Mediterranean Insecurity

Approfondimenti sul terrorismo

LE CRIPTOVALUTE COME STRUMENTO DI RICICLAGGIO DI CAPITALI ILLECITI DA PARTE DELLE ORGANIZZAZIONI TERRORISTICHE

Giulia Maria Mainardi

(tesi Master in "Geopolitica della sicurezza", Università degli Studi Niccolò Cusano UNICUSANO – a.a. 2018-2019 – relatore Prof. Laura Quadarella Sanfelice di Monteforte)

ANALISI DI UN FENOMENO

"Segui il denaro e troverai la mafia"
Giovani Falcone

ANALISI DI UN FENOMENO

1- Introduzione

Nonostante il concetto di terrorismo internazionale non abbia ancora trovato una definizione universalmente condivisa, i principali Organismi Internazionali hanno ormai da anni messo in campo strumenti di lotta a tale fenomeno, dimostrando come tale necessità si condivisa a livello planetario.

La lotta al terrorismo internazionale coinvolge infatti sia il Consiglio di Sicurezza che l'Assemblea Generale delle Nazioni Unite, e ovviamente anche la NATO, che a seguito della stipula della Convenzione di New York del 1999, del Trattato di Pratica di Mare e del Vertice di Praga (entrambi del 2002) ha introdotto nell'Alleanza il concetto di "*combined joint task force*", dando vita a comandi interforze internazionali.

Anche l'Unione europea ha tra le proprie priorità la lotta al terrorismo internazionale, e ha formalizzato i propri impegni in tale ambito con i Regolamenti CE 467/2001, 2580/2001, 881/2002, 370/2003 e 561/2003.

In Italia infine, le leggi 415, 431 e 438 del 2001 e la legge 7 del 2003 hanno contributo a definire e regolare il fenomeno, uniformandosi ai dettami europei.

Fondamentale, in quest'attività di individuazione e contrasto al terrorismo internazionale, è individuare i gruppi terroristici e collegarli con gli stati e i gruppi malavitosi che li sostengono finanziariamente attraverso il riciclaggio di capitali illeciti.

Cosa si intende dunque esattamente per riciclaggio di capitali illeciti?

2- Definizione di "riciclaggio di capitali illeciti"

Il termine riciclaggio (in inglese "*money laundering*") ha origine giornalistica ed è diventato di uso comune in tempi abbastanza recenti, per poi essere introdotto anche nel linguaggio diplomatico e giuridico, fino ad essere inserito anche nei testi di convenzioni e di altri strumenti internazionali.

Dal punto di vista meramente semantico, il termine *money laundering* sembra riferirsi alla consuetudine dei mafiosi americani degli anni '20 di comprare e gestire catene di lavanderie con i proventi delle attività illecite allora utilizzate (gioco d'azzardo, contrabbando di alcolici, prostituzione).

Non ci sono dubbi sul fatto che, in linea teorica, ogni modalità di trasferimento di valori, finanziari o reali che siano, si possa utilizzare a scopo di riciclaggio, mentre non è ancora universalmente condiviso cosa debba intendersi per "riciclaggio di capitali", ovvero quali tipi di attività illecite vadano incluse in questa definizione.

È ancora molto discusso, ad esempio, se anche il riciclaggio di denaro frutto di evasione fiscale debba essere incluso, considerato che i proventi dei reati fiscali, in linea di principio, non indicano un presupposto di reciclaggio, poiché tale denaro è frutto di attività illecite, ma non criminali.

Non è una questione di poco conto, poiché spesso il suddetto ragionamento viene utilizzato quale pretesto per negare collaborazione in indagini internazionali, adducendo una minore "pericolosità sociale" dell'evasione rispetto ad altri reati perpetrati dalla criminalità organizzata.

Il dibattito è molto acceso ed è rafforzato dal fatto che in molti paesi l'illecito tributario è spesso considerato avere spessore meramente amministrativo e non penale, e ciò permette l'opposizione del segreto bancario alle indagini delle autorità giudiziarie straniere.

3- Criminalità organizzata e riciclaggio

Il Piano d'Azione contro la Criminalità Transnazionale, così come redatto durante la Conferenza Ministeriale Mondiale di Napoli del 1994, ha messo in luce la relazione tra riciclaggio e criminalità organizzata, e ha dimostrato come tale riciclaggio non sia meramente un'attività funzionale alle associazioni criminali, ma ne sia diventato un elemento caratterizzante e strutturale.

Le organizzazioni criminali infatti, nel perseguire i propri obiettivi di profitto e auto sostentamento, tendono organizzare la loro attività secondo il seguente schema:

a - ricerca di fondi mediante attività (sia legali che illegali);

b – riciclaggio del denaro proveniente da tali attività, se illegali;

c - reinvestimento dei fondi "ripuliti";

Si può pertanto definire come riciclaggio l'insieme delle attività criminali atte a dissimulare la provenienza illecita dei beni, al fine di permettere il godimento dei frutti delle attività illecite commesse e il loro reinvestimento in attività lecite.

Il fenomeno dl riciclaggio si articola generalmente nelle seguenti fasi:

a - collocamento (*placement*);

b - stratificazione (*layering*);

c - integrazione (*integration*).

a – Il collocamento consiste nell'introduzione del denaro contante, frutto delle più svariate attività illecite, nel circuito bancario, mediante la sua conversione in altri strumenti di pagamento.

La fase di collocamento è senz'altro la più rischiosa per l'operatore del reciclaggio, poiché le possibilità di intercettazione da parte delle autorità inquirenti sono molto alte. Si tratta infatti di operazioni particolarmente laboriose, e le tecniche utilizzate tendono a essere tanto meno efficienti quanto maggiore è la somma di denaro contante da dover ripulire.

b -La stratificazione consiste in un complesso di manovre finanziarie e contabili, la cui complessità aumenta all'aumentare delle somme interessate, spesso svolte su scala internazionale, effettuate al fine di far perdere le tracce della provenienza (cd *paper trail*) e a occultare ogni legame tra denaro e attività illecite che lo hanno procurato.

c – La fase di integrazione consiste infine nel reinvestimento dei capitali illeciti in attività legali. In questa fase le autorità inquirenti perdono di fatto il potere di contrastare il fenomeno, per l'impossibilità di fatto, arrivati a questo punto, di distinguere i capitali aventi origine lecita da quelli con origine illegale. Un classico esempio di integrazione si ha nel momento in cui viene utilizzata la tecnica del "*commingling funds*", ovvero la copertura di un'attività legittima per

confondere la provenienza dei capitali; in tal caso ogni attività di *layering* successiva potrebbe venir posta in essere come mera ulteriore precauzione al fine di garantire una sufficiente separazione tra il denaro e il reato presupposto, ma agli effetti della sostanza i capitali sarebbero già stati reinvestiti.

Ovviamente nella realtà quotidiana i tre summenzionati stadi non si realizzano sempre in successione precisa e meccanica, ma spesso presentano gradi di complessità variabili, o ancora possono risultare confusi in un'unica operazione, come si verifica nel tipico caso della conversione di contanti in oro, operazione che consente a chi recicla di soddisfare contemporaneamente tre esigenze fondamentali:

- liberarsi delle banconote;

- occultarne l'origine

- effettuare un investimento.

A conferma di ciò, la Corte di Cassazione si è espressa in più occasioni, esplicitando come essendo il denaro di per sé fungibile, non si può dubitare che quando si deposita in banca denaro di provenienza illecita, si realizzi di fatto la sostituzione dello stesso in quanto la banca risulta obbligata a restituire al depositante la medesima quantità di denaro che questo ha versato.[1]

L'azione di riciclaggio del denaro consente alle organizzazioni criminali di trasformare il loro enorme potere di acquisto potenziale - non spendibile direttamente in consumi o investimenti, in quanto frutto di attività illegali - in effettivo potere d'acquisto.

I costi che un'organizzazione criminale deve affrontare sono senza dubbio molto alti, poiché alto è il rischio di individuazione da parte delle forze dell'ordine.

Tali costi sono dovuti a tre, ineliminabili, fattori:

- la commissione versata agli intermediari (mediamente il 10-15%);

- le spese organizzative legate all'accesso al mercato del reciclaggio;

[1] (Cass., sez II, 15 aprile 1996), "*in tema di riciclaggio, stante la fungibilità del denaro, non può dubitarsi che il deposito in banca di denaro sporco realizzi automaticamente la sostituzione di esso, essendo la banca obbligata a restituire al depositante la stessa quantità di denaro depositato*" e (Cass., sez. II, 2 febbraio 1983), "*il riciclaggio può realizzarsi con una sola azione, comprendente uno o più atti o fatti unitariamente collegati e susseguentesi in un breve spazio di tempo, ovvero con più distinte azioni",*

- i costi da calcolarsi in relazione al rischio di sequestro dei beni da parte delle forze dell'ordine.

Questi costi, secondo uno studio di Pierre Kopp[2] contribuiscono a definire una "*naturale tendenza all'inefficienza*" delle organizzazioni criminali, che le porterebbero a mantenersi al di sotto delle dimensioni ottimali, a contenere la propria presenza nei mercati di attività e a crearsi un punto di ancoraggio locale, spesso sulla base della propria appartenenza etnica.

È in questo stadio che si rende necessario un approfondimento sulle opportunità offerte dall'internet banking, dall'e-commerce e dai nuovi mezzi di pagamento in generale.

4- Tecniche di riciclaggio

L'esperienza sul campo delle forze dell'ordine e le statistiche giudiziarie di respiro internazionale hanno individuato un'ampia categoria di strumenti e tecniche che possono definire e integrare gli schemi di riciclaggio di fondi di provenienza illecita.

È a tal proposito importante distinguere tra:

- tecnica: intesa come singola operazione del più complesso processo di riciclaggio di fondi illeciti;

- schema: identificante una serie di precisi procedimenti applicati al fine di ripulire una transazione finanziaria;

- meccanismo: inteso come attività commerciale o istituzione finanziaria potenzialmente idonea a consentire dei processi di riciclaggio.

Un meccanismo si colloca pertanto a metà strada tra una tecnica e uno schema: il riciclaggio di fondi illeciti per mezzo di un ufficio di cambio (meccanismo) può ad esempio comportare l'applicazione di diverse tecniche, ma costituisce al contempo un mero elemento di uno schema molto più complesso.

Recenti studi hanno individuato un trend costante nell'evoluzione dei meccanismi di riciclaggio, che sembrerebbe svilupparsi seguendo le seguenti fasi:

[2] Kopp, Pierre – "L'analyse économique des organisations criminelles" in "vivre avec les drogues: régulations, politiques, marchées, usages" Collection Communications n° 62, Seuil, Paris, 1996.

- riciclaggio di tipo monetario (anni ’60-’70): basato per lo più sulla movimentazione di denaro contante;

- riciclaggio di tipo bancario (anni ’80): incentivato dalla drastica diminuzione delle restrizioni alla circolazione di capitali e dall’abbondanza di strumenti e servizi finanziari sul mercato;

- riciclaggio di tipo finanziario (anni ’90): messo in campo grazie all’intermediazione di società finanziarie.

Il passaggio dal riciclaggio monetario a quello finanziario segna altresì l’avvento del riciclaggio statico, ovvero di un sempre minor ricorso al contante, sostituito da titoli cartolari usati a titolo di garanzia per chiedere prestiti nel circuito bancario, senza più la necessità di movimentare contante, e riducendo quindi drasticamente il rischio di imbattersi nei controlli delle autorità inquirenti.

Questa evoluzione rientra nel più generale fenomeno del passaggio dal cd *bulk cash* all’*asset laundering*, con la conseguente riorganizzazione dell’intera strategia anti rociclaggio, che si basava nel passato sulla movimentazione di contante per risalire all’origine e alla portata delle attività criminali che finanziavano tale flusso.

La movimentazione di grandi quantità di contante continua ad essere il tallone d’Achille delle organizzazioni criminali che gestiscono attività dai grandi flussi di denaro, come ad esempio lo spaccio di stupefacenti.

Le difficoltà che affrontano le associazioni criminali dedite ai suddetti traffici, soprattutto in fase *placement*, sono notevoli: devono convertire massicce quantità di contante in forme di pagamento anonime e facilmente gestibili, non devono lasciare tracce che possano condurre al reato da cui proviene il denaro e, cosa più difficile tra tutte, devono trovare un modo per tenere monitorato il denaro, in modo che chi è coinvolto parte dell’operazione di riciclaggio non se lo intaschi.

Un tale groviglio di problemi si rivela spesso insuperabile, come testimoniano numerosi successi della polizia. Un esempio su tutti: durante l’operazione Green Ice, le forze dell’ordine hanno rinvenuto un magazzino contenente più di 20 metri cubi di denaro (corrispondenti a circa 5,6 milioni di sterline inglesi), che riflettono molto chiaramente i problemi dell’immettere denaro sporco nel flusso legale dell’economia.

Le organizzazioni criminali, consapevoli delle suddette difficoltà, cercano di effettuare quanto prima l’operazione di *refining*, cioè la conversione di banconote di piccolo taglio in banconote di taglio maggiore.

Da qualche tempo, tuttavia, si registra un aumento di transazioni dal contante ad altri metodi di pagamento (ad esempio assegni o carte di credito): negli Stati Uniti, ad esempio, *l'Inland Revenue Service* ha calcolato che circa il 25 - 30% circa delle transazioni criminali vengono regolate con assegno o giroconto.

L'*Office of Financiale Enforcement* degli Stati Uniti ha individuato le caratteristiche che rendono appetibile alla malavita uno strumento o un ambiente finanziario:

- rigido segreto bancario;
- conti correnti anonimi/cifrati;
- abbondanza di strumenti al portatore;
- scarsi obblighi identificativi;
- semplicità nell'acquisire/registrare società;
- scarsità di elaborazioni statistiche;
- labili controlli bancari;
- accesso a sistemi bancari *off shore*;
- ampia accettazione di dollari statunitensi;
- limitate abilità investigative delle forze inquirenti;

Analizzando ora come nella realtà vengono messe in campo alcune delle tecniche più diffuse nel riciclaggio su scala mondiale, è noto come le scelte delle organizzazioni criminali per quanto riguarda il riciclaggio siano condizionate dai seguenti fattori.

- la realtà economica in cui operano, in cui cercano di operare senza alterarne gli equilibri, ma rendersi il più possibile invisibili;
- l'ordine di grandezza dei fondi illeciti da ripulire;
- la frequenza la periodicità con cui vengono processate le somme da reciclare;
- l'eventuale grado di complicità delle istituzioni;
- l'orizzonte temporale di impiego dei beni (investimenti di breve, medio o lungo termine).

Ciò considerato, le principali tecniche per riciclare denaro proveniente da attività illecite, attualmente conosciute, si possono riassumere nelle seguenti categorie:

a - contrabbando (*smuggling*): degli operatori (cd. spalloni) sono incaricati di trasportare il denaro da uno Stato all'altro a mano o con le medesime modalità con cui viene trasportata la droga: navi, aerei, camion ecc. Questa tecnica è estremamente diffusa per far uscire denaro contante dagli Stati Uniti e farlo giungere nei paradisi caraibici.

b - *structuring/smurfing*: ingenti quantità di denaro contante vengono frazionate e disperse in un'enorme quantità di micro operazioni finanziarie, rigorosamente di ammontare inferiore alla soglia di dichiarazione obbligatoria. Queste transazioni sono effettuate da persone che operano per conto dell'organizzazione criminale all'interno di varie istituzioni finanziarie in maniera contestuale e in un breve lasso di tempo, in modo che ogni giorno, in ogni istituto bancario, non vengano superati i limiti di volta in volta fissati dalle normative antireciclaggio. In un secondo momento, tutti le piccole transazioni di denaro così create vengono convogliate verso un unico conto di accentramento, spesso tenuto in un paradiso fiscale.

c - *commingling illicit proceeds with licit funds*: si tratta probabilmente della tecnica più efficace, poiché costringe le autorità inquirenti aa enormi es estenuanti indagini per riuscire ad individuare la provenienza illecita di capitali infiltrati in transazioni perfettamente legali, di natura sia commerciale che finanziaria.

c – ricorso all'istituto valutario della compensazione: ciò avviene quando, in conti correnti in euro su cui venivano accreditate somme di origine illecita di cui viene richiesto il trasferimento estero, che però alla fine non viene realizzato in quanto vengono l'ammontare viene compensato con rimesse di ari valore provenienti da migranti.

d - utilizzo di casinò: nelle tecniche più elementari, con l'acquisto di *fiches* e la conversione poi in contanti (non necessariamente contestuale bensì differibile e anche geograficamente trasferibile grazie agli accordi di mutuo riconoscimento delle *fiches* tra le maggiori case da gioco del mondo). Ciò permette così di varcare i confini nazionali con somme anche ingenti sotto forma di *fiches*, eludendo i controlli delle autorità doganali. I maggiori casinò permettono anche di convertire le *fiches* in assegni e di trasferire poi tali assegni ad altre sedi (oltre frontiera) del medesimo casinò o addirittura presso banche straniere.

e - sfruttamento del mercato creditizio: si riscontrano sempre più spesso connivenze tra criminalità organizzata e istituzioni finanziarie, il cui staff permette e copre le attività di riciclaggio dei capitali illeciti, scavalcando deliberatamente i dispositivi di

prevenzione anti-riciclaggio[3]. Siffatte operazioni si svolgono in genere tramite l'utilizzo di conti nominativi intestati a prestanome. Si riscontrano infatti spesso finte richieste di prestiti personali, il cui rimborso è previsto in contanti, spesso per importi di modesta entità (ovviamente per non destare sospetto nel caso in cui tali operazioni vengano attribuite a clienti qualunque) ma ripetute sistematicamente su molti diversi conti correnti, così da trasferire complessivamente cifre estremante rilevanti. Si noti altresì la tecnica consistente nell'interposizione di soggetti tra operatori di paesi diversi, come nel caso di società finanziarie straniere che trasferiscono a istituti di altri paesi grandi somme sulla base di norme che regolano il trasferimento di denaro e gli investimenti in paesi esteri.

5- Bitcoin e blockchain: cosa sono e come funzionano

I bitcoin[4] (BTC) sono una moneta virtuale, decentralizzata, parzialmente anonima basata sulla crittografia e sulla tecnologia *peer-to-peer*.

Rientrano nella macro categoria delle criptovalute, e più precisamente nella categoria delle criptovalute *open-flow*, ovvero utilizzabili anche in ambienti diversi da quello virtuale, in quanto possono essere convertite in denaro avente corso legale.

I bitcoin sono un'entità virtuale: esistono solo nel mondo digitale e non sono stampati né distribuiti in forma fisica.

Sono generati da un software open source, attualmente disponibile sulla piattaforma web Github. Tale software può generare un numero predeterminato di bitcoin ogni anno, secondo un ordine decrescente: ogni anno infatti il numero di nuovi bitcoin in circolazione è minore di quello dell'anno precedente. Il numero massimo di bitcoin che potrà circolare sarà pari a 21 milioni nel 2140. Il processo di distribuzione di nuovi bitcoin si chiama *mining*.

Per mezzo di questo singolare sistema, il software elargisce nuovi bitcoin agli richiedenti in rete, che utilizzano la loro potenza di calcolo per risolvere l'algoritmo

3 Righetti, Renato – "Tecniche di occultamento della ricchezza da parte delle organizzazioni criminali" in Violante, Luciano – I soldi della mafia: rapporto '98, Laterza, Bari, 1998, p. 71.

4 Per convenzione, mentre il termine "bitcoin", scritto in minuscolo, indica la moneta virtuale, il termine "Bitcoin", con l'iniziale maiuscola, indica il protocollo, ovvero la tecnologia e la rete utilizzata per generare e trasferire moneta.

crittografico posto a base del sistema. Questi calcoli matematici hanno lo scopo di convalidare le transazioni. Ogni transazione di bitcoin necessita infatti di essere convalidata da almeno il 50% più uno dei nodi della catena. I *miner* vengono ricompensati per il loro servizio attraverso nuovi bitcoin. Siffatto sistema garantisce anche la protezione della struttura dagli attacchi informatici. Se si volesse rubare un bitcoin infatti, si dovrebbero *hackerare* contemporaneamente il 50% più uno dei computer connessi, ma ciò non è possibile, poiché nessun processore ha in linea teorica una potenza sufficiente per reggere tale operazione, e anche perché il costo di un singolo bitcoin non ripagherebbe la spesa necessaria ad un'attività così dispendiosa.

In alternativa al *mining*, gli utenti possono acquistare i bitcoin da altri utenti; sono infatti presenti numerose piattaforme online ove è possibile comprare bitcoin in cambio delle principali valute nazionali.

Una volta entrati in possesso di bitcoin, gli utenti vengono dotati di un portafoglio elettronico (cd. *wallet*). Tali portafogli elettronici non sono altro che dei semplici file di dati, dove si trovano le coordinate dell'account, le transazioni registrate e le chiavi crittografiche da usare per spendere o trasferire la moneta.

La chiave pubblica è una stringa alfanumerica che identifica il *wallet* (come un qualsiasi IBAN bancario, inizia sempre con il numero 1 e contiene 34 caratteri, ed è composta da numeri e lettere). Tale chiave serve sia per trasferire che per ricevere bitcoin, perciò se un utente vuole trasferire denaro a un terzo, deve conoscere la sua chiave pubblica.

La chiave privata è invece una sorta di password, e non deve pertanto essere comunicata a terzi. Essa serve per firmare le transazioni, perciò quando un utente invia bitcoin ad un terzo, usa la sua chiave privata per dimostrare di avere la titolarità della moneta che vuole trasferire.

Come anticipato, ciascun proprietario può trasferire bitcoin, firmando, con una chiave privata, la transazione precedente e l'indirizzo del proprietario successivo. Colui che riceve un pagamento, viceversa, deve verificare le firme digitali per validare la catena di proprietà.

Bitcoin è comunemente definito il contante di internet. Come il denaro contante infatti, può essere trasferito a chiunque senza intermediari e le sue transazioni sono irreversibili e anonime.

Attualmente esistono tante strutture, sia fisiche che in internet, che accettano i pagamenti in bitcoin. Nel 2015 il numero di commercianti che accettavano bitcoin era

superiore a 100.000. Esistono anche bancomat per bitcoin, strutture in cui introdurre denaro contante per ottenere in cambio l'accredito di moneta virtuale: negli USA solo il gruppo Coinatmradar possiede più di 500 bancomat.

6- Il carattere (quasi) anonimo dei bitcoin

Comunemente si sostiene che i bitcoin garantiscano l'anonimato ai suoi utilizzatori: Tale affermazione non è corretta.

Tutte le transazioni in bitcoin infatti sono pubbliche, in quanto contenute in un database distribuito liberamente accessibile. Chiunque può controllare chi ha ceduto un determinato bitcoin a chi, e chiunque può scoprire anche il report storico di ogni transazione.

Ovviamente, non tutto è pubblico. Infatti, mentre le transazioni sono pubbliche, l'indirizzo a cui è collegato un determinato portafoglio dei bitcoin è anonimo. E' un mero elenco di cifre e non fornisce alcuna indicazione espressa sull'identificazione del suo proprietario. Di conseguenza, se in un determinato portafoglio c'è un quantitativo sospetto dei bitcoin, non è possibile in prima battuta identificare il proprietario, se si possiede solo l'indirizzo di riferimento.

Ma non è tutto. Il sistema infatti non esclude che l'utente anonimo possa esse comunque identificato in altro modo. Mediante tecniche di *digital forensic* è infatti possibile risalire a coloro che si celano dietro un determinato indirizzo. Una volta determinato l'utente anonimo, la piattaforma Bitcoin si rivela uno strumento incredibilmente trasparente, essendo in grado di fornire indicazioni precise su tutte le attività poste in essere da un determinato soggetto, come accaduto di recente nel caso di Silk Road.

Attualmente l'anonimato è molto limitato, perché la maggior parte dei bitcoin exchange internazionali richiede un'identificazione espressa degli autori di ogni transazione.

7- Blockhain: cos'è

Bitcoin rappresenta il primo esempio di applicazione su vasta scala della tecnologia blockchain[5]. In base ai trend previsti dal World Economic Forum, circa il 10% del PIL mondiale entro il 2025 proverrà da attività basate sui principi della blockchain[6].

La blockchain è un database distribuito, condiviso e crittografato che serve come repository pubblico informativo, irreversibile e incorruttibile. È una banca dati cronologica che raccoglie tutte le transazioni presenti sulla rete bitcoin. È composta da vari sottosistemi più piccoli, denominati blocchi: in ogni blocco sono memorizzate un certo numero di transazioni. Ogni blocco è collegato ad un blocco successivo, e questo ha l'effetto di creare una catena.

La blockchain, in virtù delle sue proprietà innovative, è stata recentemente oggetto di numerosi studi. Molti hanno infatti ipotizzato un suo eventuale utilizzo in ambiti diversi da quello monetario.

8- Altre monete virtuali

Il bitcoin non è l'unica moneta virtuale dell'attuale panorama informatico. Negli ultimi anni si è assistito ad un vero e proprio boom di criptovalute. Si parla comunemente di Alternative Coin (AltCoin) per identificare le varie monete virtuali alternative ai bitcoin (alcune di esse nate da una scissione avvenuta all'interno del protocollo Bitcoin).

La più nota alternativa a bitcoin è Litecoin. Si tratta di una criptovaluta peer-to-peer nata nel 2011 da Charles Lee, ex dipendente di Google. Litecoin è molto simile al bitcoin. Anche per Litecoin infatti la coniazione e la transazione della moneta avviene grazie a un protocollo open source decentralizzato, privo di alcuna autorità centrale. Come per bitcoin, anche le operazioni effettuate con i Litecoin sono registrate in una blockchain. Attualmente il maggior successo di Litecoin si registra in Europa, specialmente nei paesi BASSI, Repubblica Ceca, Finlandia e Russia.

Un'ulteriore moneta virtuale molto diffusa è Peercoin (PPCoin o PPCCC). È la terza criptovaluta più nota. Peercoin è ispirata al bitcoin, ma presenta molte differenze. Innanzitutto, una rete peer-to-peer gestisce le transazioni, i saldi e l'emissione di

[5] J. BONNEU, Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, in Ieee Security and Privacy, maggio 2015.
[6] Emanuele Florindi, Deep web e bitcoin, Vizi privati e pubbliche virtù della navigazione in rete, Imprimatur, Milano, 2018

Peercoin. I pagamenti vengono inviati agli indirizzi PPC, basati su firme digitali. Le transazioni sono registrate nella blockchain e ogni 10 minuti viene aggiunto un nuovo blocco[7].

Le monete vengono create con due modalità: con il mining (che al contrario di bitcoin riduce la sua difficoltà con il passare del tempo e con lo schema *proof of stake*. In questa ultima ipotesi, la rete attribuisce le monete in base alla partecipazione già posseduta. Se un utente detiene l'1% di token, guadagnerà l'1% della nuova moneta[8].

La principale innovazione di Peercoin è la sua bassa inflazione. Il programma è infatti progettato per maturare un'inflazione dell'1%, con un numero illimitato di monete generabili.

Molto simile a bitcoin è Ethereum. Si tratta di una piattaforma decentrata che gestisce contratti intelligenti. Queste applicazioni vengono eseguite su una blockchain personalizzata, che consente agli sviluppatori di creare mercati, archiviare registri di debiti o di promesse, spostare fondi e molte altre cose. Ethereum è anche un netword per lo scambio di valore monetario.

L'unità di conto del sistema è l'Ether (ETH). Essa è scambiata come una criptovaluta, ma viene anche utilizzata per pagare commissioni di transazione e servizi di calcolo sulla rete. Ogni attività del sistema prevede il pagamento di una commissione, chiamata gas. Nel 2016 Ethereum ha subito una scissione, attraverso cui è nata Ethereum Classic.

Anche Titcoin (TIT) rappresenta un progetto alternativo di cryptocurrency molto noto. Titcoin è una criptomoneta creata nel 2014. Si fonda sulla tecnologia peer-to-peer ed è dedicata al mercato dell'intrattenimento per adulti. I suoi punti di forza sono l'anonimato (necessario nel mercato in cui opera) e la velocità delle transazioni.

Le monete digitali negli ultimi anni nascono con frequenza quasi mensile. Recentemente una nuova moneta digitale è nata proprio all'interno della comunità bitcoin: si tratta di Bitcoin Cash, frutto di una scissione all'interno della comunità Bitcoin. Questa moneta è nata nel 2017 ed è stata distribuita gratuitamente a tutti i titolari di bitcoin. Non è ancora chiaro che effetto produrrà sui mercati.

---

[7] Davide Capoti, Bitcoin revolution. La moneta digitale alla conquista del mondo, Hoepli, Milano, 2017

[8] Banca d'Italia (2015), "Avvertenza sull'utilizzo delle cosiddette valute virtuali", disponibile all'indirizzo: https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf

Recentemente sta riscontrando molto successo Ripple (XRP), creata nel 2011. Come per bitcoin, anche Ripple opera su una piattaforma decentralizzata open source. Al contrario di bitcoin però presenta registri di transazioni (cd. ledger) che permettono di monitorare gli scambi e completare e transazioni entro pochissimi secondi. Non adotta alcun sistema proof-to-work, quindi le monete non devono essere minate ma sono state già rilasciate tutte dal protocollo; i nodi della rete non hanno poteri paritari ma sono divisi in *monitoring* e *validating*, le transazioni sono irreversibili e non sono previsti costi di transazione. Attualmente Ripple è molto utilizzato dagli istituti bancari, come alternativa evoluta dello Swift[9]

Molto diffusa è anche Monero. Si tratta di una criptovaluta creata nel 2014 da un utente anonimo nel forum Bitcointalk. Ultilizza il protocollo Cryptonight (un derivato di CryptoNote), che consente una gestione decentralizzata delle transazioni mediante un database accessibile solo ai protagonisti delle varie operazioni. Essa garantisce quindi un elevato tasso di anonimia ai propri utenti. È inoltre fungibile, essendo ogni unità di Monero uguale alle altre.

Estremamente innovativa è anche IOTA, criptovaluta nata nel 2015. Questa moneta è già distribuita e non è minabile. Il progetto non sfrutta la blockchain ma una nuova struttura che prevede "fili paralleli". Ciò garantisce l'assenza di costi di transazione.

9- Il riciclaggio mediante bitcoin

È opinione di numerosi esperti che il riciclaggio rappresenti il principale rischio relativo all'uso dei bitcoin. È infatti estremamente facile che operatori legali alle organizzazioni criminali acquistino bitcoin con denaro di provenienza illecita, sfruttandone poi peculiarità operative per ripulire il denaro sporco[10].

Nel Rapporto 2013 dell'Unità di Informazione finanziaria per l'Italia (UIF)[11] la Banca d'Italia ha annunciato che sono in corso approfondimenti sul potenziale rischio di riciclaggio e supporto alle attività terroristiche attraverso i bitcoin. Il direttore dell'UIF, in particolare, ha dichiarato che l'urgenza di un'analisi più approfondita è confermata

[9] F. SANTELLI, Da Ripple a Cash, ecco le valute virtuali che sfidano il Bitcoin, in La Repubblica.it, 3 gennaio 2018.
[10] Gaspare Jucan Sicignano, Bitcoin e riciclaggio, Giappicchelli, Torino, 2019
[11] Rapporto UIF 2013, disponibile a https://uif.bancaditalia.it/pubblicazioni/rapporto-annuale/2014/index.html

dall'analisi di alcune segnalazioni riguardanti transazioni internazionali che destano sospetti.

Anche l'Autorità Bancaria Europea (EBA), unitamente alla Banca Centrale d Francoforte e all'Autorità di vigilanza sui mercati (ESMA) ha evidenziato i rischi delle monete virtuali.

Dello stesso avviso il Procuratore generale di Roma. Secondo il responsabile della Procura generale capitolina, i bitcoin non offrono chiarezza nella tracciabilità e possono essere strumento per il riciclaggio di denaro, per il finanziamento del terrorismo e delle mafie e per i traffici illeciti. In caso di trasferimento dei bitcoin infatti, non vi sarebbe la garanzia di poter individuare l'identità reale delle persone coinvolte.

I bitcoin rappresenterebbero uno strumento per criminali, terroristi, finanzieri e evasori secondo il Gruppo d'Azione Finanziaria Internazionale (Gafi), l'organismo intergovernativo indipendente che sviluppa e promuove politiche finalizzate a proteggere il sistema finanziario globale contro il riciclaggio, il finanziamento del terrorismo e la proliferazione delle armi.

Anche la Direzione investigativa antimafia e la Guardia di Finanza hanno lanciato l'allarme sui rischi connessi all'utilizzo dei *bitcoin.*

10- Internet e reciclaggio

Il fenomeno del riciclaggio di capitali è dato da quell'insieme di attività di re-immissione di denaro, avente origine in attività criminali, nel circuito dell'economia legale.

Nell'economia contemporanea, le operazioni di riciclaggio di denaro sporco hanno ricadute pesanti sull'economia, in quanto ne modificano la libertà di concorrenza, il fisiologico funzionamento dei mercati e i meccanismi di allocazione delle risorse. Si stima che l'impatto di tali operazioni sull'economia italiana oscilli tra l'1,7 e il 12 per cento del PIL.

Le attività di *money laundering* si sono costantemente evolute nel tempo, addivenendo a tecniche estremamente sofisticate, in parte favorite anche dalla globalizzazione dei mercati e dalle moderne tecnologie informatiche.

In tali dinamiche, Internet ha assunto un'importanza preminente e ha permesso di percorrere strade inedite da affiancare alle classiche strategie criminali.

Il web può infatti fungere da mero veicolo, il cui ruolo è quindi quello di sostituire il corriere fisico con un computer (fase di *placement)*, oppure può diventare il mezzo attraverso cui creare nuovi sistemi di reciclaggio.

Legislatore e autorità inquirenti devono pertanto possedere una conoscenza particolarmente approfondita di tali tecnologie, in modo da impedire che le organizzazioni criminali si muovano all'interno di territori di confine che si trovano nella normativa effettuando attività criminose nei fatti, ma difficilmente inquadrabili da un punto di vista giuridico e pertanto difficili da contrastare.

Quando si vogliono prevenire tali fattispecie occorre porre estrema attenzione va posta a quali strumenti di pagamento che possono essere utilizzati qualora si voglia porre in essere operazioni di natura finanziaria con lo scopo di riciclaggio. Tra l'altro l'industria dei servizi di pagamento in questi anni è stata caratterizzata da profondi mutamenti derivanti dall'utilizzo delle tecnologie informatiche e delle reti di dati. In questo contesto le criptovalute si configurano come un tassello importante nel delicato mosaico dei percorsi di evoluzione del settore. Questi infatti sono strumenti di pagamento che si caratterizzano per nuove funzionalità e per un rapido sviluppo che merita particolare attenzione.

Oggi è necessario che esse siano inquadrate all'interno della complessiva strategia di lotta al riciclaggio e al finanziamento del terrorismo. Per questo sorge l'esigenza di dotarsi delle competenze e degli strumenti necessari al fine di prevenirne e contrastarne gli utilizzi a fini criminali.

Questi innovativi mezzi di pagamento sono in effetti molto pericolosi in quanto possono configurarsi, in un numero svariato di casi, quali fattispecie di riciclaggio digitale a 360 gradi: le criptovalute infatti non rappresentano meramente uno strumento di placement, ma danno la possibilità di ideare complesse e sempre differenti strategie riguardanti tutte le varie fasi di reciclaggio. Tutto ciò rende particolarmente complessa l'attività di contrasto al riciclaggio del denaro sporco posta in essere dalle autorità competenti.

Un breve cenno al concetto di deep web sarà utile a una migliore comprensione del fenomeno, in quanto questo luogo virtuale rappresenta il contesto ideale dove sviluppare e implementare le nuove modalità di riciclaggio (anche per mezzo delle criptovalute), nonché per tutta una serie di nuovi reati informatici.

Con il neologismo di deep web normalmente si individua quella parte della rete non immediatamente raggiungibile attraverso l'uso dei normali motori di ricerca internet. Dal deep web poi si distingue anche il dark web, (è un'altra sezione del web), che può essere navigato solo con l'ausilio di appositi strumenti di surfing. In particolare esistono browser specifici come TOR (the onion router). Si tratta in buona sostanza, di una sezione nascosta del deep web. Questa infatti include contenuti normalmente e volutamente tenuti nascosti alla massa dei navigatori. Grazie alla connessione di TOR, il navigatore attraversa 3 diversi nodi, scelti randomicamente dalla rete, prima di poter accedere all'indirizzo prescelto. Ognuno di questi nodi riconosce esclusivamente l'indirizzo da cui estrae i dati e quello a cui fornire i dati stessi. In questo modo è praticamente impossibile riconoscere il percorso completo della connessione. In questo modo TOR riesce a garantire agli utenti una navigazione realmente e questi di fatto non possono essere rintracciati.

Di per sé sia le criptovalute che il deep web non sono illegali come si è soliti supporre. All'interno di questa sezione della rete sono presenti numerosi indirizzi web assolutamente legali, ma non indicizzati dai più comuni motori di ricerca (ad esempio vi si trovano pagine e contenuti ad accesso riservato oppure non testuali). Quindi per averne accesso occorre essere in possesso di una password o del link relativo. In ogni caso la non tracciabilità della connessione e l'opacità dei contenuti favorisce l'utilizzo dello strumento per finalità illecite. Secondo stime di massima circa il 90 per cento dei siti presenti sul dark web sono in realtà piattaforme finalizzate ad attività illegali o immorali. Normalmente tali attività sono peraltro finanziate con criptovalute (tra cui spiccano Bitcoin, Monero e Darkcoin).

Proprio la caratteristica del deep web di risultare anonimo e poco trasparente alla normale navigazione favorisce un uso illegittimo offrendo particolare protezione alla identità degli utenti: l'uso delle criptovalute poi è ideale in questo senso in quanto non è facilmente tracciabile mancando obblighi informativi per le controparti delle transazioni. Si prestano pertanto magnificamente a traffici illeciti.

Sulle piattaforme disponibili sul dark web si scambiano normalmente droghe, beni di rubati, armi, materiale pedo-pornografico e ogni sorta di bene illegale, si finanziano attività connesse al terrorismo e a quei traffici associati al fenomeno denominato cybercrime: quali furto di identità e di dati sensibili, traffico di organi, attività ricattatorie, ecc. Tanto per fare un esempio, sul dark web si può acquistare Command and Control (C&C). Si tratta di un server per il controllo da remoto del malware. Normalmente viene impiegato per il furto di account. È stato stimato un volume

giornaliero di traffici illeciti pari a oltre 650.000 dollari nel 2014. A questo dato va aggiunto il volume dei traffici che si effettuano su non meno di 50 store online non identificati. Smantellare questo complesso sistema di mercato online appare come un compito estremamente arduo principalmente per due motivi:

- La natura prettamente anonima del dark web fa sì che sia difficile (in molti casi impossibile) risalire all'identità degli amministratori delle piattaforme dove si compiono atti illeciti;

- Spesso quando finalmente si riesce a chiudere una piattaforma ne sorge quasi immediatamente una analoga pronta a subentrare nel segmento di mercato lasciato scoperto da quella rimossa. Esemplare il famoso caso di Silk Road insegna. Appena il sito venne rimosso e il suo amministratore condannato sono immediatamente apparsi nel dark web siti del tutto analoghi che offrivano gli stessi servizi in termini di spaccio di droga e armi.

11- Strategie mediante Bitcoin

Il mercato dei Bitcoin, non prevede intermediari finanziari e le transazioni avvengono prevalentemente in forma anonima (gli utenti utilizzano nik). Tutto ciò indubbiamente ne favorisce l'utilizzo per attività illecite quali il riciclaggio. Questo anche perché viene meno quel soggetto (l'intermediario) che, nelle forme di pagamento tradizionali, sarebbe preposto a segnalare eventuali attività sospette alle autorità competenti. Inoltre il sistema delle valute virtuali opera su scala veramente mondiale ed è per questo molto più semplice nascondere e trasferire somme di denaro ovunque e con tempi di esecuzione estremamente rapidi rendendo così molto difficile stabilire esattamente l'origine del denaro.

I bitcoin ad esempio possono essere impiegati da criminali per trasformare il denaro sporco in moneta reale e pulita. In questi casi vengono poste in essere operazioni piuttosto complesse ed efficienti nel tentativo di occultare nascondere ogni traccia alle autorità inquirenti. Vengono spesso impiegati specifici software che modificano i parametri di geolocalizzazione consentendo all'utente di apparire come se operasse in un altro Paese. Le organizzazioni criminali sono in grado di trasferire denaro sporco da carte prepagate (di solito intestate a un prestanome) operando sulle piattaforme Bitcoin acquistando criptomoneta. Dopodiché la valuta virtuale acquisita viene trasferita su

diverse piattaforme effettuando molte operazioni con controparti sparse in tutto il mondo. Viene impiegato questo trucco per muovere notevoli quantità di denaro di provenienza illecita in modo del tutto anonimo trasferendolo ad esempio a società fittizie che provvedono a pulirlo e renderlo rintracciabile.

Nei paragrafi successivi verranno illustrati alcune fattispecie tra le più comuni riciclaggio mediante bitcoin. Di norma, queste attività puntano a nascondere la fonte dei capitali illeciti, nonché a nascondere il proprietario del wallet di Bitcoin. Tali metodologie sono state analizzate dalle autorità competenti per sviluppare soluzioni che fossero efficaci a ostacolare gli illeciti e a identificare il vero il vero proprietario del portafoglio Bitcoin[12].

12- Transazioni peer to peer

Si tratta di operazioni che coinvolgono direttamente due parti senza l'intervento di intermediario. Per i Bitcoins la piattaforma più diffusa è Local bitcoin. Questa fornisce la possibilità di negoziare la valuta virtuale grazie ad un meccanismo che sul suo sito coordina le vendite, senza che sia necessario prendere direttamente parte alla negoziazione. Local Bitcoins in pratica provvede a eseguire la modalità di trasferimento "originale" prevista dal protocollo Bitcoin. Qui però vengono applicate commissioni molto elevate che variano tra il 10 e il 15 per cento (contro il normale 1 o 2 per cento applicato dalle comuni piattaforme abilitate. Proprio l'onerosità commissionale potrebbe far sorgere sospetti di illecito. Si potrebbe infatti supporre trattarsi di una fase di *integration recycling*, che in ossia mirano giustificare da un punto di vista legale un'entrata (la commissione) che in realtà fa riferimento a un'attività di riciclaggio. Le commissioni di solito non sono fisse, proprio per evitare la possibilità di identificare uno schema di riciclaggio ricorrente da parte delle forze dell'ordine.

Tali attività negoziali consentono la conversione di una grande quantità di contante di provenienza criminale in bitcoin. Il meccanismo adottato in realtà non è molto complesso: tipicamente una operazione peer to peer è fatta di persona, due soggetti si incontrano, di norma in un luogo pubblico con connessione wifi, e realizzano uno scambio di bitcoin al tasso corrente più l'applicazione della commissione. Il venditore ottiene i riferimenti del wallet a cui trasferire criptomoneta dal buyer. Quando l'iscrizione del transfert è processata nella blockchain, egli riceve in pagamento la

[12] AA.VV., Bitcoin e criptovalute. Profili fiscali, giuridici e finanziari, Maggioli, Roma, 2018

valuta legale in contanti. Per queste negoziazioni, non vengono acquisite informazioni identificative delle parti e sulla provenienza dei fondi oggetto del trasferimento. Così facendo, il compratore riesce a trasferire denaro sporco nel sistema finanziario senza destare alcun sospetto nelle autorità antiriciclaggio. I trasferimenti peer to peer sono inoltre impiegati dai malviventi che in questa maniera ottengono bitcoin dalla vendita di beni e servizi di natura non legale sul dark web. Al fine di mantenere l'anonimato, spesso i soggetti criminali evitano le piattaforme di scambio dedicate e sfruttano questa modalità operativa e, per convertire rapidamente bitcoin prima che il tasso di cambio possa essere meno conveniente, pagano tranquillamente queste commissioni così elevate.

Oltre agli scambi condotti di persona, nel tempo sono stati sviluppati innovativi schemi peer to peer. Ad esempio, quando venditore e acquirente operano in luoghi diversi, questi ultimi possono effettuare il pagamento mediante un normale deposito di valuta nel conto corrente bancario del venditore, mediante un bonifico o un vaglia postale. Alcuni venditori hanno anche iniziato ad accettare pagamenti in gift card e trasferimenti attraverso PayPal. Si tratta di certo di metodi più rischiosi; a tal proposito, Local Bitcoins ha inventato un sistema di feedback, in modo da fornire agli utilizzatori un'informazione maggiore sulla affidabilità della controparte.

Il sistema i scambi peer to peer, con finalità di reciclaggio, è quindi una realtà concreta. Recenti studi affermano che esiste ampia diffusione di tali pratiche a livello globale, tanto che le negoziazioni eseguite grazie al solo Local Bitcoins fanno riferimento a utenti di ben 249 paesi e migliaia di citta degli USA.

13- Scambi oltreoceano

Grazie alla trasformazione di moneta tradizionale in bitcoin, le organizzazioni criminali hanno trovato una modalità per far rientrare fondi dall'estero, ad esempio quelli piazzati nei paradisi fiscali, aggirando il controllo da parte delle forze dell'ordine. Viceversa, i capitali di origine illegale possono essere agevolmente cambiati in bitcoin in quei laddove i controlli antiriciclaggio sono più deboli, per essere poi riconvertiti in patria. Questo meccanismo si presta anche al finanziamento delle attività terroristiche.

La società Uquid, che ha sede in Gibilterra e opera nel campo della negoziazione di bitcoin, è un esempio di come un'organizzazione potrebbe essere implicata nel

reciclaggio. La società propone ai clienti una carta prepagata VISA, che è possibile caricare in bitcoin, senza la garanzia di tutti gli obblighi informativi verso le forze dell'ordine per intercettare capitali sospetti. Il nodo centrale qui è la giurisdizione: trattandosi di operazioni cross-border, le transazioni spesso si verificano al di fuori del raggio di azione delle autorità che contrasta il reciclaggio, sia da un punto di vista investigativo che per la possibilità concreta di intervento.

14- ATM in bitcoin

Anche le macchine di distribuzione del denaro ATM (*automated teller machine*) possono essere impiegate per operazioni di reciclaggio. Gli ATM del circuito Bitcoin non vanno confusi con i normali bancomat. Si tratta infatti di macchine in cui introdurre contanti per ottenere l'accredito in bitcoin sul proprio wallet personale o viceversa. La prima macchina di questo tipo è stata introdotta nel 2014, mentre già nel 2016 il loro numero era salito a 640 in tutto il globo.

I bitcoin acquistati tramite gli ATM, risultano negoziati in anonimato per poi essere utilizzati per l'acquisto di beni o servizi illegali, contribuendo così allo sviluppo del sommerso sul dark web. In molti paesi purtroppo gli ATM bitcoin neanche ricadono sotto la normativa antiriciclaggio.

In alcuni stati americani, gli ATM invece per operare debbono essere registrati come MSB (*money service business*) e dunque ricadono pienamente nelle norme antiriciclaggio. Nonostante ciò, spesso gli obblighi di legge possono essere agevolmente aggirati. Sebbene rientrino nella normativa, alcune compagnie di ATM chiedono soltanto il recapito telefonico dell'utente, numero che può benissimo esser di una scheda prepagata completamente anonima. Altre compagnie invece chiedono un documento di identità in fotocopia, documento che può essere ottenuto falso sul dark web.

15- Attività di tumbling

Le pratiche di tumbling possono essere utilizzate per incrementare il livello di riservatezza delle operazioni. Si tratta in buona sostanza di micro transazioni, che di fatto consentono di mimetizzare le informazioni reali relative ai soggetti della

negoziazione. Teoricamente infatti le transazioni in bitcoin sono pubblicamente visibili sulla blockchain. Attraverso le pratiche di tumbling, che di solito si svolgono sul dark web e attuate grazie a intermediari chiamati tumbler (Bitcoin Fog, BitMixer, SatoshiDice…), un soggetto può dividere un grosso ammontare d valuta virtuale in una moltitudine di piccolo ammontare unitario. In questo modo si ottengono tante transazioni di piccolo importo piuttosto che un unico ingente scambio, che potrebbe facilmente richiamare l'attenzione delle autorità competenti. Tra l'altro, questo sistema permette un certo effetto diversificazione: il rischio che una singola microtransazione possa individuata dalle forze dell'ordine ha un peso ridotto sul totale dell'importo. Lo scaglionamento si riflette poi anche nelle attività di prelievo: suddividere nel tempo i cambi in bitcoin e i prelievi di moneta legale impedisce agli investigatori di individuare, sulla base della tempistica, uno schema.

Le commissioni applicate ai servizi di tumbling di solito variano tra il 5 e il 15 per cento e dipendono dal volume dello scambio e dal livello di frammentazione. L'impiego di una pluralità di wallet su cui suddividere o da cui inviare l'importo rappresenta un servizio aggiuntivo, dato che determina una copertura più robusta delle informazioni sensibili a fronte di un costo più elevato, sempre tradotto in uno spread che va a sommarsi al tasso di cambio del mercato. Per le autorità, il problema principale delle tecniche di tumbling sta nel fatto che offuscano la blockchain, e pertanto rendono più difficile rintracciare la fonte originale del pagamento e quindi identificare le stesse operazioni sospette.

16- Transazioni sul dark web

Come detto, la diffusione di internet ha avuto un notevole impatto per le attività criminali. In particolare il dark web permette di:

- entrare in possesso agevolmente di una serie di supporti al reciclaggio: documenti di identità cartacei falsi, fare operazioni di spoofing, ossia falsificazione dell'identità attraverso l'alterazione dell'IP address, utilizzo abusivo di username e password di altri utenti, mimetizzazione di file nocivi per renderli non riconoscibili come tali;
- sfruttare l'anonimato garantito dall'uso delle criptovalute per facilitare le operazioni di riciclaggio e per trasferire, importi di denaro rilevanti di e da paradisi fiscali;

- convertire rapidamente i bitcoin ottenuti da attività illecite, questa tendenza che tra l'altro sembra confermare la scarsa attitudine del bitcoin ad essere riserva di valore;
- rendere ancora più efficienti le operazioni di layering recycling rendendo più difficile il monitoraggio da parte delle autorità e ampliando il bagaglio di trucchi per le operazioni di *integration recycling*.

Per i Bitcoin in particolare, c'è da notare che facendo seguito alle indagini su Silk Road e alla confisca della criptovaluta di Ross Ulbricht, i criminali hanno iniziato ad avere dubbi sulla reale pseudonimità di Bitcoin, virando su altre criptovalute in cerca di maggior riservatezza, come ad esempio Monero. Questa valuta difatti precede operazioni di tumbling in automatico, per rendere le transizioni ancor meno identificabili. Diverse piattaforme sul web ora danno la possibilità di accettare pagamento in moneto oltre che in bitcoin, consentendo anche scambi tra le due criptovalute: ad esempio AlphaBay, che tratta la vendita di stupefacenti. Monero ha aumentato così il proprio valore di 5 volte nell'arco di un anno.

17- Strategie alternative: Purse.io e gioco d'azzardo

Si stanno diffondendo pratiche che prevedono la vendita di oggetti in cambio di criptomoneta, su apposite piattaforme di Purse.io e similari. Purse consente di ottenere bitcoin tramite scambi peer to peer non registrate, assolutamente anonime. Gli scambi si realizzano attraverso la manipolazione delle vendite su Amazon, Amazon normalmente non accetta bitcoin come mezzo di pagamento. Il meccanismo che utilizza Purse è basato sulle wish list, un'opzione di Amazon che permette di fare una lista di oggetti di desiderati, da acquistare successivamente o da accettare in forma di regalo da altri utenti. Coloro che vogliono acquisire bitcoin non devono far altro che acquistare un oggetto presente nella wish list di un altro utente e ricevere in pagamento bitcoin; l'attività di business di Purse è quella di offrire un collegamento tra i soggetti che vogliono vendere bitcoin in cambio di beni acquistabili tramite Amazon. La piattaforma, per facilitare i deal ha sviluppato un'interfaccia che replica le wish list presenti da Amazon.

Sia Purse che Amazon non sono soggetti a specifici obblighi informativi in materia di riciclaggio e questo favorisce l'anonimato delle transazioni.

Questo metodo rappresenta uno schema che consente la cessione di bitcoin in cambio di beni di vario tipo, di solito beni facilmente rivendibili; d'altra parte per la mancanza di obblighi informativi, questo sistema rappresenta un modo per ottenere bitcoin in modo sostanzialmente nascosto per coloro i quali vogliono operare sul mercato di beni illeciti del dark web. Tuttavia, il sistema presenta commissioni piuttosto elevate: si arriva infatti anche al 15 per cento della transazione.

I bitcoin comunque diventano sempre più popolari come mezzo di pagamento nelle operazioni di riciclaggio legate al gioco d'azzardo e ai casinò online. Il mercato dell'online del gioco d'azzardo è in rapido sviluppo, e l'industria ha subito aperto agli utenti Bitcoin (in particolare per il poker online e i dadi). Questa crescita notevole è legata sia alle agenzie di gioco già presenti sul mercato che hanno iniziato a accettare criptovaluta, sia allo sviluppo di nuovi casinò online che accettano esclusivamente Bitcoin o altre criptovalute, quali Primedice e Bitcoincasino.

I siti di gioco sono dei luoghi ideali per movimentare denaro proveniente da attività criminali, o di riciclaggio senza destare troppi sospetti. Queste piattaforme infatti sono molto ramificate e quindi difficili da monitorare in relazione alle movimentazioni di fondi. Le organizzazioni criminali poi sono solite localizzare in stati esteri i server adibiti alla raccolta e alla gestione delle giocate. Spesso ciò poi avviene aggirando le normative statali che regolano il settore. Molto spesso infatti il server di un casinò online è localizzato in uno stato, mentre la sede legale dell'azienda è in un altro, e in un altro ancora viene piazzata la sede operativa. Oltretutto anche per le forze dell'ordine è molto difficile stabilire esattamente l'ubicazione del giocatore, anch'esso infatti è in grado di dislocare la propria attività in un paese diverso dalla sua residenza, rendendo così ancora più difficoltosa la sua individuazione.

Icasino online si prestano quindi a svariate strategie criminali. Ad esempio accade che un prestanome deposita in modo anonimo sul proprio conto online una somma di denaro di provenienza illecita per poi per perderlo a favore di giocatori complici, che in questo modo riescono a riciclare il denaro che figura come vincita da gioco d'azzardo. Le organizzazioni criminali inoltre potrebbero hackerare il sistema in modo da truccare giochi e indirizzare le vincite verso i membri stessi dell'organizzazione. I fondi poi possono anche essere impiegati per pagare tangenti ai pubblici ufficiali.

18- Collegamenti con il terrorismo

Il riciclaggio e il finanziamento al terrorismo presentano molti elementi coincidenti, tanto da rendere le due attività fortemente connesse: le somme da queste coinvolte spesso infatti viaggiano sui medesimi circuiti e utilizzano tecniche identiche per nascondere origine e destinazione del denaro[13].

Nel mondo del web, le criptovalute sono un elemento che ha assunto molta importanza per quel che riguarda anche la lotta al terrorismo. La possibilità di mobilizzare fondi in forma anonima ha infatti favorito la diversificazione delle fonti di finanziamento delle organizzazioni terroristiche, come nel caso dell'Isis, la cui fonte principale era prima rappresentata dal traffico di armi e droga, oppure dai proventi di estorsioni e sequestri. Alcuni studi condotti dalle autorità israeliane sembrano indicare che i terroristi siano ormai familiari con le opportunità offerte dalle criptovalute per muovere capitali in modo occulto. Secondo una fonte dell'intelligence israeliana, come riportato dal quotidiano Haaretz, esiste un'inquietante pista relativa al mondo delle criptovalute, che sarebbe utilizzato come canale per finanziare la lotta terroristica e per il reclutamento (al pari dei social network).

La possibilità che i terroristi si avvalgano delle criptovalute per finanziare le loro attività è un tema che è stato al centro di ampi dibattiti su svariati organi di stampa e informazione, particolarmente negli Stati Uniti, dove l'allarme sollevato non è parso infondato. A quanto è dato sapere apparentemente anche negli USA e in diversi paesi europei sarebbero presenti alcuni finanziatori delle attività terroristiche analogamente al fatto che ci siano ampi riscontri che anche nei paesi occidentali siano presenti sostenitori e fiancheggiatori dell'Isis in grado anche di arruolarsi per diventare soggetti attivi nelle azioni di lotta terroristica. Sarebbero a rischio terrorismo anche quelle persone che sarebbero capaci di sfruttare le innovative cripto valute facendo principalmente leva sulle eventuali zone grigie presenti nelle normative vigenti proprio al fine di spostare capitali dai paesi di residenza e dirottarli all'Isis, in questo modo favorendone la capacità economica e di conserva la pericolosità.

Il GAFI, nel 2014 ha condotta una analisi del problema portando alla luce caso davvero inquietante che racconta appunto della connessione tra Bitcoin e terrorismo di matrice islamista[14]. Ali Shukri Amin, uno studente di 17 anni residente in Virginia, il 28 agosto

[13] Galullo R. e Mincuzzi A. (2017), "Bitcoin, il riciclaggio invisibile di mafie e terrorismo internazionale", Il sole 24 ore, disponibile a: http://www.econopoly.ilsole24ore.com/2016/07/08/bitcoin-e-antiriciclaggio-i-primi-passi-delleuropa-per-un-quadro-legislativo/.

[14] GAFI/FATF Report (2014), "Valute Virtuali, definizioni chiave e potenziali rischi in ambito antiriciclaggio e finanziamento del terrorismo", http://www.fatf-

2015, ha subito una condanna a 11 anni e 7 mesi in quanto colpevole di aver spinto altri giovani a unirsi all'Isis attraverso l'utilizzo del social Twitter e un suo blog personale. Lo studente aveva poi ammesso la sua colpa in sede di processo dinanzi alla corte federale ammettendo di aver fornito aiuto anche in termini materiali allo allo Stato islamico sul web, istruendo i terroristi sull'impiego dei bitcoin per camuffare il sovvenzionamento delle attività della organizzazione del terrore.

Il GAFI ha preso l'occasione relativa a questo specifico caso per manifestare una giusta e crescente preoccupazione che comincia sempre di più a essere presente tra le autorità giudiziarie e di polizia in tutto il globo circa la concreta possibilità che le cosiddette valute virtuali possano essere utilizzate da parte delle organizzazioni che conducono la lotta terroristica. La relazione prodotta da GAFI mette in evidenza come negli ultimi anni siano cresciuti esponenzialmente in rete i siti web collegati al terrorismo internazionale che promuovono il ricorso alle nuove tecnologie anche per quanto riguarda l'impiego delle valute.

gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

CASE STUDY

19- Lo Stato Islamico e Al Qaida

Lo Stato Islamico (spesso abbreviato anche in Isis o Isil) è stato fondato nel 1999 da Abu Musaab al Zarqavi. A seguito della morte di al Zarqavi, Isis ha esteso il proprio ambito operativo dall'Iraq alla Siria, trasformandosi poi formalmente, nel 2014, nel cd. Stato Islamico, rendendo chiara, con tale denominazione, l'ambizione di espandersi oltre il Mediorente.

Già nel 2014 l'Isis era riuscito a richiamare in Siria e in Iraq numerosi *foreign fighters*, cioè dei combattenti che lasciano i propri paesi di provenienza per unirsi ai conflitti.

A partire dal 2015, Isis ha subito un ridimensionamento dei propri territori, perdendo il 55% di quelli controllati in Siria e Iraq e l'85% dei territori libici. Tale fenomeno ha comportato "l'avvio di una trasformazione di Isis con l'abbandono dell'enfasi posta sul controllo territoriale e un rafforzamento della propria capacità di organizzare attacchi anche al di fuori del Medio Oriente. Non più dunque una realtà proto-statale ma un fenomeno ideologico, terroristico e puntiforme".[15]

Tale fenomeno ha indotto numerosi foreign fighters a ritornare nei propri paesi occidentali di provenienza, aumentando così la minaccia di eventi terroristici in tali paesi. Isis ha infatti diffuso in rete numerosi video in cui si ribadisce l'importanza di sferrare attacchi all'occidente, utilizzando qualsiasi mezzo a disposizione degli adepti (armi bianche, autoveicoli, bombe incendiarie ecc).

La visibilità ottenuta da Isis non deve far passare sotto traccia la pericolosità ancora rappresentata da al Qaida che, per quanto indebolita nei suoi tradizionali luoghi di dominio (Afghanistan e Pakistan), rimane comunque molto forte nell'area del Maghreb, del Sahel, del Corno d'Africa e della Siria. A tal proposito Europol, nella propria relazione annuale 2016-2017, ha dichiarato che: "l'Europa si trova di ffronte a un mix di minacce terroristiche che non può essere trattato solo dagli Stati membri dell'Unione euopea. E' necessaria una cooperazione internazionale"[16]

---

[15] ISIS: la minaccia che cambia, Dossier ISPI, 24 agosto 2016, https://ispionline.it/it/pubblicazione/isis-la minaccia-che-cambia-15608

[16] Europol Review 2016-2017, European Union Agency for Law Enforcement Cooperation (Europol), 2017

20- Convergenza tra mondo cyber e terrorismo

Univoche analisi degli enti antiterrorismo europei hanno dimostrato come l'uso di internet sia una componente imprescindibile di ogni azione terroristica. Internet viene infatti usato come mezzo di comunicazione, come mezzo di diffusione della propaganda e come strumento per la raccolta di fondi.

Quanto all'ultimo utilizzo – la raccolta fondi – Europol ha segnalato come il finanziamento di piccole cellule terroristiche richiede importi inferiori rispetto a quelli utilizzati dalle organizzazioni transnazionali. Le forze investigative devono quindi porre particolare attenzione ai mezzi tipicamente usati da questi piccoli gruppi per finanziarsi: prestiti al consumo, uso di carte prepagate ecc. Si ricorda a tal proposito come gli attacchi al settimanale Charlie Hebdo e al supermercato kosher di Parigi sono stati finanziati con prestiti al consumo, con la vendita di un'automobile usata e con trasferimento di proventi della vendita di merce contraffatta.

Segnali di allarme della preparazione di un attacco sono quindi considerati:

- Ritiro dell'importo di prestiti in contanti;
- Utilizzo del denaro per scopi diversi da quelli per cui è stato richiesto un prestito;
- Un gran numero di piccoli prestiti richiesti a diversi istituti da parte di soggetti collegati tra loro.

È altresì essenziale identificare i trasferimenti bancari effettuati in favore di soggetti che si presumono radicalizzati.

Particolare attenzione va altresì rivolta a quei fondi che risultano raccolti da persone che operano come money collector, e che di norma si trovano in paesi limitrofi alle zone di conflitto.

Anche le organizzazioni non governative vengono talvolta usate, a loro insaputa, per finanziare attività terroristiche. A tal proposito, la Financial intelligence Unit francese ha fornito degli indicatori di allarme.

I tratti in comune a queste organizzazioni sono:

- Creazione successiva alla cd "primavera araba" (2011) e all'inizio della guerra civile in Siria;

- Attività nel campo della fornitura di medicinali, aiuti umanitari e prodotti alimentari non deperibili;
- Largo uso di internet (specialmente delle piattaforme di crowfunding) per la diffusione di massicce campagne di fundraising. I contributori di queste campagne effettuano le donazioni attraverso carte prepagate e conti PayPal;
- I meccanismi finanziari non risultano trasparenti: dietro la scusa dell'inaffidabilità dei sistemi
- bancari nelle zone di guerra, gli amministratori di queste organizzazioni effettuano prelievi di contante per decine, e talvolta centinaia, di migliaia di euro. Poiché le dichiarazioni di trasporto transfrontaliero di contante ai confini di un paese non vengono perfezionate in modo sistematico, si perde alla fine la tracciabilità di come questi fondi vengono usati nelle zone di guerra.

21- Lotta al cyber finanziamento del terrorismo

Le attuali politiche di prevenzione e contrasto dei finanziamenti al terrorismo si basano sulla collaborazione tra Autorità nazionali, e si giovano altresì della collaborazione con il settore privato. Le istituzioni private infatti, attraverso l'analisi delle abitudini dei propri clienti, possono fornire elementi utili ad individuare:

- La presenza di soggetti radicalizzati in viaggio per e dalle zone di guerra;
- Raccolte di fondi (anche di natura lecita) fatte con il nascosto scopo di finanziare il terrorismo;
- Aiuti umanitari suscettibili di essere distratti verso gruppi terroristici.

L'Italia, nella già menzionata Relazione sulla politica dell'informazione per la sicurezza, definisce la minaccia terroristica "strutturale e puntiforme", perché scaturente sì dalle note organizzazioni terroristiche, ma anche da elementi isolati, i cd. *individual terrorist*.

Secondo Europol, diversi foreigh fighters ritornano nei propri paesi – occidentali – d provenienza, aumentando quindi la minaccia terroristiche in queste aree.

A tal proposito Ispi (Istituto per gli Studi di Politica Internazionale) ha estrapolato una serie di dati caratterizzanti i foreign fighters italiani:

- Il 90,5% di sesso maschile; l'età media è 30 anni;
- Le regioni in cui si registra la più alta presenza di foreign fighters sono Lombardia, veneto e Emilia Romagna;

- Solo il 19,2% ha la cittadinanza italiana, i restanti risultano essere cittadini di Belgio, Paesi Bassi, Regno unito e Francia;
- La maggior parte dei foreign fighters è nata in Marocco e in Tunisia. Europol segnala che i cittadini extracomunitari implicati più spesso in casi di terrorismo provengono da Siria e Marocco, mentre i paesi di nascita più frequenti sono Belgio, Siria e Iraq;
- Hanno una bassa scolarizzazione e condizioni economiche basse; ricoprono spesso posizioni lavorative manuali o sono disoccupati;
- Oltre la metà non è coniugata;
- La maggioranza non ha esperienze pregresse di detenzione.

Europol ha evidenziato come la gestione dei flussi migratori e il contrasto al terrorismo sono due tra le sfide più impegnative che l'Europa si trova ad affrontare nella nostra epoca. Nonostante manchino chiare dimostrazioni di come i terroristi accedano sistematicamente all''Europa usando le rotte dei migranti, è innegabile che numerosi terroristi si siano introdotti nell'Unione europea come rifugiati, come è ad esempio avvenuto per i protagonisti degli attacchi di Parigi del 13 novembre 2015.

Bisogna d'altra parte considerare però che i terroristi riscontrano sempre maggiori ostacoli nello sfruttare i flussi dei migranti, a causa dell'intensificarsi delle misure di sicurezza adottate alle frontiere con l'UE. Questo dato è confermato anche dai report di Europol, che evidenziano come al ridursi delle possibilità di formazione (addestramento militare e propaganda) in Siria, le stesse aumentano in territorio europeo.

Il 40% delle attività terroristiche sono, almeno parzialmente, finanziate coi i proventi di attività illecite. Piccoli attacchi non necessitano però di grandi finanziamenti, e rappresentano pertanto un'enorme sfida per le autorità preposte alla loro intercettazione e contrasto. Secondo recenti studi infatti, gli individual terrorist riescono agevolmente ad autofinanziarsi, eventualmente con l'aiuto di famigliari e amici, rendendo molto difficile il compito di chi cerca di identificarli preventivamente. Tali metodi di autofinanziamento includono gli stipendi personali, la vendita di beni propri, prestiti personali e anche borse di studio.

"La capacità di lettura anticipata dei segnali, delle anomalie relative al terrorismo e al suo finanziamento rappresentano un elemento cruciale per continuare un vantaggio strategico, che deve essere costantemente alimentato da una continua collaborazione e

integrazione”[17] tra autorità inquirenti e istituzioni pubbliche e private, per contribuire alla crescita del know-how dell’intero sistema antiterroristico mondiale.

[17] Financial Intelligence Agency “Il terrorismo e il suo finanziamento. L’esperienza europea”, 2016

NUOVE SFIDE

22- Necessità di una definizione uniforme

Le nuove monete digitali sono un fenomeno di portata globale, operano infatti a livello internazionale e, proprio per tale motivo, sarebbe necessario definire un quadro regolamentare maggiormente integrato e condiviso a livello mondiale. Occorre tenere presente per questo diversi punti critici. La maggior parte degli schemi di riciclaggio presenta tipicamente una struttura decentrata (classico esempio è quello adottato per il gioco d'azzardo), che di fatto previene le singole autorità nazionali di riuscire a strutturare strategie di prevenzione e contrasto che siano completamente efficaci. Le autorità si scontrano infatti con un quadro normativo non disegnato per combattere fenomeni che operano al di fuori dei confini nazionali; inoltre, la difficoltà diventa particolarmente grave nel caso (che rappresenta la norma) gli operatori dei sistemi criminali operano in paesi che sono più deboli in tema di normativa antiriciclaggio.

Come è stato già osservato tutte queste valute digitali che possono poi essere convertite valute reali si prestano maggiormente ad essere utilizzate per finalità illecite rispetto alle monete tradizionali grazie anche (e soprattutto) alla loro attitudine a essere agevolmente trasferite a livello global secondo modalità operative che ne rendono estremamente complessa la tracciabilità da parte delle autorità. Le organizzazioni criminali quindi si avvantaggiano in tutti i modi possibili da queste difformità presenti nelle giurisdizioni nazionali.

È proprio la natura intrinsecamente globale del fenomeno che fa sorgere l'esigenza di un'armonizzazione degli ordinamenti che regolano la materia. Tale armonizzazione non deve esplicarsi limitatamente alle misure meramente, ma deve necessariamente prendere avvia da una definizione di criptovaluta che sia il più possibile condivisa. La costruzione di un efficace schema di contrasto dei fenomeni illeciti legati all'uso delle monete virtuali deve quindi basarsi prioritariamente su una definizione quanto più univoca della natura delle stesse. Questa operazione definitoria potrebbe infatti liberare il legislatore dal gravoso compito di dovere ogni volta ricondurre le fattispecie a istituti giuridici preesistenti che, nella maggior parte dei casi, non sono pienamente compatibili con la natura ibrida di questi strumenti.

Il Bitcoin e le altre monete virtuali che il mercato continuamente crea sono state infatti di volta in volta assimilate a altri fenomeni economici come le monete tradizionali, i

prodotti finanziari o le merci. Ogni tentativo esperito in tal senso è stato foriero anche di alcune interessanti analogie, ma alla fine cozza con la natura appunto complessa e nuova di tale fenomeno. Questa situazione di fatto impedisce che si crei un grado normativo di riferimento esaustivo e univoco.

Il prodotto nato da una intuizione di Nakamoto, in particolare se osservato da un punto di vista economico, non è esattamente inquadrabile come moneta; rispetto alle monete tradizionale si scontra con alcuni limiti dettati dalle sue caratteristiche funzionali (ad esempio, la volatilità). Alcuni in dottrina, partendo dalla sua natura dematerializzata, hanno provato a ricondurre il fenomeno sotto il cappello della moneta elettronica, asserendo che le monete virtuali ne potessero rappresentare un sottoinsieme. In realtà il Bitcoin non può ricadere nella fattispecie della moneta elettronica. La disciplina contenuta nelle disposizioni della BCE sulle monete elettroniche definiscono il perimetro delle stesse secondo tre criteri identificativi in cui il Bitcoin non ricade. Ad esempio la produzione di criptovaluta avviene mediante attività di mining. Queste non sono legate alla ricezione di fondi di valore equivalente a quello rappresentato nel segno monetario. Una possibile sarebbe considerare il bitcoin come una merce (la normativa francese ha adottato questa definizione), in quanto ha una sua natura di bene immateriale, specifico, divisibile e infungibile. Si osserva però che esiste una sostanziale differenza rispetto a tutte le altre merci; il suo unico valore d'uso è costituito dal valore di scambio. Questo fa sì che il suo valore presenti fluttuazioni molto più ampie rispetto a una qualunque altra merce. Un ulteriore approccio al problema assimila il bitcoin a un valore mobiliare. In tal modo si cerca di coglierne il suo utilizzo come forma di investimento. Pure questo approccio però presenta delle lacune in quanto, differentemente dagli altri strumenti finanziari, bitcoin non rappresenta la passività emessa da un soggetto, non è pertanto un titolo di credito e non prevede nessun diritto in capo al possessore. Nel nostro paese è anche stata avvertita questa difficoltà a ricondurre questi strumenti nell'alveo dei principi generali del nostro ordinamento in particolare alla luce delle loro molteplici possibilità di utilizzo. Questo ha spinto molti studiosi a riportare la fattispecie delle monete virtuali a istituti giuridici molto vasti, ad esempio quello di bene giuridico immateriale, secondo la vasta definizione contenuta nell'art. 810 del codice civile, o quello (prevista nel d.lgs 7 marzo 2005 n. 82) di documento informatico, ossia di rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Per concludere appare che oggi, la sfida posta dall'avvento delle criptovalute non sia stata pienamente colta dagli ordinamenti nazionali proprio alla luce di quest'ultimo punto. Infatti le autorità di investigazione sono per lo più portati ad adattare le leggi in

vigore a una fattispecie su cui si riscontra una forte componente di incertezza del diritto. Da questo punto di vista forse è l'ordinamento giuridico tedesco quello che ha affrontato in maniera più esaustiva il tema della qualificazione giuridica delle monete virtuali. A dire la verità, questa carenza di uniformità normativa a livello globale produce molti problemi di intervento e repressione dei fenomeni criminali, ad esempio nell'ipotesi di movimenti effettuati in criptovaluta al fine di rimpatriare capitali esteri. Un uso illecito delle monete virtuali è infatti ampiamente agevolato dalla incertezza giuridica. Da molte parti si auspica la un nuovo istituto giuridico che contenga le caratteristiche di tali strumenti e che superi le asimmetrie normative oggi prevalenti tra gli ordinamenti nazionali.

La proposta di modifica della IV Direttiva antiriciclaggio del febbraio 2017 sembra segnare quantomeno un passo avanti, se non altro rispetto al problema del riconoscimento della natura delle valute virtuali che finalmente possa essere condiviso quantomeno a livello comunitario. La proposta infatti introduce una modifica dell'articolo 3, con l'aggiunta del punto 18. La modifica finalmente vuole identificare le valute virtuali in maniera che sembra esaustiva[18].

23- Assistenza agli organismi di law enforcement

Tra i vari problemi che colpiscono le forze dell'ordine e i sistemi giuridici c'è quello della carenza di risorse (in termini di conoscenze specifiche) per affrontare in modo efficacie la nuova sfida lanciata dalle criptovalute e dal dark web.

Le nuove tecniche utilizzate dalle organizzazioni criminali nel campo degli illeciti finanziari necessiterebbero infatti di un adeguato addestramento dal punto di vista tecnico. È anche necessario fare uso di software avanzati e all'avanguardia per poter svolgere proficue indagini sulle operazioni svolte sfruttando le nuove tecnologie e il complesso e variegato mondo del web. Tra l'altro questi strumenti necessiterebbero anche di un continuo ricambio, in modo da seguire la continua evoluzione della tecnologia e non rappresentare invece un punto di debolezza. Sarebbe estremamente utile in tal senso dotarsi del supporto di una struttura centralizzata che raccolga e conservi dati sulle informazioni più rilevanti che afferiscano alle monete virtuali.

[18] *"una rappresentazione digitale di valore che non viene emesso da una banca centrale o da un'autorità pubblica e non necessariamente collegato a una moneta a corso leale, ma è accettato da persone fisiche o giuridiche come mezzo di pagamento e può essere trasferita, immagazzinata o scambiata elettronicamente"*

Sarebbe anche poi fondamentale una piena condivisione di tali informazioni tra i soggetti inquirenti.

Un contributo importante alle indagini digitali viene sempre più spesso da imprese private in molti casi finanziate dalle stesse autorità governative; il loro principale compito consiste nel migliorare il livello conoscitivo delle forze dell'ordine a proposito dei nuovi schemi di riciclaggio sviluppati di continuo e sfruttare i dati in loro possesso per costruire dei modelli di analisi sui traffici in criptovalute al fine di intercettare i vari schemi connessi a operazioni di riciclaggio. Le organizzazioni criminali si avvalgono delle più recenti tecnologie per costruire sempre nuove strategie e nuovi schemi di riciclaggio. Occorre quindi lavorare per ridurre il gap tecnologico-cognitivo e consentire la tempestività degli interventi da parte delle autorità. Nel migliore dei mondi sarebbe addirittura auspicabile arrivare a anticipare questi nuovi schemi di riciclaggio.

Esistono già degli esempi in tal senso come il software nato dalla collaborazione tra il Dipartimento della Sicurezza Interna degli Stati Uniti e Sandia National Laboratories (i Sandia National Laboratories sono laboratori dell'United States Department of Energy, dedicati alla sicurezza nazionale per conto della Nationale Nuclear Security Administration): il nuovo software dovrebbe supportare le forze dell'ordine attraverso il monitoraggio della blockchain. Questo monitoraggio è disegnato in modo da individuare schemi di riciclaggio, attività di cybercrime e commerci di natura criminale sul dark web. In pratica prevede lo sviluppo di una interfaccia grafica che consente il raffronto dei flussi di denaro osservati dalle forze dell'ordine attraverso algoritmi sviluppati da Sandia, che cercano di riprodurre schemi di operazioni illecite presenti in un archivio storico. Tra i fini c'è quello di aggirare gli effetti di camuffamento delle operazioni illecite attuato con metodi ad esempio di tumbling.

Come nel caso illustrato si stanno oggi sviluppando diversi software dedicati allee indagini, normalmente si tratta di progetti finanziati dai governi. Si parla di prodotti destinati a produrre sofisticate analisi della Blockchain e delle transazioni in criptovalute per offrire un valido supporto alle forze dell'ordine; tra questi ne citiamo alcuni: Elliptic, Block Seer, Chainalysis e Ledger Labs.

24- Equilibrio tra regolamentazione e libertà di innovazione: il caso Bitlicense

Oggi i legislatori hanno davanti anche una ulteriore sfida: individuare soluzioni efficaci di contrasto al crimine senza per questo ostacolare la crescita di nuovi mercati e prodotti. Se infatti si adottasse un approccio troppo rigido nei confronti di questa nuova tecnologia ciò si tradurrebbe in una limitazione delle offerte di servizi e prodotti connessi alle monete virtuali, Questo ne determinerebbe un aumento dei prezzi, ne danneggerebbe la qualità e potrebbe creare possibili situazioni di cartello. A questo bisogna necessariamente aggiungere anche lo sviluppo di attività professionali e l'offerta di prodotti e servizi a cui potrebbe facilmente accedere chiunque, non soltanto i clienti di istituti bancari.

Occorre quindi trovare nelle linee guida dovrebbe essere quello di trovare un corretto equilibrio tra il consentire lo sviluppo di sistemi in grado di aumentare l'efficienza dei mercati finanziari e incoraggiare lo sviluppo economico, e l'esigenza altrettanto importante di garantire l'integrità stessa dei mercati, in questo caso dettando anche limiti e regole che possano prevenire e reprimere comportamenti potenzialmente dannosi.

Le criptovalute da un lato sono foriere di effetti positivi per i consumatori in termini di innovazione nel sistema dei pagamenti, ma al tempo stesso potrebbero anche generare effetti negativi sulla politica monetaria, sulla stabilità finanziaria e, in ultima analisi, sulla sicurezza del sistema economico-sociale nel suo complesso.

Pur nella breve storia delle monete virtuali già si registrano esempi in cui la normativa si è dimostrata troppo restrittiva e ha ostacolato le naturali forze di mercato. Il Dipartimento dei Servizi Finanziari dello Stato di new York nel 2015 ha redatto lo Statuto per la regolamentazione delle attività professionali in valute digitali (denominato Bitlicense). La normativa ha introdotto stringenti requisiti di registrazione e di licenza per ogni organizzazione, piattaforma o mercato, legati al mercato dei bitcoin. La normativa fa anche un lungo elenco di attività che ricadono sotto la sua applicazione. Esiste nel dettato normativo la definizione di "*virtual currency business activity*" sotto la quale rientrerebbero: l'attività di ricezione e trasmissione di valuta virtuale; la conservazione, la custodia o il controllo di valuta virtuale per conto terzi, l'attività di acquisto e vendita di valuta virtuale in modo professionale, la prestazione del servizio di cambio valuta virtuale in valuta legale e viceversa, l'emissione, l'amministrazione e il controllo di valuta virtuale.

Il regime previsto da Bitlicense si applicherebbe tra l'altro solo nel caso in cui queste attività siano effettuate nello stato di New York o da cittadini dello stato stesso.

I requisiti previsti ai fini dell'ottenimento della licenza sono molto simili a quelli che già si trovano per le "money service business", ma appaiono ancora più severi. In particolare modo, gli exchange abilitati devono obbligatoriamente raccogliere numerose informazioni sui soggetti che effettuano le negoziazioni e segnalare, per finalità di antiriciclaggio, tutte le transazioni che eccedono i 10.000 dollari al giorno per persona e per volume e, in termini generali segnalare alle autorità tutte le operazioni sospette in termini di riciclaggio, evasione fiscale o comunque attività illecite.

La soluzione proposta da Bitlicense si è però rivelata eccessivamente restrittiva, tanto da ridurre in modo rilevante numero di organizzazioni operanti sul mercato. Molte delle imprese che si adoperavano nel mercato delle criptovalute si sono dette preoccupate per quanto riguarda l'onere eccessivo a livello informativo. Tra l'altro ritengono che Bitlicense ponga troppe limitazioni alla capacità del mercato di innovare. A quanto pare tali preoccupazioni non sono infondate: finora solo tre organizzazioni hanno ottenuto la licenza e possono operare come piattaforma di scambio Bitcoin. Il sito tiene sotto monitoraffio il numero delle entità che operano nelle monete vituali e sono soggette a Bitlicense. Nell'agosto 2015 Coindesk.com ha registrato solo 9 exchanger che si erano adoperati per ottenere la licenza, 15 invece hanno cessato del tutto la loro operatività nello Stato subito dopo l'approvazione di Bitlicense, per poi migrare in altri stati.

25- Gli interventi del GAFI

Abbiamo parlato dei rischi insiti nel mercato. Questi rischi hanno richiamato l'attenzione delle principali internazionali ed europee: il Gruppo d'Azione Finanziaria Internazionale (GAFI), l'Autorità Bancaria Europea (EBA) e la Banca Centrale Europea (BCE). Nei prossimi paragrafi si darà un quadro generale degli interventi che si sono succeduti in tal senso.

Il Gruppo d'Azione Finanziaria Internazionale (GAFI) è un organismo intergovernativo che sviluppa e propone strategie di protezione del sistema finanziario con riferimento ad alcune fattispecie quali il riciclaggio e il finanziamento al terrorismo. Il gruppo promuove il coordinamento dei diversi ordinamenti giuridici su dette materie.

Il GAFI si esprime attraverso diversi tipi di strumenti: raccomandazioni, elaborazione di standard riconosciuti a livello internazionale nella lotta alle attività illecite, elaborazione di studi di trend dei fenomeni criminali. In pratica fornisce supporto agli organismi governativi nella lotta alla criminalità. Si tratta normalmente di raccomandazioni non legalmente cogenti. Tuttavia sono un utile ausilio per i governi quale strumento aggiuntivo di grande utilità e spesso in grado di influenzarne la produzione normativa, soprattutto per quelle nazioni che presentano problemi strategici nei loro sistemi di prevenzione e contrasto.

Ogni stato ha nel proprio ordinamento un'unica agenzia antiriciclaggio, indicata come Financial Intelligence Unit (FIU), a cui è garantita autonomia da un punto di vista operativo e gestionale ed è dedicata alla analisi finanziaria delle informazioni per la doppia finalità di sorveglianza prudenziale e di prevenzione e contrasto delle attività di riciclaggio e di finanziamento al terrorismo.

In Italia, questo compito è svolto dall'Unità di Informazione Finanziaria (UIF), istituita presso la Banca d'Italia dal DLgs 231/2007 (Decreto antiriciclaggio). Il decreto recepisce la direttiva europea 2005/60/CE. I principali compiti dell'UIF sono:

a – ricezione e analisi delle segnalazioni relative a operazioni sospette e le informazioni rilevanti che riguardano tali attività;

b – la ricerca e lo studio di nuove tecnologie adoperate e le nuove tecniche di riciclaggio;

c – elaborazioni di indicatori di anomalia, finalizzati a supportare l'individuazione delle operazioni sospette;

d – invio alle autorità competenti del di informazioni raccolte al fine di un intervento legislativo e operativo.

Rispetto all'ultimo punto, l'art. 41 prevede che ci sia una stretta collaborazione con la Guardia di Finanza e la DIA (Direzione Investigativa Antimafia)[19]. Su questo aspetto l'UIF è incaricata di inviare le segnalazioni ricevute (insieme a una relazione tecnica),

[19] si veda *Relazione del Ministero dell'interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia*, primo semestre 2016. Si veda anche la *Relazione del ministro dell'interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia*, primo semestre 2017. In questo senso anche FEDERL BUREAU OF INVESTIGATION, Bitcoin Virtual Currency: Intelligence Unique *Features Present. Distinct Challenges for Deterring Illicit Activity,* 24 aprile 2012

nonché con l'Autorità Giudiziaria, a cui comunica i fatti che possano mostrare una rilevanza di natura penale.

Il GAFI fa un primo intervento riconducibile alle criptovalute in un report del 2013. In questa fase, le valute virtuali venivano solo menzionate. Nel report non era infatti presente una esaustiva definizione.

Nel 2014 però il GAFI ha ripreso il problema in un nuovo report dove ha sottolineato la pericolosità delle criptovalute, parlando nello specifico dei Bitcoin[20]. Il GAFI infatti ha come obiettivo lo sviluppo di misure di prevenzione proporzionate per i soggetti obbligati. A tali obblighi devono poi devono provvedere gli ordinamenti nazionali emanando apposite norme che siano coerenti con il quadro definito a livello internazionale. Il GAFI nel documento prende coscienza dei pericoli che derivano da certi usi delle valute virtuali, specialmente quelle convertibili e centralizzate. Ne identifica i rischi e propone le misure di contenimento maggiormente appropriate. Nel report è la questione è trattata ampiamente. Le monete virtuali qui sono definite come una tipologia di Internet-based payment service e vengono classificate in base alle caratteristiche e alle modalità di funzionamento. Il Gruppo poi si adopera a individuare i soggetti che operano nel nuovo mercato, identifica i rischi che la loro attività può comportare per l'antiriciclaggio e descrivendo alcuni casi di indagini relative ad attività illecite commesse grazie all'impiego di questi strumenti. Sottolinea anche l'importanza delle attività di ispezione e controllo nei confronti dei soggetti interessati dalla normativa: intermediari finanziari, money transfer, società fiduciarie ecc…, allo scopo di addivenire a una verifica del corretto adempimento degli obblighi previsti dalla legge e prevenire l'utilizzo del sistema finanziario finalizzato alla movimentazione di fondi di origine illecita.

26- L'opinione dell'EBA

Secondo l'art. 9 del Regolamento UE 1093/2010, l'European Banking Authority (EBA) è un organismo di vigilanza europeo il cui compito consiste nel monitorare le attività finanziarie adottando orientamenti e raccomandazioni finalizzati alla

[20] Nel report si legge: "le valute virtuali e i bitcoin in particolare sono l'ondata del futuro per i sistemi di pagamento e forniscono un nuovo e potente strumento per i criminali, terroristi, finanzieri e evasori, consentendo loro di far circolare e conservare fondi illeciti, fuori dalla portata del diritto"

promozione della sicurezza e della solidità dei mercati nonché la convergenza delle prassi di regolamentazione.

A partire dal settembre 2013 l'EBA ha cominciato ad interessarsi alle criptovalute, producendo uno studio specifico. Lo studio contiene un warning diretto ai consumatori. Nel warning si evidenzia il rischio che l'utilizzo delle valute virtuali come strumento di pagamento avrebbero potuto produrre perdite economiche. Successivamente, nel luglio 2014, l'EBA ha emesso la propria "*opinion on virtual currencies*". In questa opinione l'EBA ha espresso un giudizio decisamente critico sulle criptovalute. Basandosi su una accurata analisi costi/benefici, l'autorità europea ha affermato che i rischi derivanti dall'uso delle valute virtuali fossero in quel momento superiori ai vantaggi che gli utenti avrebbero potuto ricavare da un loro utilizzo. Nel documento inoltre EBA sollecita un intervento regolamentare da parte delle istituzioni europee.

L'approccio proposto si muove lungo due binari. Uno di lungo periodo e uno a più breve. Nell'ottica di lungo termine, l'EBA ha evidenziato l'esigenza di adottare un quadro normativo il più possibile armonizzato per il contenimento del rischio; viene pertanto proposta l'introduzione di una specifica regolamentazione secondo uno schema di *governance authority*, questa incaricata di regolamentare l'impiego della moneta virtuale e assicurare l'integrità del sistema. Si auspica inoltre un regime autorizzativo che preveda per i partecipanti al mercato, requisiti di capitale e di finalizzati al contenimento dei rischi.

Per il progetto di lungo periodo, si auspica che esista separazione tra le attività relative alle criptovalute e quelle tradizionali in capo ai soggetti che prestano servizi in valute virtuali. l'EBA inoltre ha invitato le istituzioni europee provvedere alla mitigazione dei rischi provenienti dall'interazione delle criptovalute col sistema finanziario. In particolare, si suggerisce di far ricadere sotto la disciplina comunitaria di antiriciclaggio e di contrasto al finanziamento del terrorismo anche i soggetti che forniscano servizi di conversione tra criptovalute e valute reali.

Sul fronte del breve periodo, l'EBA, ha invitato le Autorità di vigilanza degli Stati membri a fare moral suasion sui soggetti vigilati contro la negoziazione di monete virtuali fintanto che la materia non fosse adeguatamente normata.

27- Interventi comunitari

La Commissione Europea, alla luce della crescente diffusione del terrorismo internazionale e delle sue innovative modalità di finanziamento e alle connesse pratiche di camuffamento dei capitali di origine criminale, ha condotto una sua riflessione volta a migliorare la capacità di contrasto di questi fenomeni. Ha quindi prodotto un Piano d'azione che rafforzasse ulteriormente il contrasto del fenomeno del finanziamento del terrorismo. Il Piano si incentra su una duplice linea d'intervento:

a- Individuare e prevenire i movimenti di fondi e di altri beni effettuati dalle organizzazioni terroristiche e dai loro fiancheggiatori
b- Smantellare le fonti dell'entrate delle reti terroristiche colpendone le capacità di raccolta fondi.

Nel febbraio 2017, la Commissione Europea, ha prodotto una proposta di modifica della Direttiva 849/2015 (IV direttiva antiriciclaggio) e, in accordo con quanto contenuto nella "Risoluzione sulle valute virtuali" approvata il 25 maggio 2016 dal Parlamento Europeo, ha dato riconoscimento al ruolo assunto dalle valute virtuali all'interno dell'economia illegale. Le modifiche più rilevanti alla Direttiva 849/2015 riguardano ad esempio l'inclusione delle piattaforme di cambio di valute virtuali tra i soggetti obbligati, la determinazione di valori limite di transazione più bassi per alcuni strumenti prepagati, maggiori poteri alle FIU nazionali, il rafforzamento dei controlli nei confronti dei paesi terzi che presentano un rischio maggiore e la raccolta di una maggiore quantità di informazioni sulla titolarità effettiva delle piattaforme.

La Commissione europea qui propone di includere nell'ambito applicativo della direttiva antiriciclaggio anche le piattaforme di scambio di valute virtuali (cosiddetti exchange) e i prestatori di servizi di portafoglio digitale (custodian wallet provider). Il documento non si propone una regolamentazione integrale delle valute virtuali, ma incentra la sua attenzione su alcuni specifici operatori del mercato. Nell'impostazione della Commissione questi interventi possono rappresentare la chiave per un'azione efficace e risolutiva, in quanto questi raccolgono una enorme quantità di dati sensibili derivanti dagli strumenti di pagamento "tracciati" (bonifico, carta di credito…). Oggi le politiche di antiriciclaggio vengono fatte proprie su base volontaria degli organismi di exchange. Tutto ciò può risultare controproducente se non appositamente inquadrato in una cornice regolamentare che renda obbligatoria la trasmissione delle informazioni e delle operazioni sospette alle autorità competenti.

L'intervento principale da porre in essere è quindi quello di superare l'anonimato che caratterizza tali operazioni in modo da consentire alle forze dell'ordine di entrare a conoscenza di eventuali situazioni di pericolo. Il passaggio a questo scopo

evidentemente necessario è rappresentato dalla estensione degli obblighi di adeguata verifica della clientela anche alle piattaforme che permettono il cambio di valute virtuali in valute legali. Solo così gli exchanger diverrebbero soggetti obbligati cime previsto dalla direttiva antiriciclaggio. Essi infatti sono tenuti a raccogliere, e registrare i dati personali, e in alcuni casi fornirli direttamente alle autorità competenti (come ad esempio le unità di informazione finanziaria). La normativa proposta fa richiesta che gli exchanger siano soggetto a una qualche forma di autorizzazione rilasciata dalle autorità nazionali. Si rimanda però ai legislatori nazionali la scelta se si debba adottare un sistema di vera e propria licenza o semplicemente di registrazione. La stessa normativa verrebbe estesa ai wallet provider, ossia ai soggetti che offrono servizi di *hot storage*, necessari per conservare le valute virtuali sui portafogli online.

Nel documento si dà anche una precisazione della natura degli organismi a cui la normativa debba essere indirizzata. Gli exchanger vengono indicati come prestatori di servizi la cui attività principale è nel settore dei servizi di cambio tra valute virtuali e valute a corso legale. In questo contesto, anche sulla base dell'analisi condotta dalla Banca Centrale Europea sui regimi di valuta virtuale, la Commissione opera una distinzione tra exchanger "puri" e piattaforme di trading. Gli exchanger (ad esempio kraken) forniscono gli utenti di servizi di trading indicando i prezzi correnti a cui l'exchanger acquisterà o venderà valuta virtuale contro le principali valute (dollaro statunitense, yen, euro) o contro altre valute virtuali. Per lo più si fa riferimento a imprese non finanziarie, che possono essere affiliate agli emittenti di valute virtuali o a terze parti. Normalmente, gli exchanger accettano una lista ampia di strumenti di pagamento, ad esempio contanti, bonifici e pagamenti con altre valute virtuali. Diversi operatori inoltre danno al cliente anche una serie di servizi accessori, tra cui la possibilità di fungere da wallet provider, o fornire statistiche sulle evoluzioni del prezzo, sui volumi scambiati e sulla volatilità. In alcuni casi vengono anche offerti servizi di conversione ai commercianti che accettano le valute virtuali come strumento di pagamento. Si consideri che le piattaforme di trading (ad esempio Local Bitcoins) di fatto funzionano come mercati, ossia sono un veicolo che mette in contatto gli acquirenti e i venditori di valute virtuali attraverso appunto la piattaforma stessa. Infatti le piattaforme di trading non operano da intermediari diretti, a differenza degli exchanger, e pertanto non comprano o vendono per conto proprio.

28- Posizione della Banca d'Italia e normativa fiscale italiana

Nel rapporto di stabilità finanziaria del 2014 per la prima volta la Banca d'Italia si occupa espressamente del crescente fenomeno delle valute virtuali. Nel citato rapporto la banca d'Italia esprime preoccupazioni sulle criptovalute (in particolare parlando dei bitcoin). Nel documento vengono riprese le posizioni prevalenti a livello europeo; tali preoccupazioni si rivolgono in particolare al possesso e l'uso di monete virtuali, in particolar per la lacuna di forme di tutela per utilizzatori.

La Banca d'Italia affronta nuovamente il tema il 30 gennaio 2015, divulgando sul sito istituzionale una "*Avvertenza sull'utilizzo delle cosiddette valute virtuali*", emettendo in contemporanea una Comunicazione al sistema bancario. La posizione espressa dalla Banca d'Italia ha molto in comune con l'opinione divulgata dall'EBA di cui abbiamo parlato; in particolar modo la Banca aderisce a quella idea delle criptovalute come "*rappresentazioni digitali di valor*e". In questa ottica l'obiettivo prioritario è far sì che i soggetti vigilati adottino comportamenti ispirati alla massima cautela che li faccia assumete solo rischi consapevoli e ponderati. In questa ottica la negoziazione di valute virtuali o la loro accettazione come strumento di pagamento non sono di per sé considerate illecite, ma ne vengono rammentati i rischi, come ad esempio l'elevata volatilità del valore. L'analisi condotta dalla Banca d'Italia pone particolare attenzione alla incertezza che regna nel mondo delle valute virtuali, considerato come fenomeno è in continua evoluzione. Questa circostanza non consente un'identificazione completa di tutti i possibili effetti che possono derivare dal suo utilizzo; all'interno del documento infatti si legge che non si può escludere che "*l'uso di valute virtuali possa esporre l'utilizzatore a rischi ulteriori, derivanti dalle caratteristiche della specifica valuta virtuale utilizzata. Inoltre, il fenomeno è soggetto a rapida evoluzione ed è possibile che valute virtuali di ultima generazione presentino ulteriori rischi rispetto a quelli illustrati"*.

Sempre in pieno accordo con la visione dell'EBA, la Banca d'Italia tende a scoraggiare le banche e gli altri intermediari vigilati dal negoziare valute virtuali. Ciò per un duplice ordine di motivazioni; assenza di adeguati presidi e di un quadro legale definito a proposito della natura giuridica delle valute virtuali; possibilità che l'uso di detti strumenti potrebbe determinare la violazione di disposizioni normative. In altri termini, assenza di una puntuale definizione da un punto di vista normativo, le reali modalità di funzionamento delle valute virtuali potrebbero ricadere negli ambiti di quelle specifiche attività (es: bancaria) che la legge riserva a determinati soggetti. Soggetti sottoposti a uno speciale regine che ne attesti alcuni elementi quali disponibilità patrimoniali e del capitale di vigilanza.

La Banca d'Italia quindi raccomanda prudenza stabilendo che gli intermediari che vogliono negoziare valute virtuali debbano portare l'orientamento espresso dalla Banca d'Italia a conoscenza degli utenti, preventivamente all'effettuazione di operazioni con essi. Inoltre, anche la Banca d'Italia mira ad avere un quadro normativo omogeneo, possibilmente uniforme all'interno della Zona Euro. Questo per evitare che la partecipazione degli intermediari vigilati al mercato delle criptovalute, possa aumentare i rischi per la stabilità dell'intero sistema finanziario.

La Banca d'Italia opera quindi in questa fase sul piano della soft law. Non vengono posti obblighi o divieti ma si utilizza la *moral suasion* facendo appello alla prudenza e alla consapevolezza dei rischi, nonché portando i soggetti a conoscenza della loro policy interna rendendoli edotti che un loro eventuale coinvolgimento nel mercato delle criptovalute potrebbe essere in qualche misura bilanciato dall'assunzione da parte dell'Autorità di vigilanza di specifiche misure di carattere prudenziale, chiaramente rivolte alla mitigazione dei rischi assunti.

C'è solo una parte della comunicazione con contenuto prescrittivo ed è quella riguardante gli obblighi informativi sull'orientamento della Banca d'Italia, a cui si aggiunge l'ovvia conferma che chi utilizzare le valute virtuali sarà tenuto al rispetto delle norme presenti per le normali valute legali.

Da un punto vista fiscale, una prima regolamentazione ufficiale circa la questione relativa alle modalità di considerazione delle criptovalute si rinviene nella risoluzione 72/E/2016, con cui l'Agenzia delle Entrate mostra il trattamento fiscale da applicare a chi svolge attività di acquisto e cessione di moneta virtuale con contropartita di valuta standard. Per i clienti che siano persone fisiche detentrici di bitcoin al di fuori dell'attività d'impresa, si assume che si tratti di operazioni a pronti e che quindi non generano redditi imponibili, dato che è assente la finalità speculativa. In questo caso gli operatori non sono tenuti agli adempimenti come sostituti d'imposta e sono al di fuori del campo di applicazione Iva. Rimane però ferma la facoltà dell'Agenzia di acquisire le liste della clientela per le opportune verifiche nell'espletamento delle normali attività di controllo.

Con riguardo alle attività di intermediazione di valute tradizionali con bitcoin, che sia svolta in modo professionale e abituale, queste non rientrano nel campo di applicazione dell'Iva poiché il loro operato ricade tra le operazioni relative alle monete e alle banconote; tuttavia sono attività che rilevano ai fini Ires e Irap, al netto dei relativi costi di esercizio.

L'agenzia spiega anche come valutare i bitcoin di cui la società dispone a fine esercizio: si deve considerarne il valore normale, ossia la miglior quotazione disponibile sul mercato in quel momento. In particolare, ai sensi dell'art. 10 Dpr 633/1972, si è ritenuto che l'attività remunerata attraverso commissioni pari alla differenza tra l'importo corrisposto dal cliente e la suddetta miglior quotazione reperita sul mercato debba essere considerata ai fini IVA quale prestazione di servizi.

29- Conclusioni

In un periodo caratterizzato da una importante crisi economico-finanziaria, le monete virtuali si propongono come un sistema di scambi monetari alternativo potenzialmente orientato a scardinare gli equilibri di natura economico-finanziaria e forse anche sociali. La sfida parte con una feroce critica nei confronti delle banche Centrali e in generale del potere costituito, questi ritenuti responsabili di aver reso tossica l'economia globale perpetrando una manipolazione dell'offerta monetaria, reputata asservita a potentati economico-affaristici. Grazie a un meccanismo peer-to-peer, basato su un protocollo informatico, Bitcoin si è offerto come una valuta-unità di conto e un sistema di pagamento che fosse svincolato da un controllo centrale. Il suo perno di funzionamento è in realtà la stessa community degli utilizzatori (chiamati in gergo "nodi" della rete).

Però occorre considerare che l'avvento e la rapida diffusione delle monete virtuali genera contemporaneamente opportunità e rischi. Tra gli obiettivi di questa trattazione c'era l'analisi di alcuni punti deboli di Bitcoin. È stata quindi condotta un'analisi comparativa di Bitcoin con le valute a corso legale, arrivando a dimostrare come difficilmente la prima potrà imporsi in futuro come moneta alternativa: dal confronto emerge che bitcoin non sembra abbastanza robusto da essere considerato alla pari delle valute a corso legale, in quanto non assolve pienamente le comuni funzioni di una moneta (mezzo di scambio, unità di conto e riserva di valore). Inoltre tra i sui rischi deve essere menzionata la eccessiva volatilità del suo valore che si aggiunge a una strutturale lacuna nei temi della sicurezza informatica delle tutele degli utenti.

Presumibilmente il futuro di bitcoin non risiede tanto nelle sue peculiari caratteristiche, quanto sulle bontà delle novità della tecnologia su cui si basa la sua creazione. Ci si riferisce in particolare alle innovative funzionalità della blockchain che si prestano molto bene ad applicazioni nei campi più svariati offrendo un potenziale contributo

tangibile allo sviluppo in molti ambiti; giuridico, commerciale, sociale. Un esempio di ciò proviene da alcune nuove alt-coin che hanno raggiunto il mercato successivamente a Bitcoin. Invero, in considerazione della difficoltà a qualificare bitcoin come una moneta, si potrebbe identificarlo piuttosto come moneta complementare, ossia come a uno strumento di commutazione mediante il quale si rende possibile scambiare beni e servizi in affiancamento quindi alla moneta tradizionale. Il fondamento della moneta complementare non è tanto la dimensione pubblica e legale, ma quella più propriamente negoziale degli accordi tra privati, che appunto raggiungono un agreement circa la sua emissione, circolazione e accettazione. In altre parole, le monete complementari rientrano nell'antica definizione di moneta. Moneta è ciò che, in base a un accordo dentro a una comunità, si accetta di impiegare come bene di scambio nelle negoziazioni. L'emissione di valute complementari in questa accezione potrebbe essere compiuta da soggetti di diversa natura, quali ad esempio associazioni, cooperative, o, ad esempio, aziende che offrono un servizio a cui aderiscono persone fisiche e altre aziende. Si rimanda per esempio al Sardax, una moneta complementare nata in Sardegna alcuni anni fa e molto simile a Bitcoin per la caratteristica di poter circolare soltanto sul web.

Un altro problema oggi molto attuale riguarda il crescente impiego di bitcoin (e di molte altre criptovalute) per finalità illegali come, ad esempio all'interno di pratiche di riciclaggio di denaro sporco o di finanziamento al terrorismo. Il problema è normalmente legato al luogo ove si svolgono queste transazioni (il dark web). Questo rende praticamente impossibile il monitoraggio delle operazioni che avvengono al suo interno. Nel tempo si è osservata infatti una diversificazione in un crescendo di complessità delle tecniche adottate all'interno del sistema criminale per riciclare i soldi sporchi e per nascondere i movimenti di capitali. Sarebbe quindi sensata la decisione della Commissione Europea di concentrare l'intervento normativo sui quei soggetti che fanno da nodi che legano il mondo virtuale e il mondo legale, ossia gli exchanger, cercando di estendere a questi ultimi gli obblighi di adeguata verifica della clientela, di registrazione dati e di comunicazione delle operazioni sospette alle autorità competenti.

Pur nella sua utilità, l'intervento della Commissione Europea va però visto soltanto come il primo passo su un cammino di regolamentazione del mondo delle monete virtuali. Ancora sono molte infatti le questioni irrisolte. Prima di tutto si osserva che la maggior parte delle operazioni nascoste viene svolta al di fuori dei flussi di traffico gestiti dagli organismi di exchange. In secondo luogo, come indicato anche da una seconda "*opinion on virtual currencies*" dell'EBA, la possibilità di lasciare ai singoli Stati membri la scelta di assoggettare le valute virtuali a un regime di licenza o di

registrazione rischia di indebolire le finalità della direttiva; occorrerebbe chiarire quale tra i due regimi sia il più adatto a realizzare le finalità contenute nella direttiva e, ove ciò non sia possibile, di chiarire almeno quali debbano essere i requisiti minimi per ottenere la licenza o la registrazione.

Se infine spostiamo l'attenzione dall'ambito europeo a quello internazionale, è bene ricordare che, in considerazione della natura globale delle criptovalute, ogni sforzo potrebbe diventare vano senza che si fissi un inquadramento normativo comune tra tutti i sistemi giuridici. Ci si trova quindi in accordo con le posizioni dall'EBA, e si sostiene sia assolutamente necessario che venga introdotto un organismo non governativo che regoli e controlli l'utilizzo di un virtual currency scheme, col sostegno di un istituto giuridico ad hoc che risulti essere il più possibile condiviso a livello internazionale.

In conclusione, nelle attività di prevenzione e monitoraggio si profila un ruolo di crescente importanza per le agenzie di supporto private (ad esempio Elliptic e Chainalysuis) grazie al loro bagaglio di conoscenze specifiche e software dedicati in grado di individuare gli schemi di riciclaggio che spesso invece mancano alle autorità pubbliche.

Bibliografia

AA.VV., Bitcoin e criptovalute. Profili fiscali, giuridici e finanziari, Maggioli, Roma, 2018

Banca d'Italia (2015), "Avvertenza sull'utilizzo delle cosiddette valute virtuali", disponibile all'indirizzo: https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/AVVERTENZA_VALUTE_VIRTUALI.pdf

Bonneau Joseph, *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, in Ieee Security and Privacy, maggio 2015

Capoti Davide, Bitcoin revolution. La moneta digitale alla conquista del mondo, Hoepli, Milano, 2017

Financial Action Task Force, Virtual Currencies Key Definitions and Poten al AML/CFT Risks, giugno 2014

Florindi Emanuele, Deep web e bitcoin, Vizi privati e pubbliche virtù della navigazione in rete, Imprimatur, Milano, 2018

GAFI/FATF Report (2014), "Valute Virtuali, definizioni chiave e potenziali rischi in ambito antiriciclaggio e finanziamento del terrorismo", http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Galullo Roberto (2017), B*itcoin, il riciclaggio invisibile di mafie e terrorismo internazionale*, in Il sole 24 ore, disponibile a: http://www.econopoly.ilsole24ore.com/2016/07/08/bitcoin-e-antiriciclaggio-i-primi-passi-delleuropa-per-un-quadro-legislativo/.

Houy Nicolas, *The bitcoin mining game*, in Working Paper Gate, n. 12, 2014

Koop Pierre, *L'analyse économique des organisations criminelles*, in "vivre avec les drogues: régulations, politiques, marchées, usages" Collection Communications n° 62, Seuil, Paris, 1996

Rapporto UIF 2013, disponibile a https://uif.bancaditalia.it/pubblicazioni/rapporto-annuale/2014/index.html

Righetti Renato, Tecniche di occultamento della ricchezza da parte delle organizzazioni criminali, in Violante, Luciano – I soldi della mafia: rapporto ’98, Laterza, Bari, 1998

Santelli Filippo, *Da Ripple a Cash, ecco le valute virtuali che sfidano il Bitcoin*, in La Repubblica.it, 3 gennaio 2018

Sicignano Gaspare Jucan, Bitcoin e riciclaggio, Giappicchelli, Torino, 2019