute virtuali possono essere ricomprese nell'ampia formulazione di "altre utilità" presente nella fattispecie di riciclaggio, dall'altro lato una loro manifesta menzione all'interno della normativa domestica avrebbe fugato qualsiasi dubbio esegetico sul punto, che ad oggi arrovella dottrina e giurisprudenza

Abbracciando poi un'ottica di tipo preventivo, non deve, tuttavia, trascurarsi come il Legislatore eurounitario abbia comunque perseguito, con molteplici interventi, tentativi regolatori volti a rinforzare la normativa antiriciclaggio a livello europeo, incoraggiando la creazione di un ecosistema legislativo armonico per tutto l'ordinamento dell'Unione Europea. Tali interventi si sono concretizzati in cinque direttive antiriciclaggio, emanate tra il 1991 e il 2018, le quali hanno sostanzialmente incrementato obblighi di verifica e controllo, in capo a determinati soggetti, tra cui banche ed enti creditizi, nei confronti della clientela intenzionata ad operare con un determinato ammontare di denaro. Di particolare interesse è risultata senz'altro la più recente Quinta Direttiva antiriciclaggio, che è intervenuta estendendo il novero dei soggetti obbligati a conformarsi agli obblighi antiriciclaggio, i quali – ad oggi – ricomprendono anche i prestatori di servizi di cambio valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale. Non si trascuri, inoltre, che tale Direttiva, recepita internamente con il d. lgs. 125/2019, ha avuto senz'altro il pregio di aver introdotto nel nostro ordinamento una definizione di valuta virtuale. Può, pertanto, affermarsi che la sensibilità delle istituzioni sovranazionali volta a contrastare il fenomeno riciclatorio, anche attraverso l'utilizzo delle valute virtuali, sia costantemente aumentata negli anni con parziale attuazione anche sul piano nazionale.

Tuttavia, a fronte di tale presa di consapevolezza da parte dei Legislatori eurounitario e domestico, seppure si possa ritenere sussumibile il "cripto-riciclaggio" nella fattispecie ex artt. 648 *bis* c.p. e 648 *ter.*1 c.p., è emersa d'altronde la necessità di interventi ulteriori. In primo luogo, è auspicabile che il Legislatore eurounitario incrementi il livello di coordinamento tra Stati nella disciplina del cripto-riciclaggio, essendo ormai cristallini i pregi ma, al contempo, non fraintendibili le ambiguità che l'utilizzo delle criptovalute comporta all'interno dei mercati e degli ordinamenti statali. Sul piano interno, invece, il Legislatore domestico potrebbe intervenire imponendo sanzioni più severe qualora l'attività di riciclaggio avvenga utilizzando criptovalute. Si tenga presente, infatti, che, come dimostrato anche dalla casistica giurisprudenziale più recente, le operazioni in cripto sono di norma volte a movimentare ingenti somme di denaro e, dunque, sono connotate da un elevato grado di offensività per l'integrità dei mercati e degli ordinamenti economici.

Per concludere, una ulteriore prospettiva di analisi valorizzata nel presente elaborato è stata delineata grazie all'approfondimento svolto sul delitto di riciclaggio così come disciplinato nell'ordinamento olandese. Dallo studio svolto, è emerso che la disciplina contenuta nel Codice penale olandese mantiene lo stesso stampo di quella italiana, ma si presta a regolare una pluralità di fattispecie di riciclaggio, ciascuna notevolmente più dettagliata rispetto all'unica previsione presente nell'ordinamento italiano. Tra queste, ad esempio, deve menzionarsi, non solo un'elencazione più accurata di tutte le condotte considerate dal Legislatore olandese, ma anche l'espressa previsione che sanziona il delitto di riciclaggio colposo. Si noti infatti, la differenza con l'ordinamento italiano, ove l'elemento soggettivo contemplato è solamente il dolo.

In una prospettiva *de iure condendo* di riforma del delitto di

riciclaggio e di implementazione del sistema sanzionatorio, il Legislatore italiano potrebbe senz'altro ispirarsi alla normativa olandese, privilegiando il grado di specificità ivi riscontrabile. In tema di "cripto-riciclaggio", invece, i due ordinamenti paiono, attualmente, correre alla stessa velocità: entrambi i Legislatori non si sono spinti a fornire alcun tipo di regolamentazione omogenea, probabilmente in attesa di una più ferma presa di posizione da parte del Legislatore europeo. Pertanto, si auspica che quest'ultimo non rimanga mero spettatore di un'evoluzione tanto repentina quanto rischiosa per l'integrità di tutti gli ordinamenti statali eurounitari e dei loro mercati, ma che agisca da vero *deus ex machina* portatore di ordine e chiarezza nell'attuale confusionario e frammentato ecosistema delle criptovalute, con il quale il diritto penale tenta debolmente di dialogare.

BIBLIOGRAFIA

AMATO M., FANTACCI L., *Per un pugno di Bitcoin. Rischi e opportunità delle monete virtuali*, Milano, 2018

AMEDEO, A., BAGELLA M., BUSATO F., *Money laundering in a two sector model: Using theory for measuremenT. CEIS Tor Vergata Research Paper Series* 6 (8): 128, 2008

ACCINNI G. P., *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017*), in Archivio Penale, 2018, n. 1, p. 1

ACQUAROLI R., *Il riciclaggio*, in *Trattato teorico-pratico di diritto penale*, vol. VII, PALAZZO, PALIERO (diretto da), Torino, 2015

AGENZIA DELLE ENTRATE, *Trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali*, 2016

ALCINI J., "*Mondi paralleli, bitcoin e reati virtuali",* in *La giustizia penale*, 2, 2018, p. 438

ANGELINI M., *Il reato di riciclaggio (art. 648 bis c.p.). Aspetti dogmatici e problemi applicativi*, Torino, 2008

ANTI MONEY LAUNDERING CENTRE, *The bitcoin trader – a facilitating role in the cash out of criminal proceeds*, August 2017

ANTOLISEI F., *Manuale di diritto penale. Parte speciale*, Torino, 2016

ARNONE M., S. GIAVAZZI, *Riciclaggio e imprese*. *Il contrasto alla circolazione dei proventi illeciti*, Milano, 2011

ASPEN PUBLISHERS, *Liberty reserve founder pleads guilty to laundering more than $250m*, in *The computer & Internet lawyer*, 2016-05-01, Vol.33

ASSEMBLEA GENERALE ONU, Risoluzione 75/282, "*Lotta all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali*", 26 maggio 2021

BALENA G., *Il web nascosto: i segreti della rete e del deerk web: deep web, dark web e criptovalute*, 2020

BALDUZZI M., *Cybercrime in the Deep Web*, Amsterdam, 2015

BALSAMO A. E MATTARELLA A., *Criminalità organizzata: le nuove prospettive della normativa europea*, in Sistema Penale, 3/2021, p. 35

BANCA D'ITALIA, Quaderni di Ricerca Giuridica, *Lineamenti della disciplina internazionale di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo*, n. 69, (a cura di) M. Condemi e F. De Pasquale, 2008

BANCA D'ITALIA, sez. II, *Comunicazione sulle valute virtuali*, 30 gennaio 2015, in Bollettino di Vigilanza n. 1/2015.

BANCA D'ITALIA, *Le funzioni della moneta e le proposte di "moneta fiscale",* 2017

BANCA D'ITALIA E CONSOB, *Comunicato Stampa, CONSOB e Banca d'Italia mettono in guardia contro i rischi insiti nelle cripto-attività*, 18 aprile 2021

BARTOLI R., PELISSERO M., SEMINARA S., *Diritto penale. Lineamenti di parte speciale,* Torino, 2021

BCE, in *Virtual currency schemes*. *A further analysis,* 2015

BECKER G.S., *"Crime and Punishement: an economical approach*", in *Essays in the Economics of Crime and Punishment*, Chicago, 1974, p. 1

BIONDI F. A., *How Block- chain technology and its regulation could promote the Capital Markets Union: focus on ICO*, 2019

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 (II), fasc. 1, 2017, p. 27

BRAGA R. R. P., LUNA A. A. B., *Dark Web and Bitcoin: an anaylsis of the impact of digital anonymate and cryptocurrencies in the practice of money laundering crime*, in *Direito e Desenvolvimento*, 2018

CADOPPI A., *Elementi di diritto penale – Parte generale*, Padova, 2021

CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Trattato di diritto penale, parte speciale*, vol. X, *I delitti contro il patrimonio*, Padova, 2011

CALZONE O., *Servizi di mixing e Monero*, in Gnosis, 2017, p. 1

CAMPBELL-VERDUYN M., *Bitcoin and beyond: cryptocurrencies, blockchains and global governance*, 2018

CAPACCIOLI S., *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015

CAPPA E. E CERQUA L.D. *(a cura di), Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*, Milano, 2012

CARRER S., *Lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti: emanata la direttiva (UE) 2019/71*3, in Giurisprudenza Penale Web, 2019, p.7

CASSANO G., DI CIOMMO F., RUBINO DE RITIS M., *Banche, Intermediari e Fintech. Nuovi strumenti digitali in ambito finanziario,* 2021

CASTALDO A.R., NADDEO M., *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio,* Padova, 2010

CIAN M., SANDEI C., *Diritto del Fintech*, Padova, 2020

CIANCAGLINI V., *Below the Surface: Exploring the Deep Web,* 2015.

CIRAULO A., voce *Autoriciclaggio*, in *Digesto disc. pen*., IX agg., 2016, p. 122

COCCO G., *Il cd. Autoriciclaggio – art. 648-ter1*, in COCCO G. (a cura di), *Trattato breve di diritto penale. Parte speciale. Vol. II: I reati contro i beni economici*, Padova, 2015

COX D., *Handbook of Anti-Money Laundering*, Cornwall, 2014

COMMISSIONE PARLAMENTARE DI INCHIESTA SUL FENOMENO DELLE MAFIE E SULLE ALTRE ASSOCIAZIONI CRIMINALI, ANCHE STRANIERE, *Relazione sulle infiltrazioni mafiose e criminali nel gioco lecito e illecito*, 2017

CONSOB, Deliberazione n. 19866, *Sospensione, ai sensi dell'art. 101, comma 4, lett. b), del D.lgs. n. 58/1998, dell'attività pubblicitaria effettuata*

tramite il sito internet www.coinspace1.com relativa all'offerta al pubblico promossa dalla Coinspace Ltd. avente ad oggetto "pacchetti di estrazione di criptovalute", 1° febbraio 2017

CONSULICH F., *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*, in Diritto penale e processo 2/2022, p. 153

CORAPI E., LENER R. (a cura di), *I diversi settori del Fintech*, Padova, 2019

CROCE M.., *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy,* in Sistema Penale 4/2021, p. 127

CUZZOCREA L., *La ricostruzione del* paper trail *nelle indagini penali,* in (a cura di) M. ARNONE-S. GIAVAZZI, *Riciclaggio e imprese*. *Il contrasto alla circolazione dei proventi illeciti*, Milano, 2011

D'AGOSTINO L., *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio abusivo di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, in *Rivista di Diritto Bancario*, n.5, 2018, p. 1

DA ROLD M., *Innovazione tecnologica ed implicazioni penalistiche. Le monete virtuali*., in Giurisprudenza Penale Web, 2, 2019, p. 1

DALIA A. A., *L'attentato agli impianti e il delitto di riciclaggio,* Milano*,* 1982

DEMURO G.P.*, Il bene giuridico proprio quale contenuto dei reati a soggettività ristretta*, in Riv. it. dir. e proc. pen., 1998, p. 845

DELL'OSSO A. M.*, Il reato di autoriciclaggio: la politica criminale cede il passo a esigenze mediatiche e investigative,* in *Riv. it. dir. proc. pen.,* 2015, p. 796

DELL'OSSO A.M., *Riciclaggio di proventi illeciti e sistema penale*, Torino, 2017

DE STASIO V., *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca, borsa, tit. cred.*, 2018, I, p. 131

DIEPENMAAT F., *De Nederlandse strafbaarstelling van witwassen, Een onderzoek naar de reikwijdte en de toepassing van artikel 420bis Sr*, 2016

DI PAOLO E., *Cyber crime. Il Phishing: prospettive di un delitto*, in Archivio penale Web, 2017, n.2, p. 1

DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti, in Dir. pen. contemp*., 10/2018, p. 21

DI VIZIO F., *Gli obblighi antiriciclaggio per operatori in valute virtuali*, in Discrimen.it, 2019, p. 1

EUROPEAN BANKING AUTHORITY, *Virtual Currency Schemes,* 2012

EUROPEAN BANKING AUTHORITY, *Opinion on virtual currencie*s, 2014

EUROPOL, *Public Awareness and Prevention Guides*, 2019

EUROPOL-EUROJUST, *Common challenges in combating cybercrime*, June 2019

EUROPOL, *European Union Serious and Organised Crime Threat Assessment 2021 - A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime*, 2021

EUROPOL Spotlight, *Cryptocurrencies: tracing the evolution of criminal finances*, 2022

FAIELLA S., *Riciclaggio e crimine organizzato transnazionale,* Milano, 2009

FATF, Raccomandazione 3, 2012

FATF, *Virtual currencies: key definition and potential AML/CFT Risks*, 2014

FATF, *Mutual Evaluation Report, Anti-Money Laundering and Combating the Financing of Terrorism*, THE NETHERLANDS, 25th February 2011

FAVA S., *Il reato di riciclaggio* (intervento al seminario *Criminalità economica, economia criminale,* Roma, 27-28 maggio 2011) in *Quest. Giust.*, 2012, p. 4

FIANDACA G., MUSCO E., *Diritto penale. Parte speciale*, 2015

FILIPKOWSKI W., *Cyberlaundering: An Analysis of Typology and Techniques*, in *International Journal of Criminal Justice Sciences*, vol. 3, 2008, p. 15

FISCAL INFORMATION AND INVESTIGATION SERVICE OF THE NETHERLANDS, TAX AND CUSTOMS ADMINISTRATION, *Indirect Method of Proof. Providing Evidence in stand-alone money laundering investigations*, 15th April 2019

FLOR R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in Riv. it. dir. proc. pen., 2007, n. 1-3, p. 899

FLOR R., *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di internet*, in Diritto Penale Contemporaneo, 2010, p. 1

FLOR R., *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in (a cura di) A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *op. ult. cit.,* 2019, p. 141

FORTE G., *L'elemento soggettivo nel riciclaggio*, in MANNA A. (a cura di), *Riciclaggio e reati connessi all'intermediazione mobiliare,* Padova, 2000

FOURMAN M., *Informatics*, 2002

FRANZA E., *Le valute virtuali e prodotti finanziari con sottostanti valute virtuali. Una prima indagine sugli interventi*, in *Foroeuropa*, 2018, p. 20

GAFI, *Macroeconomic Implication of Money Laundering*, giugno 1996

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, fasc. 3, 2015, p. 415

GIRINO E., *Criptovalute: un problema di legalità funzionante*, in *Rivista di Diritto Bancario*, fasc. IV, 2018, p. 733

GRANDI C. (a cura di), *I volti attuali del diritto penale europeo*, Pisa, 2021.

GULLO A., *Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato*, in Dir. Pen. Contemp., 2018, p. 262

HOUBEN R., SNYERS A., *Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering and tax evasion,* Study requested by the TAX3 committee of the EU Parliament, July 2018

HUNT J., *The new frontier of money laundering: How terrorist organisations use cyberlaundering to fund their activities, and how governments are trying to stop them. Information and Communications Technology Law* 20, 2011

IMF BOARD EXECUTIVE BOARD PAPER, "*Integrating Stability Assessments Under the Financial Sector Assessment Program into Article IV Surveillance*" and "*Background Material*", August 2010

JONES J., *Tor: accessing the deep web and dark web with Tor. How to set up Tor, stay anonymous onlune, avoid NSA spying and access the deep web and dark web*, 2017

LAGI V.*, Deep web, dark web e indagini informatiche*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime,* Padova, 2019

LESLIE D. A., *Legal Principles for Combatting Cyberlaundering, Law, Governance and Technology Series*, London, 2014

LONGOBARDO C., *Riciclaggio (art. 648-bis c.p)*, in *I reati contro il patrimonio,* (a cura di) FIORE S.*,* Padova, 2010

MAGRI P., *I delitti contro il patrimonio mediante frode,* in *Trattato di diritto penale. Parte speciale*, (diretto da) G. MARINUCCI, E. DOLCINI, vol. VII, tomo 2, Padova, 2007

MAIELLO V., *Il riciclaggio: fenomenologia ed evoluzione della fattispecie normativa, sez. I, Il fenomeno criminale* in L. DELLA RAGIONE; V. MAIELLO (a cura di) *Riciclaggio e reati nella gestione dei flussi di denaro sporco, aggiornato al d.lgs. n. 90/2017*, Milano, 2018

MAJORANA D., *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in Corriere Tributario, 8, 2018, p. 630

MANNA A., *Il bene giuridico tutelato nei delitti di riciclaggio e reimpiego: dal patrimonio all'amministrazione della giustizia, sino all'ordine pubblico e all'ordine economico*, in AA. VV. *Riciclaggio e reati connessi all'intermediazione finanziaria*, (a cura di) A. MANNA, Padova, 1999

MANTOVANI F., *Diritto penale – parte speciale*, *Delitti contro il patrimonio*, Vol. II, Padova 2021

MARINUCCI G., DOLCINI E.*, Codice penale commentato*, Milano, 2021

MARK N., *Designing the Total Area Network: Intranets, VPN's, and Enterprise Networks Explained.,* 2000

MASCIANDARO D., "*Economia del riciclaggio e della politica antiriciclaggio*", in Giornale degli Economisti ed Annali di Economia, 1995

MASCIANDARO D., *Riciclaggio dei capitali illeciti: profili di analisi economica*, in E. CAPPA E L.D. CERQUA (a cura di), *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*., Milano, 2012

MATTARELLA A., *La Convenzione di Palermo: il futuro della lotta alla criminalità organizzata transnazionale,* Torino*, 2020*

MATTARELLA A., *La futura convenzione ONU sul Cybercrime e il contrasto alle nuove forme di criminalità informatica*, in Sistema Penale, Fasc. 3/2022, p. 41

MAURUSHAT A., HALPIN D., *Investigation of Cryptocurrency Enabled and Dependent Crimes*, 2022

MCCLEAN D., *Transnational Organized Crime. A Commentary on the UN Convention and its Protocols*, 2007

MENDERA L., *De reikwijdte van de witwasartikelen in het Wetboek van Strafrecht*, 2012

MEZZETTI E., *Reati contro il patrimonio,* in *Trattato di diritto penale, Parte speciale,* GROSSO C. F., PADOVANI T., PAGLIARO (diretto da), Milano, 2013

MOCCIA S., *Impiego di capitali illeciti e riciclaggio: la risposta del sistema penale italiano*, in *Riv. it. dir. proc. pen*., 1995, p. 375

MORABITO M.A.*, Lo schema di decreto legislativo per l'attuazione della direttiva UE 2018/1673 sulla lotta al riciclaggio mediante il diritto penale: analisi e considerazioni*, in Giurisprudenza penale Web, 2021, p. 9

MUCCIARELLI F., PICOTTI L., RINALDI G., UGOCCIONI, *Commentario alla l. 1° dicembre 1993 contro la criminalità informatica*, in *Legislazione penale*, 1 e 2, 1996.

MUCCIARELLI F., *Qualche nota sul delitto di autoriciclaggio*, in *Diritto Penale Contemporaneo*, 1/2015, p. 108

NADDEO M., *Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale*, in Diritto penale e processo, fasc. 1/2019, p. 150

NAKAMOTO S., *Bitcoin*: *A peer-to-peer electronic cash system*, 2008

NATARAJAN H., KRAUSE S., GRADSTEIN H., "*Distributed Ledger Technology (DLT) and blockchain*", 2017

PALIERO C.E., *Criminalità economica e criminalità organizzata: due paradigmi a confronto,* in M. BARILLARO (a cura di), *Criminalità organizzata e sfruttamento delle risorse territoriali*, Milano, 2004

PARBONETTI A., *Caratteristiche e modalità di gestione delle aziende criminali*, in R. Borsari (a cura di), *Itinerari di diritto penale dell'economia*, Padova, 2017

PARODI C., LOMBARDO S., GHIRARDI L., *Riciclaggio e aggiotaggio telematicco*, in C. PARODI, V. SELLAROLI (a cura di), *Diritto penale dell'informatica: reati della rete e sulla rete*, Milano, 2020

PASSERELLI N., *Bitcoin e antiriciclaggio*, in *Gnosis*, Rivista italiana di intelligence, 2016, p. 1

PASSERETTA M., *Bitcoin: il leading case italiano*, in Banca Borsa Titoli di credito, fasc. 4, 2014, p. 471

PATALANO R., *Riciclaggio e flussi finanziari illeciti nel capitalismo contemporaneo*, in *economiaepolitica, Riv. online della politica economica, 10 marzo 2022

PECORELLA G., *Circolazione del denaro e riciclaggio*, in *Riv. It. Dir. e Proc. Pen*., 1991, p. 1221

PERRI P.; ZICCARDI G., *Dizionario Legal tech*, Milano, 2020

PESTELLI G., *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 12/2021, p. 49

PETERS G. W., "*Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective*", 2015

PICOTTI L., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in L. PICOTTI (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013

PICOTTI L., *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in Riv. Trim. Dir. pen. dell'economia, 3-4, 2018, p. 590

PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (DIRETTO DA), *Cybercrime*, Padova, 2019

PICOTTI L., *Cybercrime e diritto penale*, in V. SELLAROLI, C. PARODI, *Diritto penale dell'informatica,* Milano, 2020

PILLER G., ZACCARIOTTO E., *Cyber-Laundering: The Union Between New Electronic Payment Systems and Criminal Organizations*, in Transition Study Review, 2009

PLANTAMURA V., *Tipo d'autore o bene giuridico tutelato per l'interpretazione, e la riforma, del delitto di riciclaggio?*, in *Riv. trim. dir. pen. econ*., 1-2, 2009, p. 165

PLANTAMURA V., *Riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, e confisca (artt. 648-bis, 648-ter e 648-quater)*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale, parte speciale*, vol. X, *I delitti contro il patrimonio*, Padova, 2011

PLANTAMURA V.*, Il cybericiclaggio*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Padova, 2019

POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, in Riv. Trim. Dir. Pen. Contemp., 2/2019, p. 159

RACCOMANDAZIONE DEL COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Misure contro il trasferimento e la custodia di fondi di origine criminale*, n. 80/10, 1980

RAPETTO U., *Il riciclaggio del terzo millennio, in Gnosis, Rivista italiana di intelligence,* 1999

RAYMAKERS J., *ICLG, The International Comparative Legal Guide to: Anti-Money Laundering 2019, 2nd Edition, chapter 24 "Netherlands*", 2019

RAZA M. S., *Role of money mules in money laundering and financial crimes. A discussion through case studies*, in Journal of financial crime, 2020, p. 15

RAZZANTE R.*, Il riciclaggio nella giurisprudenza. Normativa e prassi applicative*, Milano, 2011

REICH C., *The New Property,* in *The Yale Law Journal*, Vol. 73, no. 5, 1964

REUTER P., TRUMAN E.M., *Chasing dirty money*, 2004

REYES A., BRITTSON A., O'SHEA K., STEELE J., *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors*, 2007

RINALDI G., *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contr. e impr.*, 2019, p. 271

SANTINI C., *Globalisation and Offshore Dimension – Building Integrity, Confidence and Cooperation*, Relazione tenuta al *Nineteenth International Symposium on Economic Crime*, Cambridge, 12 settembre 2001, in *Journal of Money Laundering Control*, Volume V, n. 4, London, 2002

SANTONI L., *Operazioni in criptovaluta e abusivismo finanziario: nota a Cass. Pen., sez. II, 25 settembre 2020, n. 26807*, in Riv. Dir. Bancario, Fascicolo 2/2021, p. 2

SAVONA E., *Criminalità organizzata*, in Enciclopedia del Novecento, 1998

SAVONA E. E MIGNONE M., *The fox and the hunters: how IC Technologies change the crime race,* in *Crime and Technology*, 2004, p. 3

SCAPELLATO F., *Il fenomeno del riciclaggio e la normativa di contrasto*, Torino, 2013

SICIGNANO G. J., *L'acquisto di bitcoin con denaro di provenienza illecita,* in Archivio Penale 2020, p. 2

SOTIS C., *I principi di necessità e proporzionalità della pena nel diritto dell'Unione europea dopo Lisbona*, in Riv. Dir. Pen. Contemp., 1/2012, p. 111

STALENBERG F., *Find out How You Can Start Making a 6487 a Month at Home!*, 2002

STURZO L., *Bitcoin e Riciclaggio 2.0*, in *Dir. pen. contemp*., 2/2018, p. 19

TAKATS E., *Domestic money laundering enforcement*, in D. MASCIANDARO, E. TAKATS, B. UNGER, *Black Finance,* 2007

TARANTOLA A. M., *La prevenzione del riciclaggio nel settore finanziario. Il ruolo della Banca d'Italia*, in https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2011/Tarantola_100511.pdf, 2011

TATOZZI C., *Bitcoin: natura giuridica e disciplina applicabile al contratto di cambio in valuta avente corso legale*, reperibile in Banca Dati *online* al sito www.Ridare.it, 9 agosto 2017

TRANSCRIME, *Il rischio riciclaggio in Italia. Rapporto finale del progetto IARM*, 2017, p. 10

TRANSCRIME, *Assessing the risk of money laundering in Europe. Final report of project IARM*, 2017, p. 12

UN CONVENTION AGAINST ILLICIT TRAFFIC AND NARCOTIC DRUGS AND PHSYCHOTROPIC SUBSTANCES, 2008

UNIVERSITY OF UTRECHT AND AUSTRALIAN NATIONAL UNIVERSITY, B. UNGERDRS. M. SIEGEL, *The Amount and Effects of Money Laundering*, 2006

VADALÀ R.M., *Criptovalute e cyberlaundering: novità antiriciclaggio della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in Sistema Penale, 2020

VAN DUYNE P. C. & VAN DER LANDEN D., *"De kennelijke" oorsprong van sneeuwwtije. De nieuwe witwaswet en het "goede verhaal"*, 1999

VIGNA P.L., *Il fenomeno criminale*, in *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto.,* in (a cura di) E. CAPPA E L.D. CERQUA, Milano, 2012

WALL D. S., *Cybercrime: The transformation of crime in the information age* (*PCSS-Polity Crime and Society*), 2007

WARNAARS W. M., *Witwassen van bitcoins. De omgekeerde bewijlast bij het witwassen van bitcoins in het licht van de onschuldpresumptie*, 2019

YERMAK D., *Is Bitcoin a real currency? An economic appraisal*, NBER Working Paper No. 19747, 2013

ZACCHIA A., *La natura del reato di riciclaggio*. Nota a Cass. sez. II pen., 13 luglio 2016, n. 29611, in Cass. pen. 2017, 7, p. 2824

ZANCHETTI M., *Riciclaggio di denaro proveniente da reato*, Milano, 1997

GIURISPRUDENZA

Cass. Pen. sez. II, 30 giugno 1980, n. 2347

Cass. Pen., sez. II, 19 settembre 1988, n. 1101

Cass. Pen. sez. II, 5 giugno 2015, n.27806

Cass. Pen., 20 giugno 2012, n. 36759

Cass. Pen., sez. II, 6 novembre 2009, n.47375

Cass. Pen., sez. V, 1° ottobre 1996

Cass. Pen., sez. II, 11 aprile 2014, n. 1771

Cass. Pen., sez. II, 13 luglio 2020, n. 23774

Cass. Pen., sez. II, 12 gennaio 2006, n. 2818

Cass. Pen., sez. II, 9 marzo 2015, n. 26208

Cass. Pen., 5 ottobre 2011, n. 39756

Cass. Pen., sez. V, 18 gennaio 2018, n.5459

Cass. Pen., sez. II, 14 giugno 2018, n. 29920

Cass. Pen., sez V, 2 febbraio 2017, n. 25924

Cass. Pen., sez II, 11 giugno 2015, n. 41330

Cass. Pen., sez. II, 7 gennaio 2011, n. 546

Cass. Pen., sez. VI, 18 dicembre 2007, n. 16980

Cass. Pen. sez II, 6 novembre 2009, n. 47375

Cass. Pen., sez II, 6 novembre 2009, n. 47375

Cass. Pen., sez. II, 23 ottobre 2018, n. 56633

Cass. Pen., 29 aprile 2009, n. 246561

Cass. Pen., 14 gennaio 2010, n. 17694

Cass. Pen., 2 febbraio 1983

Trib. Nuoro, 3 novembre 2000

Corte App. Cagliari, 19 febbraio 2002

Cass. Pen. sez. II, 24 aprile 2012, n. 43534

Cass. Pen., sez. II, 7 ottobre 2021, n. 2868

Cass. Pen., 7 marzo 2019, n. 13795

Cass. Pen. 14 luglio 2016, n. 33704

Cass. Pen., sez II, 5 giugno 2015, n. 27806

Cass. Pen., sez. VI, 29 ottobre 2015, n. 563

Cass. Pen. sez. II, n. 47147, 2013

Trib. Milano, 10 dicembre 2007

Cass. Pen., sez. II, 24 ottobre 2013, n. 47147

Trib. Verona, sent. 195 del 2017

C.G.U.E., sez. V, n. 264, 2015

Trib. di Brescia, 25 luglio 2018, n.7556, in *Rivista del Notariato*, 2018, 6, II, 1283

Corte d'Appello di Brescia, sez. I, 30 ottobre 2018, in *Rivista dei Dottori Commercialisti*, 2019, 1, 52

Cass. Pen., sez. II, 10 ottobre 2021, n.44337

Cass. Civ. sez I, 26 maggio 2000, n. 6957

Cass. Civ. sez III, 12 dicembre 1986, n. 7409

Cass. Civ. sez. I, 30 gennaio 1997, n. 934

Cass. Civ., sez. II, 5 febbraio 2013, n. 2736

Cass. Civ., sez. II, 15 aprile 2009

Cass. Civ., sez. II, 5 febbraio 2013, n. 2736

Cass. Pen., sez. II, 13 aprile 2020, n. 11959

Cass. Pen., sez. II, 17 gennaio 2012, n. 6061

Cass., sez. II, sent. 14 luglio 2017, n. 42561

Cass. Pen., sez. II, 17 gennaio 2018, n. 17235

Hoge Raad (Corte Suprema Olandese), 7 ottobre 2008, 03511/06, LJN: BD2774

Hoge Raad (Corte Suprema Olandese), 26 ottobre 2010, LJN: BM4440, NJ 2010, 655

CEDU, Zschüschen *v*. Belgio, 2 maggio 2017

Corte Distrettuale Overijssel, ECLI: ECLI:NL:RBOVE:2014:2667

Trib. Distrettuale dei Paesi Bassi, Rb. Midden-Nederland, 24 gennaio 2018, ECLI:NL:RBMNE:2018:234

ECLI:NL:RBROT:2019:2408

ECLI:NL:RBMNE:2017:5713