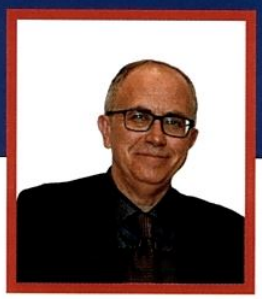
Rassegna dell'Arma dei Carabinieri

Istituto Poligrafico e Zecca dello Stato S.p.A. — Maria C. Perrini *inc.*

Scuola Ufficiali Carabinieri

POLIGRAFICO E ZECCA DELLO STATO ITALIANO
IPZS S.p.A.

3
Anno LXVI - luglio / settembre 2018



Criptovalute e rischi per la sicurezza[1]

Prof. Avv. Ranieri RAZZANTE

Docente di Legislazione antiriciclaggio all'Università di Bologna

SOMMARIO: 1. Premessa metodologica. - 2. Il riciclaggio "virtuale" di denaro. - 3. Il finanziamento del terrorismo con criptovalute.

1. Premessa metodologica

La Relazione annuale della UIF (Unità di Informazione Finanziaria per l'Italia), ha recentemente rilanciato gli allarmi sulle criptovalute[2]. Si parla nientemeno anche di possibili utilizzi distorti della *Financial Technology*[3]. Il rischio "ontologico" all'utilizzo di criptovalute è quello di facilitare transazioni di denaro di illecita provenienza[4]. L'avvento della tecnologia ci mette a confronto con la sconfinatezza del *world wide web* e di fronte a una difficoltà - sempre crescente - di contrasto ai fenomeni illeciti. Il *deep web*, ovvero quella parte di internet che si nasconde al di sotto del *web*, è un territorio che si presta ad attività illecite per celare la tracciabilità delle operazioni[5].

---

(1) Lo scritto riproduce, con le opportune modifiche, un analogo studio pubblicato nel settembre 2018 in un libro, a cura del sottoscritto, edito da Maggioli.

(2) "Una elevata criticità è associata (...) al ricorso a prototti emergenti legati alle applicazioni di nuove tecnologie alla finanza (Fintech), quali le valute virtuali e le piattaforme di *crowdfunding*". Così C. CLEMENTE, *Relazione per l'anno 2017 della Unità di Informazione Finanziaria*, pag. 4, in www.uif.it.

(3) "È importante che l'economia digitale non diventi una zona franca. (...) La UiF è consapevole di tali esigenze e sta dedicando attenzione al mondo del Fintech", op. cit., pag. 17.

(4) Al contrario di quanto affermato dai sostenitori della assoluta tracciabilità e liceità delle monete in discorso, cito l'allarme riportato dai nostri servizi di sicurezza nella recente *Relazione sulla politica dell'informazione per la sicurezza 2017*, a pag. 8 e poi diffusamente nel prosieguo dell'illuminante testo.

(5) Sul tema del *cyber crime*, da ultimo, *Darkweb and cybercrime*, di N. Var DEN MEULEN, e *Cybercrime and international relations*, di F. RUGGE, sul sito www.ispionline.it.

Nel *black market* vengono scambiati armi, esplosivi, soldi rivenienti dal traffico di esseri umani, sostanze farmaceutiche e droga senza correre rischi di individuazione, pagando con moneta virtuale[6].

2. Il riciclaggio "virtuale" di denaro

È opportuno ricordare che il riciclaggio di denaro è il processo con il quale vengono sostituiti, trasferiti o occultati - attraverso operazioni formalmente lecite - denari o altre utilità provenienti da delitto non colposo, in modo da ostacolarne la loro illecita provenienza[7].

Principio cardine attorno al quale ruota la normativa antiriciclaggio delineata dal D.Lgs. 231 del 2007, integrato dal decreto legislativo 90/2017, è quello della prevenzione. Gli strumenti di prevenzione prevedono una serie di obblighi per gli intermediari finanziari finalizzati alla conoscenza del cliente[8], alla tracciabilità delle transazioni, all'individuazione e alla segnalazione di operazioni sospette[9].

L'identificazione e la costante verifica dell'operatività della clientela, basata sul principio di proporzionalità, risulta fondamentale per determinare la misura del rischio associabile al singolo cliente e all'operazione messa in atto, in modo da valutare la coerenza delle operazioni con il profilo del cliente stesso[10].

(6) La soluzione auspicabile per contrastare il riciclaggio e il finanziamento del terrorismo, rivendicata dal Professor Robby Houben dell'Università di Antwerp, durante il *workshop* "*Taxation and fight against money laundering: crypto currencies, digitalization and the European semester*", tenutosi presso la Commissione per i reati finanziari, evasione ed elusione fiscale del Parlamento Europeo, è la registrazione obbligatoria per tracciare il flusso delle valute digitali per risalire al nome del soggetto che si cela dietro alla moneta digitale.

(7) Il presupposto comune alle tre fattispecie previste dal codice penale (artt. 648-*bis*, 648-*ter* e 648-*ter* 1) è la commissione pregressa di un delitto che abbia generato un profitto illecito utile alla reimmissione nel circuito economico legale delle relative somme. Cfr. R. RAZZANTE, *Il riciclaggio come fenomeno transnazionale: normative a confronto*, Giuffré Editore, 2014, pag. 185; ancora, dello stesso Autore, *Il riciclaggio nella giurisprudenza*, Giuffrè, 2011.

(8) Il concetto di riciclaggio e di identificazione del cliente è stato introdotto per la prima volta nella *Dichiarazione di Principi sulla prevenzione dell'utilizzo a fini criminosi del sistema bancario per il riciclaggio di fondi di provenienza illecita*, adottata dal Comitato di Basilea per le regolamentazioni bancarie e le pratiche di vigilanza, istituito per fronteggiare le crisi bancarie e valutarie insorte nei mercati interni ed internazionali.

(9) Ai sensi dell'art. 39 del D.lgs. 231/2007, la segnalazione di operazione sospetta deve essere effettuata "quando (gli operatori) sanno, o sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa". Per un commento, R. RAZZANTE, *Codice della normativa antiriciclaggio*, Maggioli, 2018.

(10) R. RAZZANTE, *Il riciclaggio come fenomeno transnazionale: normative a confronto*, cit., pagg. 180-181.

Senza l'obbligo dell'identificazione certa si può consumare facilmente ogni genere di illecito, soprattutto in campo finanziario[11].

L'assenza di intermediari finanziari e l'anonimato delle transazioni previsti dal *Protocollo di Nakamoto* complicano questo tipo di indagine.

Le transazioni con le valute virtuali sono tracciabili, ma coloro che le effettuano sono e restano anonimi, e sono sottratte al controllo delle banche centrali e dei governi che si basano su un sistema "decentralizzato".

Il monitoraggio sul collocamento, la stratificazione e l'integrazione del denaro sporco è molto complicato per gli enti di controllo, considerato che la rete Bitcoin permette a ogni utente di trasferire soldi a velocità quasi istantanea, senza barriere all'ingresso, a bassissimo costo, nell'anonimato virtuale e in assenza di tracciabilità.

Anche se al momento in cui i bitcoin vengono spostati da un indirizzo all'altro, ogni transazione viene registrata presso la *blockchain*[12], il sistema è stato ideato anche per poter creare un numero infinito di indirizzi bitcoin, attraverso i quali, per l'appunto, "annebbiare" i trasferimenti e le identità collegate.

Non si deve dimenticare che, come ricordano le Autorità internazionali nelle loro innumerevoli pronunce, i bitcoin (e le cripovalute):

- sono rappresentazioni digitali di valore;
- sono decentralizzate, cioè non emesse e garantite da banche centrali;
- non sono collegate a una valuta legale e stabile;
- non possiedono lo status di moneta legale o valuta;
- sono trasferibili elettronicamente, archiviabili e trattabili[13].

---

(11) Riprendendo la relazione Uif sopra citata, a pag. 17, si legge che "*(…) la rarefazione delle relazioni personali, le ampie possibilità di preservare l'anonimato e la perdita di significato dei riferimenti geografici rendono questi mercati attrattivi per il riciclaggio*".

(12) Ritengo "strategica" ai fini della comprensione di quanto stiamo trattando la pubblicazione *Cryptocurrencies and blockchain*, di R. HOUBEN, A. SNYERS, *EU Parliament, TAX3 Committee*, del luglio 2018, reperibile sul sito internet dell'Autorità.

(13) Segnalo come "scandalosi" i concetti a tal riguardo contenuti in un rapporto (del febbraio 2018) di Standard & Poor's, *The future of banking: cryptocurrencies will need some rules to change the game*, ove tra l'altro si afferma - come efficacemente riassume M. BUSSI in un articolo su MF (Milano Finanza) del 20 febbraio scorso - che in attesa di regolamentare il settore, si possono far crollare i prezzi delle criptovalute, facendo rimettere "solo i piccoli risparmiatori", ma nel frattempo regolamentando il settore.
A ciò mi basta allegare riferimento a procedimento della nostra Autorità Antitrust contro "Onecoin", per pubblicità ingannevole e danni ai risparmiatori, di cui al provvedimento in adunanza del 25 luglio 2017, riportato nel Bollettino n. 31, del 16 agosto 2017, alle pagg. 154-177, che consiglio di leggere come *leading case* di "antigiuridicità potenziale" delle valute in discorso.

Ma queste "valute" sono accettate in pagamento da "comunità" di soggetti collegati; ed è qui che si concentra l'attenzione degli esperti di reati come quelli in predicato.

Il riciclaggio non si preoccupa dell'intensità e possibilità di frazionamenti. Con la V Direttiva UE in materia di prevenzione del riciclaggio e del finanziamento del terrorismo, è stato previsto l'assoggettamento alle norme antiriciclaggio di coloro che, non solo cambiano valute virtuali in altre monete aventi corso legale (i cosiddetti "*exchangers*", peraltro già soggetti alle regole oggi in Italia), bensì i «prestatori di servizi di portafoglio digitale», cioè quei soggetti che forniscono "servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali" (cfr. art. 1, comma 1, lett. c, sub g ed h).

Clienti e movimenti saranno chiari, imponendosi la compilazione di schede di adeguata verifica all'atto dell'accensione di conti e/o di cambio di valute, così come l'obbligo di segnalazione di operazioni sospette.

Giova ricordare che per il finanziamento del terrorismo le disposizioni sono le stesse, gli obblighi gli stessi, e cambia lo scopo.

Nessuna zona franca verrà consentita a chi opererà - legittimamente, accreditandosi nei modi che le norme sia primarie che secondarie decideranno - nel settore.

A tale ultimo proposito, mentre scriviamo è presente sul sito del Ministero dell'economia e delle finanze una bozza di decreto, pubblicata il 31 gennaio 2018 per la consultazione, nella quale si prevede una regolamentazione dei soggetti "prestatori di servizi relativi all'utilizzo di valuta virtuale"[14].

Attualmente non vi sono ulteriori sviluppi (la consultazione si è conclusa il 16 febbraio 2018, con la partecipazione di ben trenta utenti), ma il DM si può anticipare come segue.

La valuta virtuale, che la lettera e) del comma 2 dell'art. 1 indica come "la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente", non ha quindi "valore legale" e non è "moneta"[15].

(14) La lettera b) del comma 2 dell'art. 1 del provvedimento in commento li definisce come "ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale".

(15) Non in linea con quanto affermo, e verifico, appare l'articolo (*rectius*: l'affermazione) di C.

In secondo luogo, il decreto istituisce uno speciale "Registro" per i suddetti soggetti, ricavandolo in una sezione speciale di quello già tenuto per gli intermediari finanziari sotto la vigilanza dell'OAM (Organismo degli agenti e dei mediatori creditizi).

La formula suddetta consente la vigilanza di una *Authority*. Nel citato registro potranno iscriversi solo coloro che avranno preventivamente comunicato al Ministero dell'economia e delle finanze l'intenzione di iniziare le attività descritte.

Il Ministero trasmetterà poi alla Guardia di Finanza i dati e le informazioni raccolte che le renderà disponibili, su richiesta, alla Polizia Postale. In Italia, l'Agenzia delle entrate ha attuato encomiabili tentativi "definitori", in occasione delle opzioni da dettare ai possessori per la tassazione dei proventi derivanti dalla negoziazione.

Per quanto riguarda i rapporti con gli utilizzatori, la Banca d'Italia è intervenuta con due importanti raccomandazioni:

- la prima, del 30 gennaio 2015;
- la seconda, più recente, del 19 marzo 2018.

Quest'ultima, in particolare, ha ripreso l'avviso pubblicato in pari data da ESMA (Autorità Europea degli Strumenti finanziari e dei mercati), ABE (Autorità Bancaria Europea) e IEOPA (Istituto Etico per l'Osservazione e la Promozione degli Appalti) - le tre autorità di vigilanza Ue su mercati e intermediari - sui rischi delle valute virtuali, per i risparmiatori, tra i quali vanno necessariamente ricordati in questa sede:

- mancanza di trasparenza sui prezzi;
- assenza di opzioni di uscita;
- interruzioni delle operazioni;
- informazioni fuorvianti;
- inidoneità delle valute virtuali per scopi previdenziali e di investimento;
- rischio di volatilità estrema e di bolle speculative;
- assenza di protezione.

Relativamente a questo ultimo aspetto, devo segnalare un interessante Parere del Consiglio Nazionale del Notariato, pubblicato sul sito di categoria come "Quesito antiriciclaggio n. 3/2018/B, intitolato *Compravendita di immobile-Pagamento del prezzo in Bitcoin.*

GAGLIARDUCCI, in *Criptovalute: l'Europa le riconosce ufficialmente*, pubblicato il 13 luglio 2018 su www.money.it, l'Autrice scrive che in virtù della già analizzata (qui) V Direttiva Ue contro il riciclaggio, si legittimano le valute in discorso. Al contrario, credo, le valute virtuali non diventino *ipso facto* (e non *ipso iure*) "moneta riconosciuta" (mia l'affermazione), bensì i loro *traders* diventino "sorvegliati speciali".

Il Notariato ha voluto studiare gli effetti della transazione sulle limitazioni al contante di cui alla normativa antiriciclaggio.

Vanno riportate di sicuro due statuizioni importanti contenute nel Documento *de quo*:

- "i sistemi di accesso informatici, senza eccezioni, non si fondano sul concetto di identificazione, bensì sulla mera verifica di credenziali informatiche[16]; la differenza, soprattutto ai fini della normativa antiriciclaggio, non è di poco conto.

L'utilizzo di un sistema informatico non può mai garantire, pertanto, l'identità del soggetto che effettua un accesso";

- "ne deriva che (...) il tracciamento, meramente informatico, potrebbe essere del tutto ininfluente ai fini della normativa che ci occupa".

Ciò detto, giustamente si conclude che il Notaio non può assistere alla *traditio* del mezzo di pagamento, requisito essenziale dell'atto prima di tutto (in uno con l'indicazione analitica dei mezzi di pagamento), ma poi dell'applicazione dei criteri antiriciclaggio.

Che il (così definito) "contante digitale" non può paragonarsi a quello reale.

Concludo allora confermando le mie ipotesi sulla mancata ricostruibilità - al momento - della natura giuridica della fattispecie "*criptocurrencies*".

Solo un "baratto" potrebbe forse oggi aiutarci a connotare le operazioni di trasferimento di detti "oggetti" all'interno di un sistema che, come abbiamo visto, è chiuso e "autoreferenziale".

L'esempio della compravendita commerciale è emblematico del riconoscimento circa la non contemporaneità del pagamento e della consegna del bene.

3. Il finanziamento del terrorismo con criptovalute

Per quanto attiene ai profili problematici delle criptovalute, l'utilizzo da parte delle mafie e dei terroristi è indubbiamente al primo posto.

Le investigazioni sono difficili, e si orientano sia sull'analisi delle transazioni attraverso i registri, sia sulle segnalazioni degli intermediari finanziari delle FIU (*Financial Intelligence Units*) o autorità di settore.

(16) Viene preliminarmente ricordato nella nota (pag. 3) che nel registro resta sì traccia della transazione in bitcoin, ma di un ignoto detentore che detiene una chiave privata, corrispondente ad una data chiave pubblica, sia come venditore che compratore.

Oltre alle ricerche su fonti aperte[17], l'utilizzo di programmi appositi sulla *blockchain* è consigliato dagli esperti.

In particolare, il terrorismo islamico ha mostrato di saper sfruttare al meglio le innovazioni tecnologiche e digitali, tanto che utilizza i bitcoin per finanziare tuttora le proprie attività e il reclutamento degli adepti[18].

Va ricordato che non esiste a tutt'oggi una definizione univocamente accettata di "finanziamento del terrorismo", ma analizzando il fenomeno emerge che si tratta di un processo di raccolta, accumulo, movimentazione di denaro ottenuto attraverso mezzi leciti o illeciti per scopi terroristici, o per supportare la struttura logistica di una organizzazione terroristica.

Si distinguono in fonti "apparentemente lecite", quali le rimesse che gli emigrati fanno giungere nei Paesi di origine per il sostentamento dei propri familiari; gli utili e i profitti derivanti dalle attività delle piccole e medie imprese operanti in vari settori economici; le liberalità e le donazioni versati dai membri della comunità islamica (di queste donazioni è stato rilevato un uso distorto da parti di alcuni enti quali *Non-governmental Organization* e *Non-profit Organization*); lo sfruttamento di sussidi statali.

Le fonti illecite più sfruttate invece risultano essere:

- il traffico di sostanze stupefacenti;
- il traffico di armi;
- il traffico di petrolio e di risorse naturali;
- il traffico di beni culturali;
- il racket e le estorsioni;
- i furti e le rapine.

Il potenziale utilizzo di bitcoin quale strumento per il finanziamento del terrorismo è supportato da una intensa attività di propaganda di taluni gruppi.

Sono state create pagine *web* in cui sono inseriti inviti a donare bitcoin segnalando l'indirizzo del *wallet* verso il quale inviare il denaro, oltre a un breve messaggio di propaganda, che spesso si accompagna a richieste di moneta.

---

(17) Interessanti profili su queste ultime sono contenuti nello studio di Benjamin Brown, *Tracing a jihadi cell, kidnappers and scammer using the blockchain: an open source investigation*, pubblicato il 18 giugno 2018 sul sito www.medium.com.
A livello di inchiesta, si segnalano, su tutti, due interessanti studi: A. TORCHIA, B. VIZCAINO, *Criptocurrency traders use old gold in drive to draw Islamic investors*, Reuters, 8 aprile 2018; Y. J. FANUSIE, T. ROBINSON, *Bitcoin Laundering*, Elliptic, Center on Sanctions & Illicit Finance, 12 gennaio 2018.

(18) Cfr. R. MUGAVERO, R. RAZZANTE, *Terrorismo e nuove tecnologie*, Pacini Editori, 2016, pagg. 51-60.

Nell'ambito di questo nuovo "mercato", Autorità e investigatori non possono lasciare "libertà di azione" che consenta ai suoi fruitori di operare in un contesto privo di regole giuridiche ed economiche ben codificate.