CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

NUOVE FRONTIERE DELL´AUTORICICLAGGIO: CYBERLAUNDERING E RESPONSABILITÀ DELL´ENTE

Il necessario bilanciamento tra esigenze di trasparenza e sicurezza nelle transazioni in criptovalute: responsabilità dell´exchanger nello scambio di moneta elettronica.

di **Alessandra Rea**
IUS/05 - DIRITTO DELL'ECONOMIA
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Mercoledì 12 Febbraio 2020

CamminoDiritto.it
ISSN 2421-7123

Sommario: 1. Premessa - 2. Sistema della Blockchain e Network di Controllo. - 3. Effetti distorsivi del sistema: lo pseudoanonimato garantito dal sistema di controllo peer-to-peer. - 4. La figura dell'exchanger. Profili di responsabilità alla luce delle ultime Direttive Antiriciclaggio. - 5. Fenomenologia criminale.

1. Premessa

Sulla scia della crisi del 2008 si è sviluppato un complesso sistema di criptovalute, che, lungi dal configurare una moneta elettronica, può definirsi alla stregua di uno «strumento, accettato su base volontaria, che non costituisce mezzo legale di estinzione delle obbligazioni pecuniarie»[1]. Ad oggi Bitcoin rappresenta la più diffusa delle cryptocurrencies tra le species di altcoins, con un valore di capitalizzazione pari a circa 98 miliardi di euro; definita la 'nuova frontiera' delle transazioni economiche, reca in sé i vantaggi della moneta elettronica e quelli del contante[2], rappresentando un 'ibrido' tra le due figure[3], pur potenzialmente mezzo di trasferimento di denaro per scopi illeciti: Bitcoin «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» [4].

2. Struttura della Blockchain e Network di Controllo

Il sistema criptovalutario presenta profili controversi, evidenti sin dall'analisi delle modalità di trasferimento. In buona sostanza, Bitcoin non può essere definita moneta elettronica, in quanto «nello schema tradizionale la moneta elettronica non è altro che una disponibilità di potere d'acquisto registrata su un conto corrente acceso presso una Banca» [5]: imprescindibile sarà la presenza di un sistema centralizzato, facente capo ad una Banca che, in quanto intermediario finanziario, sarà tenuta agli obblighi antiriciclaggio ex D.lgs. 231/2007. A medesima conclusione non può giungersi per il Bitcoin, che trova la sua peculiarità proprio in un sistema che sembra aver superato il network di controllo centralizzato: le transazioni saranno verificate attraverso una blockchain, una 'catena di controllo' formata da diversi miners che operano mediante un sistema peer-to-peer.

In altre parole, per espressa volontà dell'ideatore del Bitcoin, i trasferimenti di valuta virtuale devono avvenire in un ambiente accessibile al pubblico[6], al punto che si è reso necessario un bilanciamento tra esigenze di privacy, sicurezza nelle transazioni e tutela del mercato sano. Il processo di blockchain è stato costituito proprio per essere diffuso, apparentemente 'trasparente' ma sicuro, pur tuttavia non conservando il sistema di

CamminoDiritto.it
ISSN 2421-7123

centralizzazione proprio della moneta elettronica. La blockchain è proprio «una serie concatenata di blocchi (da cui il nome) i quali registrano, per ogni transazione, l'identità del pagante, l'importo trasferito e l'identità del beneficiario»[7]. Una volta che nel singolo blocco sono acquisite le informazioni richieste, questo viene 'chiuso' da un 'sigillo', il cd. hash, costituito da un codice alfanumerico. Ogni modifica del blocco comporta un'alterazione dell'hash, con conseguente impossibilità di riconoscere il blocco modificato come originale.

La blockchain si impianta nel momento in cui si 'collegano' diversi blocchi tra loro: nella catena, ogni blocco non solo conterrà il proprio hash, ma anche l'hash del blocco precedente.

Fatta eccezione per il primo anello, ogni elemento della catena dovrà contenere non solo gli elementi identificativi della transazione compiuta (ovvero, come detto, l'identità del pagante, l'importo trasferito e l'identità del beneficiario, che configurano l'hash), ma anche l'hash del blocco precedente, nella rappresentazione grafica indicato come p. hash (previous hash).

Ogni catena in tal modo realizzata è trasmessa ad una serie di utilizzatori, scelti tra coloro che sono in grado di decriptare la chiave utilizzata per l'accesso al sistema. Questi utenti, definiti miners, verificano la fattibilità dell'operazione di trasferimento che si 'innesta' nella blockchain[8]; il corrispettivo per l'attività da essi prestata, anche mediante l'utilizzo di hardware dalle altissime prestazioni, è in Bitcoin[9].

E dunque, il Bitcoin può essere definito come una «moneta virtuale decentralizzata»[10]: i verificatori non sono identificabili in un solo organismo (come avviene nel caso di moneta elettronica, nella persona della Banca), ma in una pluralità di utenti «tra loro legati in modo orizzontale e senza vincoli gerarchici»[11], che devono approvare la transazione.

Oltre ai miners, vi sono diversi soggetti nel sistema dei Bitcoin, che possono organizzarsi anche sotto forma di Società. Di particolare interesse la figura degli users e degli exchangers.

3. Effetti distorsivi del sistema: lo pseudoanonimato garantito dal sistema di controllo peer-to-peer

Gli users (utenti) sono «persone o società che acquistano od ottengono la valuta virtuale per acquistare beni o servizi materiali o virtuali, per poi trasferirla ad altri soggetti a fini

CamminoDiritto.it
ISSN 2421-7123

personali o per detenerla a titolo di investimento»[12]. Gli utenti sono garantiti da un anonimato 'controllato', detto pseudoanonimato: all'interno del network, saranno titolari di una 'chiave pubblica' e di una 'chiave privata' (rectius, di un username e di una password). Ogni utente può visionare in qualsiasi momento la rete di operazioni compiute mediante Bitcoin[13], ma il nominativo degli utenti non sarà corrispondente al loro nome reale, quanto piuttosto ad un numero identificativo della propria chiave pubblica. E il c.d. pseudoanonimato del sistema Bitcoin, consiste proprio nella possibilità di avere una piena visione di tutte le attività compiute, ma l'user potrà accedere attraverso più chiavi pubbliche, mediante la creazione di più account, al fine di dissimulare la tracciabilità dei suoi movimenti economici. Al medesimo scopo sono asservite diverse piattaforme che si stanno diffondendo tra i trader, i cd. mixers, ossia dei «software sempre più complessi ed efficienti che vengono offerti dagli utenti interessati e la cui finalità è proprio quella di aumentare la privacy bypassando la natura pubblica della blockchain»[14], dirottando la transazione su un server diverso da quello dell'agente.

Il – potenzialmente – totale anonimato garantito dall'utilizzo delle criptovalute si presta ad essere un buon incentivo alle condotte criminose – anche, ma non solo – di ripulitura di capitali illeciti. In particolare, il programma criminoso può realizzarsi per il tramite di tre canali[15]:

è possibile che il Bitcoin sia frutto 'mediato' di reati comuni, nel caso in cui la moneta reale venga convertita in criptovaluta per oscurare l'identificazione della sua provenienza illecita; si può avere anche l'ipotesi di una moneta che nasce come Bitcoin ed è direttamente riconducibile alla categoria di denaro sporco, come è capitato nel celeberrimo caso WannaCry[16]; infine, può anche darsi il caso del criminale che voglia conservare il Bitcoin come moneta virtuale finché, attraverso le transazioni e la messa in circolo nell'economia legale, esso non potrà essere riconvertito in moneta reale 'ripulita' [17]. **4. La figura dell'exchanger. Profili di responsabilità alla luce delle ultime Direttive Antiriciclaggio**

Con il D.lgs. 25 maggio 2017 n. 90 l'Italia (prima in Europa) ha dato attuazione alla IV Direttiva Europea in tema di antiriciclaggio[18] prevedendo un adeguamento della disciplina antiriciclaggio di cui al D.lgs. 231 del 2007. Il Decreto contiene una vera e propria definizione di valuta virtuale, qualificata nei termini di una «rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente»[19], dopodiché precisando chi siano gli exchangers, ossia «ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali [...] allo scambio [...] di valuta virtuale e alla loro conversione da ovvero in valuta avente corso legale»[20], ed altresì qualificandoli come soggetti gravati dagli oneri antiriciclaggio.

CamminoDiritto.it
ISSN 2421-7123

Nella pratica, gli exchangers sono quei soggetti che, in veste privata o di società, creano piattaforme che mettono in contatto domanda e offerta, ove quindi è possibile tanto depositare una tipologia di criptovalute che convertirle in valute avente corso legale o in altre criptovalute. Potrebbero essere parificabili a delle agenzie di cambio, ed è esattamente questa la soluzione prospettata dal legislatore del 2017, in quanto li sottopone alla disciplina antiriciclaggio.

Gli exchangers sono tenuti all'iscrizione in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli Agenti e dei Mediatori ex art. 128-undecies del T.U.B., essendo così parificati ai cambiavalute. In quanto soggetto obbligato agli oneri antiriciclaggio ex D.lgs. 231/2007, l'exchanger sarà tenuto ad identificare il cliente attraverso l'esecuzione di un profiling, così come previsto dagli artt. 17 e seguenti del D.lgs. 231/2007. Gli obblighi di verifica possono essere qualificati in obblighi semplificati (art. 23 D.lgs. 231/2007) e obblighi rafforzati (art. 25 del medesimo Decreto) di adeguata verifica[21]:

coloro che sono sottoposti ad obblighi ex D.lgs. 231/2007 sarà tenuto ad una verifica semplificata, ai sensi dell'art. 23 della disciplina antiriciclaggio, nel caso in cui vi sia «un basso rischio di riciclaggio o di finanziamento del terrorismo»: in questi casi, gli obblighi di verifica si definiscono semplificati in ragione della minore estensione e frequenza degli adempimenti previsti dall'art. 18 del D.lgs. 231/2007; ai sensi dell'art. 25 del medesimo Decreto, «i soggetti obbligati, in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo, adottano misure rafforzate di adeguata verifica della clientela acquisendo informazioni aggiuntive sul cliente e sul titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto ed intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale». Ma non solo: la conseguenza dell'impostazione assunta dal legislatore è che gli exchangers, ad oggi, potrebbero rispondere di riciclaggio nel caso in cui «prestando la propria attività di cambio valuta, in via amatoriale o professionale, contribuiscano dolosamente a mutare la natura del provento del delitto presupposto, pur sospettandone la provenienza illecita»[22].

Seguendo l'orientamento attualmente più diffuso in giurisprudenza, peraltro, l'attività di cambiavalute virtuale potrebbe anche essere suscettibile di imputazione per concorso in autoriciclaggio, pur con le critiche che sono state mosse da diffusa dottrina sulla conseguente estensione dell'ambito di operatività della fattispecie di cui all'art. 648-ter.1 del codice penale.

CamminoDiritto.it
ISSN 2421-7123

Da valutare la possibilità che l'exchanger risponda di autoriciclaggio per concorso nel reato proprio, nel caso in cui l'autore del predicate crime abbia voluto investire Bitcoin derivanti da una condotta illecita nell'attività di cambia valute (attività economica finanziaria), ostacolando concretamente l'identificazione della loro provenienza illecita[23]. Alla stessa conclusione dovrà pervenirsi nel caso di attività di exchanging esercitata con finalità illecite[24]: la soluzione dipenderà dal corretto inquadramento giuridico dell'attività dell'exchanger e dalla sua riconducibilità nell'alveo dell'art. 648-ter.1 del codice penale.

Ad ogni modo, è evidente l'importanza della funzione dell'exchanger nel contrasto al riciclaggio operato mediante valuta virtuale; ciononostante, non può tacersi come l'utente (nonché autore del predicate crime) abbia la mera facoltà di avvalersi di un exchanger, ben potendo autonomamente acquistare o trasferire dei Bitcoin senza la necessità di un 'intermediario'[25]: anche per questo l'intervento legislativo lascia con l'amaro in bocca, non risultando idoneo a prevenire tutte le fattispecie di reato che la realtà criminologica lascia prospettare, non risolvendo i dubbi riguardo l'effettiva compatibilità delle fattispecie codicistiche con i cybercrimes. Chiaro sarà che un eventuale amministratore di società che effettui, nell'interesse o a vantaggio della società, attività di acquisto o trasferimento di Bitcoin volte a mascherare la provenienza illecita dell'utilità, possa rispondere di autoriciclaggio con relativa estensione della responsabilità anche all'ente ex art. 25-octies D.lgs. 231/2001[26].

5. Fenomenologia criminale

È quindi da chiarire se e in che modo l'autoriciclaggio via web possa essere sussunto nel paradigma codicistico, al di là di esempi scolastici di relativo interesse scientifico ed oltre le novità introdotte dal D.lgs. n. 90 del 2017, onde determinare l'efficacia repressiva della normativa vigente.

Al fine di valutare l'applicabilità degli artt. 648-bis e seguenti del codice penale, nonché dell'art. 25-octies del D.lgs. 231/2001, ci si dovrà preliminarmente chiedere se la valuta virtuale può essere considerata un 'bene'. Alla luce dei più recenti orientamenti dottrinali, nella nozione di bene di cui all'art. 648-bis c.p. è ricompreso anche il concetto di 'bene immateriale'[27]. Anche qualora così non fosse, la criptovaluta può ritenersi sussumibile nella categoria delle 'altre utilità' richiamata dalla disposizione[28].

In secondo luogo, dovrà chiarirsi quando si tratterà di riciclaggio e quando di autoriciclaggio, non essendo chiaro il (controverso) confine tra riciclaggio e concorso dell'extraneus in autoriciclaggio: è già stata valutata la posizione dell'exchanger, ora si ritiene opportuno ampliare il discorso anche ad altre figure (come ad esempio i wallet provders, gli host providers o i miners) che operano nel settore delle criptovalute. Come

CamminoDiritto.it
ISSN 2421-7123

innanzi evidenziato, vi sono – fra l'altro – due modalità mediante le quali il 'criminale' può strumentalizzare la valuta virtuale per scopi di riciclaggio: c'è il caso in cui il Bitcoin 'nasca' come denaro sporco, ed il caso in cui valuta reale avente origine illecita venga convertita in Bitcoin[29]. Appare questo l'utile punto di partenza per la qualificazione degli elementi essenziali del cyberlaundering.

Nel primo caso, avremo un paper trail completamente sviluppatosi online: si dia il caso in cui una società di telefonia mobile decida di danneggiare un proprio diretto concorrente nel mercato infettandone i sistemi operativi con un malware (immesso nella rete da un operatore informatico facente capo all'azienda della società agente), successivamente chiedendo riscatto in Bitcoin per il ritiro dell'attacco. L'utilità così ricavata viene reinvestita nel mercato mobiliare informatico, ottenendo un utile che a sua volta viene movimentato attraverso diverse attività di trading. Rilevandosi come il reato di danneggiamento a sistema operativo rientri nel numerus clausus ex D.lgs. 231/2001, ci si chiede se la condotta di reinvestimento possa essere considerata idonea a costituire un ostacolo concreto all'individuazione illecita dell'utilità e, successivamente, se l'attività di trading possa ritenersi ricompresa tra le attività economiche, imprenditoriali, finanziarie e speculative di cui all'art. 648-ter.1 del codice penale. Quanto al primo profilo, si ritiene che l'attività di trasferimento di Bitcoin possa essere definita dissimulatoria solo laddove essa sia compiuta in modo da rendere complessa anche ai miners la provenienza del denaro o l'identificazione del soggetto: potrà reputarsi tale, ad esempio, uno spostamento di Bitcoin compiuto in più tranches e con l'ausilio di un mixer. Sarà meno sensibile alla libera valutazione del giudice la configurabilità dell'attività di trading quale attività rilevante ex art. 648-ter.1 c.p.: difatti, dottrina e giurisprudenza ormai uniforme[30] tendono a considerare l'attività di cambio valuta come attività finanziaria.

Soluzioni meno controverse si avranno nel caso di paper trail realizzato soltanto parzialmente online: ad esempio, nel caso di una società che investa in Bitcoin le utilità frutto di false comunicazioni sociali (o, a contrario, nel caso di estorsione online che genera un profitto in Bitcoin trasformato in valuta reale), imprescindibile sarà l'attività di conversione della valuta reale in valuta virtuale (o viceversa), con conseguente realizzazione di autoriciclaggio, laddove ne sussistano gli ulteriori requisiti.

Note e riferimenti bibliografici

[1] Clemente, intervento nel corso del convegno di studi Nuova finanza, prevenzione dell'illegalità e tutela del risparmio, tenutosi presso l'Università degli Studi di Salerno il 21 maggio 2018.

[2] Cfr. Passerelli, Bitcoin e antiriciclaggio, in https://www.sicurezzanazionale.gov.it.

CamminoDiritto.it
ISSN 2421-7123

[3] Accinni, Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017), in Archivio penale, n. 1/2018, p. 2.

[4] Amato-Fantacci, Per un pugno di Bitcoin, Milano, 2016, p. 3.

[5] Accinni, op. cit., p. 2.

[6] Nakamoto, Bitcoin: a peer-to-peer electronic cash system, in {https/URL}

[7] Amato-Fantacci, Per un pugno di Bitcoin, Milano, 2016, p. 16.

[8] Mancini, Bitcoin: rischi e difficoltà normative, in Banca impresa soc., n. 1/2016, pp. 126 ss.

[9] Tuttavia, può porsi il problema dell'hacker che, utilizzando un potente hardware, possa non solo modificare l'hash del blocco manomesso, ma anche tutti gli hash della catena di controllo affinché non risulti la variazione degli elementi costitutivi il blocco. Per eludere un tale rischio, è attivato un timer di dieci minuti (chiamato "periodo di verifica") dalla richiesta all'autorizzazione dell'incatenamento: pertanto, un eventuale hacker non solo dovrà modificare gli hash dell'intera catena, ma dovrà farlo ad intervalli regolari di dieci minuti.

[10] Accinni, Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017), in Archivio penale, n. 1/2018, p. 4.

[11] Krogh, Transazioni in valute virtuali e rischi di riciclaggio. Il ruolo del notaio, in Il Notariato, n. 2/2018, p. 159.

[12] Accinni, Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017), in Archivio penale, n. 1/2018, p. 4.

[13] Sul sito www.blockexplorer.com

[14] Accinni, Op. cit., p. 6. Si stanno diffondendo anche criptovalute (come Monero e ZCash) che garantiscono ai propri utilizzatori un simile sistema di anonimato.

CamminoDiritto.it
ISSN 2421-7123

[15] Naddeo, intervento nel corso del convegno di studi Nuova finanza, prevenzione dell'illegalità e tutela del risparmio, tenutosi presso l'Università degli Studi di Salerno il 21 maggio 2018.

[16] L'attacco WannaCry, posto in essere nel corso del mese di maggio 2017, ha avuto ad oggetto la diffusione di virus su larga scala, infettando alcuni sistemi informatici preposti ad attività (non solo) economiche rilevanti (come Renault, il Ministero dell'interno russo e l'Università degli Studi Milano-Bicocca). Successivamente, sono stati colpiti altre 230.000 computer in 150 diversi Paesi. L'epidemia era finalizzata a scopi di estorsione, in quanto il virus diffuso dagli hackers poteva criptare i file presenti sul computer per renderli inaccessibili agli utenti, con conseguente richiesta di riscatto in Bitcoin per decriptarli; Accinni, Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017), in Archivio penale, n. 1/2018, p. 9.

[17] Anche attraverso l'attività di cd. money mule, ossia soggetti che acquisiscono e ripuliscono i proventi dell'attività illecita.

[18] Direttiva (UE) n. 849/2015.

[19] Art. 1 comma 2 lett. qq) del D.lgs. 231 del 2007, così come modificato dal D.lgs. 90 del 2017.

[20] Art. 1 comma 2 lett. ff) del D.lgs. 231 del 2007, così come modificato dal D.lgs. 90 del 2017.

[21] Castaldo, Riciclaggio, in Pulitanò (a cura di), Diritto penale parte speciale, vol. II: tutela penale del patrimonio, Torino, 2013, p. 224.

[22] Sturzo, Bitcoin e riciclaggio 2.0, in Diritto penale contemporaneo, n. 5/2018, pp. 27 s.

[23] Rilevante questione si pone sul piano del dolo eventuale: nel caso in cui l'exchanger (od anche il miner) abbia dubbi sulla provenienza lecita o meno del denaro, ma comunque provveda a convertirlo in Bitcoin (o, nel caso dei miners, questi ultimi autorizzino la conversione), si potrà avere concorso in autoriciclaggio? Il discorso è ben controverso in dottrina, ma si propende per la non configurabilità del dolo eventuale, onde non proporre una moltiplicazione ad infinitum del rischio di autoriciclaggio: cfr. Cap. I § 7, infra.

[24] Degno di nota è il caso della piattaforma BTC-e, «un intermediario mobiliare estero

CamminoDiritto.it
ISSN 2421-7123

che cambia valute e criptovalute quali Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum e Dash. È uno dei maggiori convertitori di valute al mondo ed ha agevolato transazioni di denaro provenienti da attacchi ransomware, hackeraggio informatico, furti di identità, evasione fiscale, corruzione e spaccio di droga. [...] Tra le altre violazioni, BTC-e ha omesso di richiedere agli utenti informazioni ulteriori rispetto a username, password ed indirizzo e-mail. Invece di agire per scongiurare rischi di riciclaggio, BTC-e ed i suoi amministratori hanno abbracciato gli evidenti intenti criminosi dei propri utenti. Gli utenti discutevano apertamente ed esplicitamente la natura e le finalità della propria attività criminosa sulla chat di BTC-e. Il servizio clienti di BTC-e offriva consigli su come processare ed avere libero acceso a proventi di attività illecita quale la vendita di droga sui dark-net markets quali Silk Road, Hansa Market ed Alphabay»: Accinni, Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017), in Archivio penale, n. 1/2018, p. 16.

[25] Messina, Bitcoin e riciclaggio, in Quattrociocchi (a cura di), Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale, Torino, 2017, pp. 381 s.

[26] Ovviamente, se ed in quanto l'attività distrattiva costituisca un concreto ostacolo all'individuazione dell'oggetto del reato presupposto, in esecuzione del cd. paper trail; Simoncini, Il cyberlaudering: la "nuova frontiera" del riciclaggio, in Riv. Trim. dir. pen. econ., n. 4/2015, p. 915.

[27] Capaccioli, Riciclaggio ed antiriciclaggio nell'era del Bitcoin, in Coinlex, 2015. L'autore ritiene che l'oggetto materiale del reato comprenda «anche i beni riconducibili ad un'essenza economico finanziaria»; Sturzo, Bitcoin e riciclaggio 2.0, in Diritto penale contemporaneo, n. 5/2018, p. 24.

[28] Capaccioli, Criptovalute e Bitcoin, un'analisi giuridica, Milano, 2015, p. 252.

[29] Sturzo, Bitcoin e riciclaggio 2.0, in Diritto penale contemporaneo, n. 5/2018, pp. 24 s.

[30] Cass. pen., Sez. II, sentenza del 28 luglio 2016 n. 33074, con nota di Carrelli Palombi, Autoriciclaggio. Prime precisazioni della Cassazione sull'elemento materiale e quello psicologico, in Il Penalista web; Gullo, Il delitto di autoriciclaggio al banco di prova della prassi: i primi (rassicuranti) chiarimenti della Cassazione, in Dir. pen. proc., n. 4/2017, p. 482. Secondo l'autore «è da ritenersi finanziaria l'attività così qualificata dalle disposizioni del Testo Unico in materia (nella specie il riferimento è all'art. 106 del T.U.F.) ovverossia "l'assunzione di partecipazioni, la concessione di finanziamenti sotto qualsiasi forma, la prestazione di servizi di pagamento, l'attività di cambia valute"».

CamminoDiritto.it
ISSN 2421-7123

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina: https://rivista.camminodiritto.it/articolo.asp?id=4748