

*Quaderni di*  **C.R.S.T.**

Centro Ricerca Sicurezza e Terrorismo

---

Direttore Ranieri Razzante

**Alessandro Anselmi**

*Onion routing, cripto-valute  
e crimine organizzato*

  
**Pacini  
Giuridica**



1. Dante Gatta, *Africa occidentale e Sabel: problematiche locali dalla valenza globale. Tra terrorismo, traffici illeciti e migrazioni*
2. Miriam Ferrara e Dante Gatta, *Lineamenti di counter-terrorism comparato*
3. Alessandro Lentini, *Selected Issues in Counter-terrorism: special investigative techniques and the international judicial cooperation Focus on the European Union*
4. Michele Turzi, *The effects of Private Military and Security Companies on local populations in Afghanistan*
5. Ilaria Stivala, *Hezbollah: un modello di resistenza islamica multidimensionale*
6. Alessandro Anselmi, *Onion routing, cripto-valute e crimine organizzato*
7. Fabio Giannini, *La mafia e gli aspetti criminologici*

© Copyright 2019 by Pacini Editore Srl

*Realizzazione editoriale*



Via A. Gherardesca  
56121 Pisa

*Responsabile di redazione*  
Gloria Giacomelli

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume /fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941 n. 633.

## Indice

<b>Introduzione</b> .....	3
<b>Capitolo I – Onion Routing e Cripto-valute</b> .....	6
1.1 Introduzione all’anonimato in rete .....	6
1.2 The Onion Router- TOR.....	8
1.2.1 I servizi nascosti .....	11
1.2.2 La suddivisione del Web .....	13
1.3 Le Cripto-valute .....	15
1.3.1 L’evoluzione della cripto-valuta.....	20
1.3.2 Altcoin: le altre cripto-valute.....	21
1.3.2.1 <i>Le cripto-valute anonime</i> .....	21
<b>Capitolo II - Il Crimine Organizzato nel mondo della rete</b> .....	24
2.1 Introduzione al crimine organizzato.....	24
2.2 Criminalità informatica organizzata: vecchi e nuovi modelli. ....	27
2.2.1 Lo scenario del crimine organizzato in rete: il modello McGuire.....	28
2.2.3 Incontro tra due culture criminali .....	31
2.3 I nuovi ruoli del crimine organizzato digitalizzato .....	34
2.3.1 Fornitori di prodotti e servizi.....	35
2.3.2 Investitori in cripto-valute .....	35
2.3.3 Mano Guida: .....	37
<b>Capitolo III - L’economia sotterranea del crimine: dalle Darknet al Cybericiclaggio</b> .....	39
3.1 Il mondo delle reti oscure: i cripto-mercati .....	39
3.1.1 Modelli di mercati neri della rete.....	41
3.1.2 Prodotti e servizi .....	44
3.1.2.1 <i>Droga</i> .....	45
3.1.2.2 <i>Falso Documentale</i> .....	46
3.1.2.3 <i>Banconote false e carte di credito</i> .....	46
3.1.2.4 <i>Armi</i> .....	47
3.1.2.5 <i>Malware</i> .....	47
3.2 Gli altri illeciti nelle darknet.....	48
3.3 Il Cybericiclaggio .....	50
3.3.1 Il riciclaggio di denaro: verso nuove frontiere .....	51
3.3.2 Il nesso con le cripto-valute.....	54
3.3.2.1 <i>Il caso riportato dalla UIF</i> .....	56

<b>Capitolo IV- Aspetti di regolamentazione e controllo</b> .....	58
4.1 Approccio penalistico alle sfide del Crimine Informatico .....	58
4.2 Normativa e istituti di contrasto al crimine informatico .....	59
4.2.1 Il Livello Internazionale .....	60
4.2.2 Il livello Europeo .....	66
4.2.3 Il livello italiano.....	68
4.2.3.1 Legame tra aspetto normativo ed operativo nel contrasto ai reati nelle Darknet .....	69
4.3 Attività di contrasto dell'Interpol .....	70
4.4 Prospettive normative e politiche pubbliche nel contrasto all'economia sotterranea del crimine organizzato .....	72
4.4.1 La normativa applicabile .....	73
4.4.2 Politiche pubbliche nella lotta contro l'anonimato del crimine in rete.....	75
4.4.3 Possibili strategie d'intervento in tema di diritto penale sostanziale: Unione Europea e Italia .....	77
4.4.3.1 Criminalizzare l'accesso di alcune aree di TOR.....	79
4.4.3.2 Limiti all'operatività del crimine organizzato nelle reti (dal 416 al 416bis c.p.) .....	80
4.5 L'ambito del Cybericclaggio.....	84
4.5.1 L'azione Internazionale: il GAFI.....	84
4.5.2 Le Direttive Europee.....	86
4.5.3 L'Ordinamento Nazionale .....	89
4.5.4 Nuove prospettive nello scenario italiano.....	92
<b>Conclusioni</b> .....	95
<b>Bibliografia</b> .....	99

## Introduzione

L'incremento dei mezzi di comunicazione dovuto alle innovazioni tecnologiche, la libera circolazione di capitali, dei servizi e degli individui a livello internazionale e l'unificazione dei mercati globali, hanno radicalmente cambiato il contesto socioeconomico in cui viviamo. Di contro, il parallelo processo di *governance* non è riuscito a tenere il passo con gli sviluppi di tale globalizzazione economica. In queste circostanze anche il crimine organizzato ha mutato la sua natura, diventando transnazionale.

Gli Stati oggi si ritrovano a dover controllare attività criminali che passano da una giurisdizione all'altra, dovendo affrontare il problema delle disomogeneità legislative e i limiti posti all'operatività degli organi di controllo. Specialmente con l'arrivo delle nuove tecnologie computerizzate oggi esiste la possibilità di inviare ingenti somme di denaro da una parte all'altra del mondo ed aver accesso a determinati spazi della rete nei quali perpetrare commerci illeciti. Per questo motivo si presuppone che per combattere la criminalità organizzata ci sia bisogno di una forte cooperazione tra paesi seguita da una legislazione internazionale adeguata.

La Convenzione di Palermo delle Nazioni Unite contro la criminalità organizzata transnazionale (2000) è stato un importante primo passo in questo senso, coinvolgendo un numero enorme di Stati nella lotta alle nuove forme di reati transfrontalieri compiuti da associazioni criminali strutturate e radicate in differenti paesi.

L'anno seguente il Consiglio d'Europa istituisce il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, per mezzo della Convenzione di Budapest (2001).

A quasi vent'anni dagli accordi presi, le due Convenzioni rappresentano ancora oggi i due strumenti normativi di rilievo a livello internazionale nella lotta alla criminalità organizzata e ai crimini commessi attraverso le reti telematiche.

Tuttavia, nell'arco degli ultimi dieci anni, l'enorme sviluppo dell'elettronica di consumo (l'uso degli *smartphones*) il *network computing*, l'anonimato in rete, le nuove piattaforme e-commerce, i bitcoin, le chat e i social rendono l'interazione con le tecnologie digitali parte integrante del modo di vivere le azioni quotidiane.

Le organizzazioni criminali, al passo con gli sviluppi sociali, sono andate a rinnovare metodi e tecniche attraverso le quali perpetrare i propri interessi.

Tra i diversi usi impropri delle tecnologie informatiche, le organizzazioni criminali tradizionali e i nuovi gruppi organizzati online, si impegnano negli spazi anonimi della rete per dar vita a vere e proprie attività commerciali dedite alla compravendita di droga, armi, *malware*, falso documentale e

altri prodotti e servizi illeciti. Inoltre, le cripto-valute, quali nuovi *asset class*, sono stati sfruttati non solo come mezzo di pagamento per i mercati occulti della rete, ma come nuovo strumento adatto per riciclare i proventi illeciti.

Oggi queste realtà poco regolamentate, rappresentano, solo in Europa, affari da decine di milioni di euro al mese, che vanno a rinforzare l'economia delle diverse organizzazioni criminali presenti sul territorio.

La crescita di nuovi mezzi attraverso i quali realizzare condotte illecite, pone in essere la necessità di aggiornare i passati strumenti normativi e di intervenire politicamente in senso legislativo, prendendo consapevolezza dei nuovi fenomeni criminali in crescita.

Il tema del presente lavoro indaga il rapporto che l'*onion routing* (la tecnica che rende anonime le comunicazioni in rete) e le cripto-valute hanno con le odierne forme di crimine organizzato, cercando di apportare dei contributi da un punto di vista normativo alle maggiori problematiche derivanti da questa relazione.

Ai fini di un'analisi più possibile esaustiva dell'argomento, questo studio prende in considerazione diverse discipline. Partendo da un ambito tecnico-informatico si passerà a quello di tipo storico-sociologico per poi spostarsi nell'esplorare diverse aree giuridiche, quali il diritto penale, il diritto internazionale, il diritto europeo e il diritto bancario.

Lo sviluppo del tema sarà strutturato in quattro capitoli che vanno parzialmente a circoscrivere i diversi ambiti trattati.

Il primo capitolo si occuperà dell'ambito tecnico informatico ed è diviso principalmente in due macro-aree: una riguardante le tecniche d'anonimato delle comunicazioni online, l'*onion routing*, e l'altra riguardante le cripto-valute, i nuovi mezzi di pagamento. Si descriverà il funzionamento e l'implementazione dei siti *.onion* attraverso la rete TOR, cercando di comprendere il legame che queste reti hanno con le cripto-valute, andando ad indagare le diverse configurazioni delle monete virtuali.

Nel secondo capitolo si affronterà il rapporto tra le tecnologie di rete e il crimine organizzato, delineando come quest'ultimo sia mutato nel processo di digitalizzazione. Si concentrerà l'attenzione su due forme di criminalità organizzata: quella a stampo tradizionale - come possono essere le associazioni mafiose - e quella cyber, ovvero nuovi gruppi criminali operanti esclusivamente attraverso l'uso di canali telematici.

Compresi i ruoli che tali organizzazioni svolgono in relazione alle tecniche digitali, il terzo capitolo descriverà nello specifico le condotte illecite connesse. Dalle attività svolte nei mercati della rete

oscura all'ambito del riciclaggio di denaro sporco per mezzo dei nuovi mezzi di pagamento e delle cripto-valute.

Il quarto capitolo infine approfondirà l'ambito giuridico andando ad esporre la normativa e le azioni di contrasto concernenti sia il web oscuro (meglio conosciuto nella versione inglese di dark web) che il cybericiclaggio. Mentre quest'ultimo settore possiede un suo corpus di leggi, sviluppate principalmente nell'arco degli ultimi anni, per l'ambito del web oscuro o dei mercati occulti della rete, ci si ritrova davanti ad un panorama giuridico mancante.

Seguendo l'analisi normativa, si cercherà di offrire degli strumenti di riflessione utili a capire come limitare l'anonimato in rete, proponendo infine delle possibili soluzioni che possano andare a riempire alcune delle lacune poste dall'uso improprio delle reti da parte della criminalità organizzata.

## Capitolo I – Onion Routing e Cripto-valute

### 1.1 Introduzione all'anonimato in rete

Ogni giorno più di due milioni di persone<sup>1</sup> usano le tecnologie di *onion routing* per rendere anonime le loro comunicazioni su Internet.

L'intensificazione di questo fenomeno procede di pari passo ad una crescente preoccupazione relativa alla protezione della privacy. Nelle dinamiche di rete questo vuol dire avere il controllo sulla riservatezza delle proprie attività come foto, video, comunicazioni via web che, in una società in cui siamo in contatto costante con il digitale e la rete, è di fondamentale importanza.

Un'importanza tale da far affermare al presidente della Corte Suprema degli Stati Uniti che se gli alieni facessero visita al pianeta terra potrebbero pensare che i dispositivi che utilizziamo giornalmente, come *smartphones* o *tablet*, siano una parte integrante dell'anatomia umana<sup>2</sup>. Alla base di questa supposizione si pone in essere il valore di quell'insieme di attività sopracitate che nella loro totalità rappresentano i dati.

Oggetto della normativa sulla privacy sono i dati personali, ovvero “qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”<sup>3</sup>.

Oggi l'economia odierna è sempre più basata sull'impiego di canali digitali e il trattamento<sup>4</sup> dei dati personali in rete rappresenta per le aziende che operano online un mezzo efficace per strutturare strategie tese ad influenzare i comportamenti d'acquisto delle persone, i cui dati di consumo sono stati definiti nel rapporto 2011 del World Economic Forum report come "il nuovo petrolio"<sup>5</sup>. Queste pratiche che oggi giorno fanno parte del business internazionale nella nuova era dei *big data*

---

<sup>1</sup> Tor Metrics. Si veda il link: <https://metrics.torproject.org/userstats-relay-country.html?start=2018-09-20&end=2018-12-19&country=all&events=on>

<sup>2</sup> Chief Justice John G. Roberts Jr., writing for the court, was keenly alert to the central role that cell phones play in contemporary life. They are, he said, “such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.”

Si veda il link: <https://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html>

<sup>3</sup> D.Lgs. 196/03, Codice Privacy, Art. 4 Definizioni, lettera b).

<sup>4</sup> Quando si parla di trattamento dei dati personali, la legge italiana ( in maniera specifica il Codice Privacy), intende: “qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati”.

<sup>5</sup> Professor Xavier Sala-i-Martin, World Economic Forum Editor, The Global Competitiveness Report 2011–2012

possono avere molteplici rovesci della medaglia, come l'abuso dei dati personali fino ad arrivare alla manipolazione dei metadati<sup>6</sup> da parte sia di soggetti privati che pubblici.

La rivelazione di indirizzi IP, dei dati di navigazione, l'estorsione di informazioni on line al fine di ricatto, fino ad arrivare ai casi Snowden e Cambridge Analytica ha fatto sì che sempre più utenti scelgano di voler rafforzare maggiormente la propria privacy on line navigando anonimamente su Internet.

Le soluzioni all'avanguardia che soddisfano questo bisogno di anonimato sono una serie di tecniche basate sulla crittografia a chiave pubblica<sup>7</sup> che consentono di nascondere le comunicazioni e il loro contenuto sfruttando il sistema delle telecomunicazioni via web. Sin dal 1981 David Lee Chaum, informatico statunitense, elabora i primi sistemi di comunicazione anonima su Internet, basati sugli algoritmi crittografici a chiave pubblica e a chiave privata. Tale sistema, denominato anche crittografia asimmetrica, permette ad un utente A di inviare un messaggio ad utente B, in modo tale che solo B possa (con l'uso della chiave privata) decodificare il messaggio. Dal '96 vennero sfruttate le nuove tecnologie di rete, quali i router, per inoltrare messaggi criptati protetti da più strati di crittografia. Da questi primi esperimenti i ricercatori coniarono il termine *onion routing*, traducibile in italiano come l'instradamento della cipolla. Oggi tale tecnica è meglio conosciuta attraverso il suo sistema di implementazione TOR (*The Onion Routing*), il quale cerca di trovare un equilibrio tra privacy e prestazioni, consentendo comunicazioni anonime a bassa latenza<sup>8</sup> adatte alle tipiche attività quotidiane svolte in rete (ad esempio, la navigazione web e la messaggistica istantanea).

Tali caratteristiche rendono così le *onion network*, impermeabili ad eventuali tipi di intrusione, risultando strumento ideale per chi ne volesse fare un uso improprio. Infatti, questa tecnica d'anonimato viene sempre più utilizzata da gruppi criminali in tutto il mondo per perpetrare molteplici interessi. Nell'arco dell'ultimo decennio la criminalità organizzata ha sfruttato spazi della rete anonimi nei quali creare veri e propri mercati criminali online. Queste attività commerciali, che rappresentano a livello internazionale un giro da miliardi di euro all'anno, devono assicurare transazioni sicure tra acquirenti e compratori. Pertanto, le cripto-valute si prestano perfettamente a

---

<sup>6</sup> In informatica il metadato è un sistema strutturato di dati sui dati. Il suo scopo è di descrivere il contenuto, la struttura e l'ambito in cui s'inquadra un documento informatico, per la sua gestione e archiviazione nel tempo ( dalla seguente fonte: <https://www.bucap.it/focus/conservazione-digitale/conservazione-digitale-i-metadati> ).

<sup>7</sup> La crittografia a chiave pubblica, o crittografia asimmetrica, è un sistema crittografico che utilizza coppie di chiavi: chiavi pubbliche che possono essere diffuse ampiamente e chiavi private che sono conosciute solo dal proprietario. Consideriamo due soggetti A e B: se A vuole mandare un messaggio esclusivamente a B, questi deve cercare su un elenco la chiave pubblica di B attraverso la quale potrà criptare il messaggio. Per leggere il messaggio, B deve possedere la sua chiave privata o inversa per decifrarne il contenuto, che in questo modo rimarrà oscuro a tutti compreso al mittente, il quale non possedendo la chiave privata non avrà modo di poter leggere il testo da lui stesso composto.

<sup>8</sup> Nel linguaggio informatico, la latenza corrisponde ad una misura del ritardo di tempo (alta/bassa latenza) richiesto da un sistema, affinché le informazioni possano viaggiare attraverso una rete.

tal requisito in quanto possono bilanciare tra trasparenza della transazione, attraverso la *blockchain* (un grande registro delle transazioni online), e anonimato dell'utente, attraverso il sistema della crittografia asimmetrica. Dal 2015, l'anonimato della transazione viene rafforzato ulteriormente con l'introduzione di nuove cripto-valute quali Monero e Zcash.

L'insieme di queste caratteristiche unite alla mancanza di controllo sulla tracciabilità da parte di istituti centralizzati, l'affidabilità garantita dalla *blockchain* e l'immediatezza attraverso la quale trasferire ingenti somme di denaro a livello internazionale rende le cripto-valute un mezzo ideale per ripulire i proventi illeciti. Le organizzazioni criminali infatti, in Italia come all'estero, sfruttano le nuove monete online per riciclare denaro e trasferire, con sempre maggior facilità, una buona parte del fatturato in paradisi fiscali e società offshore.

Sia *l'onion routing* che le cripto-valute diventano pertanto, insieme o separatamente, facili strumenti per scampare dai controlli delle autorità.

Prima di calarsi in questo scenario nello specifico, ovvero capire i soggetti operanti e le condotte conseguenti agli usi impropri, è necessario offrire un quadro tecnico-informatico relativo al funzionamento di queste nuove tecnologie.

## 1.2 The Onion Router- TOR

Nel 1996, tre ricercatori della NRL, Goldschlag, Reed e Syverson, pubblicarono il saggio "Hiding Routing Information"<sup>9</sup> coniando il termine *the onion routing*, in riferimento alla tecnologia che permetteva alle forze statunitensi di poter comunicare online per la prima volta in maniera anonima. Per capirne il funzionamento è importante partire da una rete di *router*<sup>10</sup>. Supponiamo che la rete formi un grafico connesso, il che significa che esistono percorsi che legano più *router*.

Attraverso questi percorsi, criptati, fluiscono i dati di più *host* privati (dispositivi alla sorgente delle trasmissioni). In tal modo gli utenti usano un set predefinito di *router* crittografato a cipolla. Tale metafora deriva dalla configurazione della rete basata sulla tecnica per la quale i messaggi sono incapsulati in "strati" di crittografia per poi essere trasmessi attraverso un percorso di nodi, scelti casualmente dai *router*, ognuno dei quali sfoglia via, metaforicamente, un singolo strato di crittografia, scoprendo così il nodo successivo fino ad arrivare a quello di destinazione. Oltre che il messaggio in tutto questo anche il mittente rimane anonimo perché ciascun nodo intermedio conosce solo la posizione del nodo immediatamente precedente e di quello immediatamente

---

<sup>9</sup> "Nascondere Informazioni di instradamento".

<sup>10</sup> Un router (CERN, 1987) è un dispositivo di rete che inoltra i pacchetti di dati tra le reti di computer. I router eseguono le funzioni di indirizzamento del traffico su Internet. I dati inviati attraverso Internet, come una pagina Web o e-mail, sono sotto forma di pacchetti di dati. Un pacchetto viene generalmente inoltrato da un router a un altro router attraverso le reti che costituiscono un internetwork fino a raggiungere il nodo di destinazione.

successivo. Per comunicare con un destinatario, un utente seleziona tale set di *routers* a cipolla e costruisce un circuito o una connessione persistente su quella sequenza. I messaggi da e verso la destinazione vengono inviati sul circuito. Da qui il traffico, invece di prendere un percorso diretto dalla fonte alla destinazione, viene inoltrato tramite un relè<sup>11</sup> casuale, passando per punti qualunque sparsi nel globo. Ogni volta che il segnale passa per un nodo<sup>12</sup>, uno strato di crittografia viene rimosso, rivelando dove si trova il pacchetto per andare avanti; il vantaggio è che il nodo conosce solo i dettagli dell'indirizzo precedente e di quello successivo ma non l'intera catena attraverso la quale passa il segnale, garantendo così l'anonimato tra i due comunicanti. Inoltre, tale sistema, non richiede che il destinatario partecipi al protocollo della rete di anonimato, permettendo così di allargare le proprie attività all'intera rete.

Questo nuovo progetto negli anni successivi venne finanziato dal Dipartimento della Difesa statunitense che diede vita ad ulteriori miglioramenti quali i così detti servizi nascosti, vere e proprie pagine web anonime create da indirizzi anonimi, diventate strumento controverso negli anni proprio perché sfruttate dai criminali per vendere prodotti e servizi illegalmente. La moderna rete TOR è stata sviluppata nell'ottobre 2003, come un progetto di transizione da prodotto interno del laboratorio di ricerca navale degli Stati Uniti a quello open source di proprietà di un'organizzazione no profit, la *Electronic Frontier Foundation* (EFF)<sup>13</sup>, comunque di sua influenza.

Da questo punto in poi, sono state sviluppate ulteriori tecniche all'avanguardia e la gestione della rete è progressivamente andata in mano alla "Tor Project", un'organizzazione non-profit statunitense composta dai progettisti originali e da nuovi arrivati. Fondata nel dicembre 2006, l'organizzazione fu sponsorizzata fiscalmente dalla EFF, insieme ad altri sostenitori finanziari che hanno incluso diverse entità quali: U.S. International Broadcasting Bureau, Internews, Human Rights Watch, l'Università di Cambridge, e Google. Sebbene lo scopo iniziale del progetto *Onion Routing* fosse quello di proteggere le comunicazioni online di intelligence degli Stati Uniti, il

---

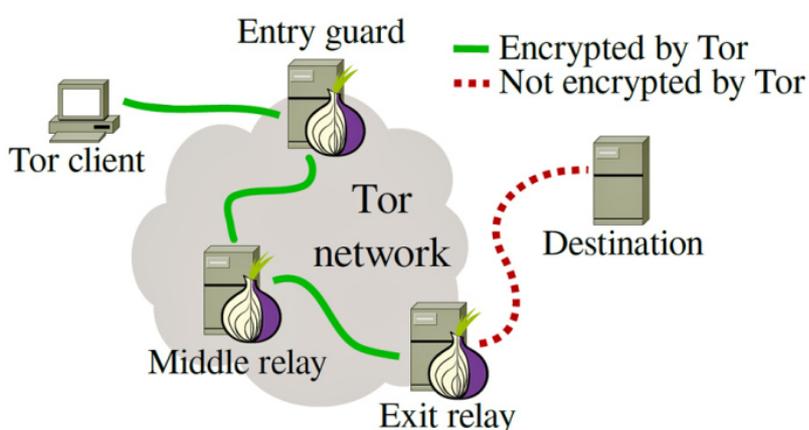
<sup>11</sup> Un relè è un interruttore elettronico utilizzato per l'apertura o la chiusura di un circuito. Hanno la possibilità di comandare una serie di circuiti sulla base di variazioni di una o più grandezze nel circuito, o nei circuiti, di alimentazione. Una rete di relè è un'ampia classe di topologia di rete comunemente utilizzata nelle reti wireless, dove l'origine e la destinazione sono interconnesse per mezzo di alcuni nodi. Una rete di relè è un tipo di rete utilizzata per inviare informazioni tra due dispositivi, come ad esempio tra un server e un computer, che sono troppo lontani per inviare le informazioni direttamente tra loro. Pertanto, la rete deve inviare o "trasmettere" le informazioni a diversi dispositivi, quali i nodi, che trasmettono le informazioni alla loro destinazione. [Un esempio di una rete di relè più in generale è Internet. Un utente può visualizzare una pagina Web da un server a metà del mondo inviando e ricevendo le informazioni attraverso una serie di nodi connessi]. In questo modo funziona la rete TOR, passando il segnale attraverso più server.

<sup>12</sup> Un nodo (o come si è accennato in precedenza un *host*) è un punto di redistribuzione della comunicazione. Ovvero un qualsiasi dispositivo hardware del sistema in grado di comunicare con gli altri dispositivi che fanno parte della rete.

<sup>13</sup> un'organizzazione internazionale non profit di avvocati e legali rivolta alla tutela dei diritti digitali e della libertà di parola nel contesto dell'odierna era digitale.

software TOR è ora distribuito con licenza BSD<sup>14</sup> ed utilizzato da milioni di persone al mondo, da aziende, attivisti politici, informatori e media.

Oggi, basandosi sul sistema della rete di *router* elaborata dai fondatori e grazie alle innovazioni portate avanti dalle generazioni successive, l'implementazione del protocollo di *onion routing* attraverso TOR si può dividere in diverse fasi. Una volta che l'utente ha composto il messaggio da inviare, il browser TOR, correttamente installato sul proprio computer, seleziona tre server di TOR in maniera casuale scegliendo tra più di seimila sparsi in tutto il globo<sup>15</sup>. Il grafico seguente mostra un esempio di come avvenga la trasmissione:



16

Come riportato, il software crea un percorso tra questi tre *server* iniziando con il crittografare il messaggio ed inviarlo al primo *server*, ovvero al nodo di guardia (Entry Node). Il nodo conosce l'indirizzo IP da cui proviene il messaggio ma non può leggere il messaggio originale perché ci sono ancora due livelli di crittografia aggiuntivi. Tuttavia, il software include l'indirizzo del prossimo server nel percorso di crittografia del messaggio. A questo punto il primo nodo invia il messaggio al *server* nel mezzo del percorso (il Middle Relay). Questo *server* rimuove il secondo livello di crittografia e, come nel passaggio precedente, non è ancora possibile leggere il messaggio perché esiste un ulteriore livello di crittografia. Conseguentemente ripete l'operazione rimuovendo il proprio strato di crittografia indicando l'indirizzo del nodo di uscita (Exit Relay o Exit Node). Il nodo di uscita rimuove il livello finale di crittografia ed è quello che ha modo di connettersi con l'internet pubblica in modo di inoltrare al destinatario il messaggio. Ciò significa che il nodo di uscita può leggere il messaggio originale, tuttavia, poiché il messaggio è stato inoltrato attraverso gli altri server nel percorso, l'*exit node* non sa chi ha inviato il messaggio. Nessun server sa o può

<sup>14</sup> Berkeley Software Distribution (BSD) è un tipo di licenza permissiva per software

<sup>15</sup> Tor Metrics, si veda il link: <https://metrics.torproject.org/networksize.html>

<sup>16</sup> Si veda il link: <https://www.whizlabs.com/blog/tor-the-onion-router/>

sapere sia da dove viene il messaggio o che cosa dice. Questo è il modo in cui TOR fornisce l'anonimato.

Ci sono motivi legittimi per cui qualcuno potrebbe voler interagire con altri utenti su un servizio nascosto; per esempio, una persona potrebbe voler diffondere letteratura, informazioni o documenti liberamente dalle regole imposte da un regime repressivo. Tuttavia, lontano da tutti gli utenti e dagli usi legittimi di questo spazio, i servizi nascosti TOR, principalmente quelli a scopo commerciale, appaiono come mercati non convenzionali che offrono una gamma di prodotti e servizi illegali.

### 1.2.1 I servizi nascosti

I servizi nascosti consentono di eseguire una qualsiasi prestazione della Internet (ad esempio un sito Web) in modo tale che i *client* della pagina non conoscano l'effettivo indirizzo IP del server<sup>17</sup>. Ciò si ottiene instradando tutte le comunicazioni tra il *client* e il servizio nascosto attraverso il punto di “rendez-vous” che collega i circuiti anonimi al *client* e al *server*.

*TorHiddenServices*<sup>18</sup> è una versione migliorata dei servizi nascosti che sono stati introdotti e implementati nel 2004. Un *client* oggi deve conoscere una chiave condivisa e utilizzare questa chiave per decodificare la parte di un descrittore di servizi nascosti contenente i punti nei quali si potrà introdurre. Successivamente deve usare delle informazioni nella parte crittografata per autenticarsi in qualsiasi punto di introduzione che utilizza per accedere al servizio nascosto stesso. L'uso di tale autenticazione permette solo agli utenti autenticati di poter sapere se il servizio nascosto è online.<sup>19</sup>

Queste pagine non sono raggiungibili dai normali motori di ricerca ma da piattaforme specifiche, come Ahima<sup>20</sup>. Per accedervi, si richiede l'installazione sul proprio dispositivo del browser TOR con il quale è possibile raggiungere un livello ottimale di anonimato della navigazione. Il software TOR che funziona su un *host* TOR creerà un *file directory*<sup>21</sup> locale, assegnando un numero sulla porta d'accesso al servizio nascosto e al momento della configurazione di quest'ultimo genererà una coppia di chiavi, pubblica e privata. A questo punto TOR crea un *hostname*<sup>22</sup> di 16 caratteri attraverso la funzione di *hash*<sup>23</sup> rendendo conforme il nome ai *server* responsabili del dominio di

---

<sup>17</sup> Il nodo terminale della rete che instrada il client alla pagina web da lui fornita.

<sup>18</sup> Tor Rendezvous Specification, si veda il link: <https://gitweb.torproject.org/%20torspec.git/tree/rend-spec.txt>

<sup>19</sup> Si veda il link: [www.blog.torproject.org/top-changes-tor-2004-design-paper-part-1](http://www.blog.torproject.org/top-changes-tor-2004-design-paper-part-1)

<sup>20</sup> Si veda il link: <https://ahmia.fi/>

<sup>21</sup> In informatica, una *directory* è una struttura di catalogazione del file system che contiene riferimenti ad altri file di computer e probabilmente ad altre *directory*.

<sup>22</sup> Ovvero il nome identificativo di un dispositivo (*host*) all'interno della rete ( che puo associarsi, attraverso un DNS, all'indirizzo IP).

<sup>23</sup> Da Hash di Adam Back, le funzioni di hash possono essere impiegate anche per la generazione di stringhe pseudorandom o per la derivazione di chiavi e password da una singola chiave o password sicura.

“radice” o DNS (Domain Name System). Questi sistemi, che si pongono come servizi di traduzione di *host* in indirizzi IP, sono database distribuiti che risolvono le singole parti di un indirizzo simbolico in maniera gerarchica. Ad esempio, il *server* DNS responsabile del dominio .it, una volta consultato (mettiamo da agenzie governative) potrà fornire informazioni riguardanti *server* di *secondo livello* <sup>24</sup>, e risalendo potrà restituire l’indirizzo IP<sup>25</sup>. Questo all’interno del protocollo *hidden service* di TOR non è possibile grazie allo “pseudo” dominio di primo livello, detenuto dalla rete TOR: i domini *.onion* esclusi dal global-DNS. Questo protocollo aiuta i servizi a rendere note le loro esistenze e aiuta i clienti a trovare i servizi, preservando l’anonimato e la posizione (indirizzo IP) di entrambi. In questo modo, per creare un determinato servizio nascosto un *host* TOR deve “pubblicizzare” un *service descriptor* (descrittore di servizio)<sup>26,27</sup>. Questo descrittore contiene la chiave pubblica del servizio nascosto e un elenco di nodi TOR che fungeranno da punti di introduzione, intermediari e fidati. Successivamente, l’*host* TOR di partenza creerà connessioni ai punti di introduzione elencati. Qualsiasi *client* TOR che voglia connettersi al servizio nascosto può ora farlo attraverso questi punti di introduzione. Il *client* (TOR) interessato a connettersi sceglie casualmente un punto di *rendez-vous* nella rete TOR; grazie a questo potrà collegarsi in modo anonimo al punto di introduzione scelto trasmettendo un messaggio al servizio nascosto. Questo messaggio contiene l’identità del punto di *rendez-vous* crittografato, usando la chiave pubblica del servizio nascosto e il materiale necessario (pacchetti per regolare i parametri di connessione) per iniziare un “handshake” crittografico<sup>28</sup>. Il servizio nascosto crea anche una connessione al punto di “rendez-vous” scelto e invia un messaggio che completa l’*handshake* crittografico.

A questo punto, il *client* e il servizio nascosto hanno impostato un percorso di rete privato resistente alla sorveglianza e possono scambiare dati in modo anonimo e confidenziale.

La creazione di numerose pagine online anonime ha dato modo che si facessero adeguate divisioni tra spazi di rete differenti, distinguendo tra i contenuti indicizzati dai motori di ricerca e quelli che non lo sono.

---

<sup>24</sup> Ad esempio, il server “google.it”.

<sup>25</sup> Ruffo Giancarlo, da *Rete e Reti*, 2.4 il “cuore” pulsante della rete: il DNS (p.32), - Durante Massimo – Ugo, Pagallo, Manuale di Informatica Giuridica e diritto delle nuove tecnologie 2017.

<sup>26</sup> Questo service descriptor è interfaccia che definisce come il servizio viene implementato, riportandone anche i metadati che descrivono a loro volta come l’interfaccia viene mappata su un livello di trasporto (transport protocol, come TCP) sottostante.

<sup>27</sup> Piscitello Dave, *The Dark Web: The Land of Hidden Services*, VP of Security and Information and Communications Technologies (ICT) Coordinator, ICANN, 2017. Si veda il link: [www.icann.org](http://www.icann.org)

<sup>28</sup> Avvio di una sessione di connessione attraverso tecniche crittografiche.

### 1.2.2 La suddivisione del Web

In materia si cerca di concepire la rete come un oceano di dati nel quale si possono fare una serie di distinzioni tra tutto ciò che c'è in superficie e quello che c'è sotto, ovvero il web “sommerso”, meglio conosciuto come *deep web*, che nelle sue profondità ospita il mondo delle reti oscure; le Darknet.

Il web in superficie, *Surface web* o *clearnet* è la parte del Web che è stata scansionata e indicizzata<sup>29</sup> da motori di ricerca standard come Google, Bing, Yahoo o tramite altri normali browser web<sup>30</sup>. Nonostante la quantità di informazioni riportate sembri sconfinata, al contrario questa rappresenta solo il 4%<sup>31</sup> dei contenuti che girano sul web. Il restante 96% circola nel *deep web*, la rete sommersa, termine che può essere riferito a qualsiasi contenuto Internet che, per vari motivi, non può essere o non è indicizzato da motori di ricerca tradizionali<sup>32</sup>. Questa definizione include quindi pagine web dinamiche<sup>33</sup>, siti bloccati (compresi quelli che chiedono per accedere di rispondere ad CAPTCHA<sup>34</sup>), siti non collegati, siti privati (come quelli che richiedono credenziali di accesso), siti con contenuti in script<sup>35</sup>/ non in HTML/ e altre reti ad accesso limitato<sup>36</sup>. Tali reti coprono tutte quelle risorse e servizi che non sarebbero normalmente accessibili, includendo tutti quei siti, con nomi di dominio registrati sul DNS (Domain Name System), ma non gestiti dalla *Internet Corporation for Assigned Names and Numbers (ICANN)*<sup>37</sup>. Conseguentemente si deve avere un URL preciso per accedere alla pagina nella quale si vuole entrare. Altri esempi sono siti che hanno registrato il loro nome di dominio su un sistema completamente diverso dal DNS standard, come i domini .BIT. Questi sistemi non solo sfuggono ai regolamenti sui nomi di dominio imposti dall'ICANN ma la loro natura decentralizzata, in quanto alternativi al DNS, rende anche molto difficile appropriarsi di questi domini, se necessario.<sup>38</sup>

---

<sup>29</sup> ovvero ricercabile.

<sup>30</sup> Daniel Sui, James Caverlee, Dakota Rudesill, *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*, 2015.

<sup>31</sup> Joseph Hirschhorn Howard, Wrote "Searching The Deep Web and The Unmapped Internet" 2015, si veda il link: <https://www.quora.com/How-big-is-the-deep-web>

<sup>32</sup> Trend Micro, *Exploring the Deep Web*, 2015.

<sup>33</sup> Una pagina web dinamica è una pagina web il cui contenuto, in tutto o in parte, è generato sul momento dal server, potendo dunque essere diversa ogni volta che viene richiamata consentendo un'interattività con l'utente, secondo il paradigma di programmazione web noto come web dinamico.

<sup>34</sup> Completely Automated Public Turing-test-to-tell Computers and Humans Apart, un test di questo genere è tipicamente utilizzato quando richiede all'utente di scrivere quali siano le lettere o i numeri presenti in una sequenza, che appare distorta o offuscata sullo schermo, ai fini di accedere ad una determinata pagina.

<sup>35</sup> pagine accessibili solo tramite link prodotti da JavaScript e contenuti scaricati in modo dinamico dai server Web tramite Flash o Soluzioni AJAX.

<sup>36</sup> Ibid. Trend Micro

<sup>37</sup> Ibid.

<sup>38</sup> Ibid.

Per “immergersi” nelle profondità della rete si possono utilizzare, a seconda degli obiettivi, due principali metodi<sup>39</sup>: utilizzare i motori di ricerca speciali (come The WWW Virtual Library, SurfWax, IceRocket ecc..) <sup>40</sup> a cui si accede da browser regolari (come Internet Explorer, Firefox, Chrome, Safari, ecc.) conoscendo l’URL specifico, o in alternativa sempre da motori di ricerca speciali (come Ahima o TorDi) a cui si ha accesso da TOR (comprendendo anche I2P e Freenet). Tuttavia, in alcuni casi utenti che navigano sui normali motori di ricerca, potrebbero interagire con una parte del *deep web*, senza esserne a conoscenza<sup>41</sup>. Ad esempio, l’elenco della Biblioteca del Congresso degli Stati Uniti ([www.loc.gov](http://www.loc.gov)) è un database online che risiede nel *deep web*<sup>42</sup>. Tra questo tipo di siti ritroviamo database disponibili al pubblico (come alcuni siti di librerie virtuali, [findlaw.com](http://findlaw.com), [copyright.gov](http://copyright.gov)) database a pagamento (come Westlaw e LexisNexis) archivi di servizi di chat e servizi di sola sottoscrizione (presenti nella maggior parte delle biblioteche accademiche)<sup>43</sup>. Nonostante molte delle credenze su le parti nascoste della rete, il *deep web* non è il luogo della rete dove vige l’illegalità, ma un vastissimo spazio di dati e contenuti nel quale solo in una parte più “oscura” e “profonda” si cela un ulteriore spazio adatto alle attività criminali. Le Darknet, o reti oscure, inaccessibili attraverso metodi di navigazione standard<sup>44</sup>, sono reti criptate in cui gli utenti possono scambiare in modo anonimo beni e servizi, sia legali che non<sup>45</sup>. Questo *hidden space*, o spazio nascosto, è popolarmente noto come piattaforma per attività di *hosting* illecite come il commercio di droga, la presenza di pornografia infantile, di informazioni rubate e diversi tipi di *malware*, fino a servizi di riciclaggio di denaro<sup>46</sup>. Questi domini nascosti ospitano siti visualizzabili anche dalle *clearnet*, attraverso Ahima, motore di ricerca che indicizza, cerca e cataloga i contenuti pubblicati sui servizi nascosti di TOR<sup>47</sup>. Per accedere a tali servizi, e conseguentemente all’intero del web oscuro, è necessario installare TOR browser sul proprio dispositivo, che attraverso la *onion routing*<sup>48</sup>, crittografa l’identità degli utenti in entrata e in uscita. Tale meccanismo che fornisce l’anonimato, allo stesso modo consente ai contenuti dei servizi di essere ospitati in modo anonimo sulla rete, apparentemente non rintracciabili pur rimanendo accessibile dall’interno della Internet. Quando si utilizza TOR, gli URL dei siti web cambiano

---

<sup>39</sup> Ibid. Daniel Sui, James Caverlee, Dakota Rudesill, 2015.

<sup>40</sup> Vinciarelli Alessandro, *Motori di ricerca per il Deep Web*, 2016 disponibile al link: <https://www.html.it/pag/58845/motori-di-ricerca-per-il-deep-web/>

<sup>41</sup> Ibid, Daniel Sui

<sup>42</sup> Ibid.

<sup>43</sup> Ibid.

<sup>44</sup> Abdulmajeed Alhighbani, *Going Dark: Scratching the Surface of Government Surveillance*, 23 *CommLaw Spectus* 2015.

<sup>45</sup> UNODC, *The Drug Problem and Organized Crime, Illicit financial Flows, Corruption and Terrorism, documento che costituisce*, World Drug Report 2017.

<sup>46</sup> Ibid. Abdulmajeed Alhighbani.

<sup>47</sup> TorProject blog, Ahmia Search After GSoC Development, 09, 2014. Per Ahmia si veda: <https://ahmia.fi/>

<sup>48</sup> In riferimento a Capitolo I

formato. Invece di siti web che terminano in .it .com, .org, .net, ecc., i domini terminano con il suffisso “a cipolla” *.onion*, che identifica un “servizio nascosto”<sup>49</sup>. Nonostante questo spazio di rete sia utilizzato da attivisti contro la censura, da giornalisti che devono comunicare informazioni sensibili o semplicemente da *host* intenti a mantenere al sicuro la propria privacy, la fetta più significativa che naviga in questo spazio è composta da organizzazioni criminali<sup>50</sup>.

### 1.3 Le Cripto-valute

Sin dal 1983, si sono susseguiti numerosi tentativi per cercare di bypassare gli istituti finanziari intermediari e le commissioni sulle singole transizioni apportati dalle banche con la creazione di monete virtuali legate a mezzi di crittografia quali *l'e-cash* (un tipo di sistema che consente ad un consumatore di effettuare pagamenti per determinati beni o servizi tramite la trasmissione di una moneta, contante in forma digitale, non legata a una persona specifica, pertanto firmata “ciecamente”<sup>51</sup> da una banca, rendendo così la transazione non rintracciabile) o i *b-money* (un sistema che permetteva a mittenti e ricevitori di nascondere la propria identità attraverso l’uso delle chiavi pubbliche<sup>52</sup>, sulle quali un utente doveva aggiungere l’importo desiderato per il trasferimento di denaro). Nonostante una crescita iniziale, la fiducia nei confronti di questi nuovi esperimenti da parte degli utenti diminuiva (nonché la circolazione e il mantenimento della valuta), specialmente con l’arrivo, alla fine degli anni ’90, dei nuovi mezzi di pagamento digitale. Con la possibilità di trasferire capitali da una parte all’altra del mondo, grazie ai bonifici on-line e alla diffusione dell’*home banking*, la sfera del commercio internazionale ebbe un mutamento decisivo. Banche, società di carte di credito e altri intermediari digitali divennero ancora più protagonisti nello scenario finanziario. Seguendo l’intento iniziale della generazione cyberpunk di liberarsi dai vincoli imposti dai grandi istituti finanziari, nel 2009 viene presentato pubblicamente in rete il *white paper*: “Bitcoin: A Peer-to-Peer Electronic Cash System” firmato dallo pseudonimo Satoshi Nakamoto. “La loro definizione più corretta è quella di cripto-asset e lo schema negoziale di riferimento è quello della permuta tra un bene reale ed un bene virtuale”<sup>53</sup>.

---

<sup>49</sup> InfoSec Institute, Diving in the Deep Web, March 14, 2013, <http://resources.infosecinstitute.com/diving-in-the-deepweb/>.

<sup>50</sup> In riferimento a McGuire, riportato nel Capitolo II.

<sup>51</sup> Crittograficamente.

<sup>52</sup> Un messaggio che viene crittografato utilizzando una chiave pubblica può essere decifrato solo utilizzando una chiave privata (riferimento alla nota 7).

<sup>53</sup> Laudati, Antonio, Procura Nazionale Antimafia ed Antiterrorismo – *Prefazione Bitcoin e criptovaulte* (a cura di) Razzante Ranieri 2018.

Il bitcoin è una valuta digitale decentralizzata, priva dal controllo bancario, che si basa sulla crittografia<sup>54</sup> e su una rete broadcast<sup>55</sup> peer-to-peer<sup>56</sup>. La nuova cripto-valuta infatti non viene emessa da una banca centrale e la quantità di unità in circolazione non è controllata da alcuna autorità o governo, ma da un algoritmo software generato attraverso le operazioni di “mining”. Tale processo, parlando in senso metaforico, consiste nell’estrarre moneta da un giacimento virtuale attraverso determinate tecniche<sup>57</sup>. Queste operazioni corrispondono ad una serie di processi di verifica delle transazioni messi in atto dai *miners* ovvero persone che attraverso potenti sistemi computerizzati, risolvono complesse operazioni matematiche, creando una serie di bit (numeri), che di fatto generano elettronicamente i “coin” virtuali. In pratica, qualsiasi computer può scaricare un software e collegarsi alla rete bitcoin; attivando l’opzione ‘genera bitcoin’ sarà in tal modo possibile partecipare al processo di creazione<sup>58</sup>. Tali processi di generazione e verifica avvengono per mezzo della *blockchain*, che letteralmente può essere definita come una catena di blocchi virtuale, ovvero un database immutabile, gestito da una rete di nodi, che memorizza tutte le transazioni bitcoin in ordine cronologico. Ad ogni conferma di transazione avvenuta, questa viene correttamente registrata all’interno di questo database. Di fatto, una volta effettuata una transazione, i dati vengono salvati in uno dei blocchi della catena, e non possono essere in alcun modo modificati e manomessi nel tempo; restando immutabili<sup>59</sup>. Ne consegue che la “catena dei blocchi” contiene lo storico di tutti i movimenti di tutti i bitcoin generati a partire dagli “indirizzi”, ovvero dalle chiavi pubbliche, del loro creatore fino all’attuale proprietario. I *token* inviati nella rete vengono registrati come appartenenti a questi “indirizzi” criptati. A questo punto le transazioni sono raggruppate nei blocchi della *blockchain*, percepite da ogni nodo della rete che dovrà approvare o meno l’entrata di un nuovo blocco nella catena per permetterne la registrazione.

L’innovazione che garantisce oltre modo la sicurezza del sistema è l’applicabilità di una rete distribuita che migliora ulteriormente l’immutabilità e garantisce l’affidabilità della *blockchain*. Poiché tutti i nodi possono memorizzare la stessa copia di *blockchain*, è estremamente difficile per

---

<sup>54</sup> ovvero sul sistema delle chiavi pubbliche e private per essere spesa

<sup>55</sup> Il broadcasting è la radiodiffusione ovvero la distribuzione di contenuti, compresi audio e video, a un pubblico disperso tramite qualsiasi mezzo elettronico di comunicazione di massa, ma in genere uno che utilizza lo spettro elettromagnetico (onde radio), in un modello uno-a-molti.

<sup>56</sup> I p2p sono nati tra la fine degli anni ’90, inizio anni 2000, grazie al programma di file sharing, inventato da Shwan Fanning, Napster. I sistemi p2p appaiono come piattaforme altamente decentralizzate o distribuite per raccogliere, distribuire o reperire informazioni in rete: sono diventati popolari come network di condivisione. Si tratta di sistemi con strutture gerarchiche nelle quali esistono alcuni nodi, detti super peer, che possono rivestire ruoli particolari come quello d’instradare le ricerche tra i nodi della rete. In questo modo tali sistemi garantiscono un alto livello di confidenzialità nelle comunicazioni.

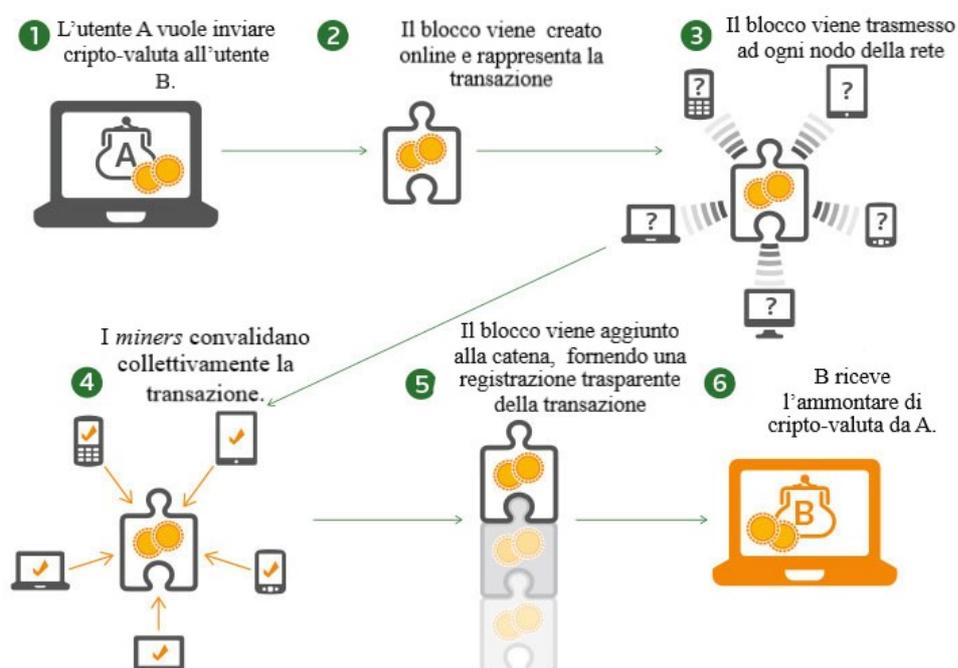
<sup>57</sup> Narayanan Arvind, Joseph Bonneau, Edward Felten, Andrew Miller Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies*, 19 lug 2016.

<sup>58</sup> Razzante Ranieri, cit. da *Bitcoin e monete digitali Problematiche giuridiche*, Rivista Italiana d’Intelligence, GNOIS, 2014.

<sup>59</sup> Leone, Federico e Parisella, Simone - *La blockchain, il protocollo cryptonote e le criptovalute* (par. 1.2.1, p.11), Bitcoin e criptovalute (a cura di) Razzante Ranieri 2018.

un malintenzionato modificare le memorizzazioni presenti in tutti i nodi. Per permettere tali procedimenti è essenziale la funzione del *mining*, il processo di “estrazione” o generazione delle cripto-valute accennato in precedenza, che avviene attraverso il meccanismo di consenso per determinare quali transazioni possono essere incluse nella *blockchain*. Un blocco viene creato in un asso temporale di 10 minuti, e affinché una nuova pagina possa essere aggiunta è necessario che la maggior parte dei nodi della rete bitcoin sia d’accordo sulle pagine precedenti, andando così di volta in volta a fortificare il sistema<sup>60</sup>. I *miners* mettono a disposizione la potenza di calcolo dei loro software specializzati per eseguire complessi calcoli matematici al fine di arrivare al compimento delle operazioni di approvazioni delle transazioni. In cambio ricevono un determinato quantitativo di bitcoin. Questo sistema insito nelle *blockchain* fornisce un modo per emettere valuta, incentivando più persone ad entrare nel mondo del *mining*, al fine della tutela dell’intero sistema. Proprio l’invenzione di questo archivio di dati relativo ai trasferimenti ha permesso l’eccezionale diffusione del bitcoin, la moneta virtuale che permette di bilanciare tra trasparenza della transazione e anonimato dell’utente.

Nell’immagine sottostante possiamo osservare, in cinque passaggi, come funziona il sistema di verifica per mezzo della *blockchain*:



Il valore di un bitcoin è determinato dai mercati online automatizzati che si basano sugli acquirenti e sui loro prezzi di offerta, confrontandoli con i venditori e i prezzi richiesti<sup>61</sup>. Il valore di mercato

<sup>60</sup> Ibid. Narayanan 2016.

<sup>61</sup> Ibid. Narayanan 2016.

quindi dipende dalla semplice legge della domanda e dell'offerta, come altri beni in commercio; più il bitcoin è richiesto e più il suo valore aumenta. Da un punto di vista economico la valuta rappresenta un nuovo mezzo di scambio, scevro dalla gestione monopolista di istituzioni bancarie, e se si volesse fare un paragone, può essere assimilata all'oro. La cripto-valuta infatti, chiamata anche "oro digitale", rappresenta un mezzo di scambio come un bene o una merce di valore, in quanto, l'aspettativa/fiducia sulla possibilità di utilizzarla in altri scambi è legata alle sue caratteristiche intrinseche, ed essendo per definizione le cripto-valute virtuali, non possono rappresentare un credito. Tuttavia, oltre che come mezzo di scambio, i bitcoin possono essere considerati economicamente riserva di valore, sia per scopi speculativi (come nuovo asset class) che precauzionali (ovvero per proteggerne il potere d'acquisto). È importante ricordare inoltre che i bitcoin, proprio come l'oro, non sono infiniti ed è previsto un ammontare massimo di 21 milioni che nell'arco degli anni va sempre diminuendo<sup>62</sup>.

L'idea iniziale alla base del progetto è quella di andare ad eliminare la possibilità della "double spending"<sup>63</sup>, basandosi su un sistema di registro delle transazioni totalmente affidabile. Per farlo, il suo creatore, ha saputo conciliare diverse caratteristiche. In primo luogo, l'apposizione della firma digitale per eseguire una transazione attraverso le *private key*, garantendo al solo proprietario del bitcoin di poter spendere il fondo<sup>64</sup>.

I bitcoin una volta generati, vengono memorizzati e protetti da un portafoglio (*il wallet*) assegnato ad ogni proprietario. Un portafoglio di cripto-valute memorizza le chiavi pubbliche e private che possono essere utilizzate per ricevere o spendere moneta<sup>65</sup>. Questi possono essere di tipo software, come applicazioni scaricabili direttamente sul proprio computer, tablet, smartphone o con l'uso di *wallet cloud*<sup>66</sup>. Inoltre, possono essere di tipo hardware collegando dispositivi esterni, come USB, facilmente supportabili da diverse interfacce del Web, facili da utilizzare, mantenendo la moneta offline e garantendone una maggiore sicurezza<sup>67</sup>. Infine, esistono i portafogli di tipo cartaceo, considerati i più sicuri di tutti, in quanto i codici di accesso (la chiave privata) vengono riportati su una tessera o su un foglio, ed averne cura è solo ed esclusivamente una responsabilità del proprietario. Il fatto che i codici non siano caricati in un sistema computerizzato può prevenire la

---

<sup>62</sup> Avanzando di questo passo nel 2030 si arriverà ad aver "estratto" 20 milioni.

<sup>63</sup> Come enunciato dal suo creatore nel white paper.

<sup>64</sup> Ibid. Narayanan 2016.

<sup>65</sup> Liu, Yi; Li, Ruilin; Liu, Xingtong; Wang, Jian; Zhang, Lei; Tang, Chaojing; Kang, Hongyan *An efficient method to enhance Bitcoin wallet security*. 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), 29 ottobre 2017.

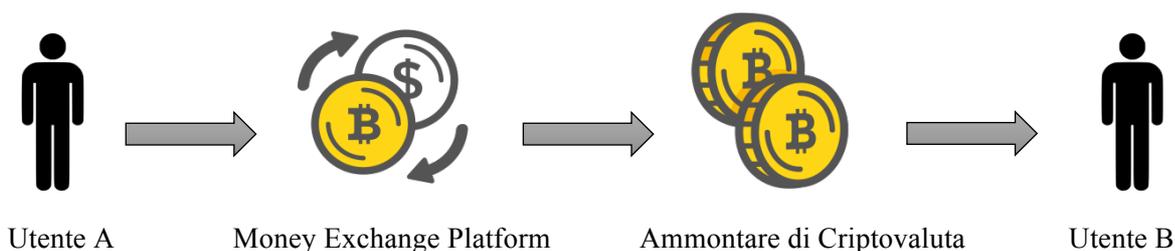
<sup>66</sup> i *wallet* possono essere conservati direttamente on line anche attraverso la *cloud*.

<sup>67</sup> I portafogli on line o attraverso applicazione offrono uno dei più alti livelli di sicurezza, tuttavia se il tuo computer/dispositivo viene hackerato o viene colpito da un virus, c'è la possibilità che il proprietario possa perdere tutti i tuoi fondi. I portafogli online possono esporre gli utenti a possibili vulnerabilità nella piattaforma che possono essere sfruttate dagli hacker per rubare le monete.

perdita o il furto telematico, specialmente alla luce della quotazione che hanno raggiunto le cripto-valute negli ultimi anni.

A questo punto se un qualsiasi acquirente volesse scambiare/comprare bitcoin può farlo attraverso i siti web di *exchange* (ovvero di scambio e compravendita di cripto-valute) acquistando o vendendo cripto valute, al prezzo di mercato, in cambio di valute legali come euro o dollari<sup>68</sup>. Nel concreto tali piattaforme di scambio si comportano come intermediari tra coloro che vogliono comprare e coloro che vogliono vendere le proprie cripto-valute, chiedendo in cambio delle commissioni. Il mittente per scambiare cripto-valuta deve possedere la propria chiave privata, conservata nel *wallet*, e la chiave pubblica del destinatario che potrà visualizzarne il contenuto solo se a conoscenza della propria chiave privata.

Attraverso il percorso mostrato nell'immagine sottostante, l'utente A per trasferire denaro all'utente B, deve scambiare online, su una piattaforma di money exchange (come Coinbase, Kraken, Poloniex ecc..) il denaro reale (dollari, euro yen ecc..) in denaro virtuale. Una volta aver ottenuto l'ammontare desiderato in cripto-valuta può trasferire il denaro sull'indirizzo (a chiave pubblica) dell'utente B.



La cripto-valuta offre in questo modo l'anonimato dell'utente, in quanto non si ha modo di incontrare il ricevitore faccia a faccia, pertanto l'unica caratteristica identificativa di entrambe le parti sono le loro chiavi pubbliche<sup>69</sup>. Tuttavia, la letteratura a riguardo<sup>70</sup> fa notare che le cripto-valute sono solo pseudo-anonime, ovvero che ogni transazione fatta usando la cripto-valuta è di dominio pubblico, riscontrabile per chiunque sul grande registro delle transazioni in cripto-valuta (la *blockchain*). Seguendo il percorso della catena diventa abbastanza facile capire quale *wallet* abbia inviato denaro ad un *wallet* ricevente, in questa maniera si può sapere quali siano le attività e gli spostamenti del portafoglio. Nonostante questo, le principali problematiche risiedono nel capire chi si cela dietro al *wallet*, il quale nella maggior parte dei casi è anonimo; identità protetta dai

<sup>68</sup> Ibid.

<sup>69</sup> Si veda Capitolo I.

<sup>70</sup> Reynold Perri & Irwin Angela S.M., *Anonymity within the Bitcoin system*. Tracking digital footprints: anonymity within the bitcoin system” 2017, Research Paper, pubblicato da: Emerald Publishing Limited.

*provider* e dalle diverse modalità precedentemente elencate attraverso i quali l'utente può tenere al sicuro la sua chiave privata.

### *1.3.1 L'evoluzione della cripto-valuta*

Dopo la divulgazione del documento<sup>71</sup> nasce la piattaforma per le transazioni bitcoin grazie al rilascio del primo Client - Bitcoin open source e della concomitante emissione di Bitcoin. Nel luglio del 2010 il sito lancia il servizio di scambio di cripto-valute, quotandone i prezzi. La circolazione inizialmente si è svolta tra volontari e appassionati del mondo dell'informatica per poi cominciare a crescere fino ad arrivare ad altri siti, come la piattaforma giapponese Mt. Gox<sup>72</sup>. Nello stesso anno il bitcoin viene immediatamente sfruttato da uno dei primi mercati illeciti della rete, il famoso Silk Road sito all'interno delle Darknet. Il portale permetteva transazioni per gli acquisiti di prodotti illegali (principalmente narcotici) attraverso l'uso della cripto-valuta e più volte è stato segnalato per rappresentare la metà del primo volume di transazioni bitcoin<sup>73</sup>. L'associazione Silk Road in un primo momento ha influenzato la reputazione dei bitcoin inquadrandoli come strumento dell'illegalità agli occhi dell'opinione pubblica. In senso contrario la piattaforma Mt. Gox cresceva tanto da rappresentare il più grande sito di scambio di cripto-valute esistente, consegnando oltre il 70% di tutte le transazioni bitcoin al mondo<sup>74</sup>, fino alla sua bancarotta nel 2014. Le preoccupazioni relative al fatto che fosse una valuta decentralizzata e sfuggente al controllo delle autorità hanno portato molti governi (da quello Cinese a quello Pakistano) a delegittimare il bitcoin come mezzo di scambio online, rendendolo illegale. Nonostante ciò la notorietà della moneta virtuale continuava a crescere, richiamando sempre più l'attenzione dei mercati finanziari internazionali. Nel contesto internazionale, la Russia dopo lunghe contrattazioni ha legalizzato l'uso dei bitcoin<sup>75</sup> mentre in Giappone le cripto-valute sono diventate mezzo di pagamento legale, in conformità con le leggi antiriciclaggio, e vengono definite valore di proprietà<sup>76</sup>. La Norvegia ha integrato i conti bancari in bitcoin, mentre in Svizzera il comune di Zugo ha aggiunto il bitcoin come mezzo per pagare le tasse cittadine<sup>77</sup> ed il sistema ferroviario federale, di proprietà governativa, vende bitcoin presso le sue

---

<sup>71</sup> "Bitcoin: A Peer-to-Peer Electronic Cash System", nel 2009.

<sup>72</sup> Che era stato originariamente creato come una piattaforma per lo scambio di carte collezionabili del gioco fantasy Magic.

<sup>73</sup> Yermack, David, Is Bitcoin a Real Currency? An economic appraisal, Dicembre 2014.

<sup>74</sup> Frunza, Marius-Cristian, Solving Modern Crime in Financial Markets: Analytics and Case Studies. Academic Press., 9-12-2015.

<sup>75</sup> Si veda il link: [www.cryptocurry.com/news/russia-officially-legalizes-bitcoin/](http://www.cryptocurry.com/news/russia-officially-legalizes-bitcoin/)

<sup>76</sup> Regulation of Cryptocurrency. Library of Congress. June 2018., si veda il link: [www.loc.gov/law/help/cryptocurrency/japan.php](http://www.loc.gov/law/help/cryptocurrency/japan.php)

<sup>77</sup> 7 Si veda: [www.dw.com/en/alpine-crypto-valley-pays-with-bitcoins/a-19371082](http://www.dw.com/en/alpine-crypto-valley-pays-with-bitcoins/a-19371082)

biglietterie automatiche. Nel dicembre '17, 1 bitcoin è pari a quasi 19000 dollari americani<sup>78</sup>. Questa enorme crescita quotata sui mercati regolamentati ha fatto sì che sempre più investitori si interessassero al trading digitale<sup>79</sup> e conseguentemente alla creazione di fondi di investimento per il trading della valuta digitale (specialmente negli USA). Nonostante questo, dopo il 2017 c'è stato un progressivo calo del bitcoin a causa della concorrenza sul mercato delle altre monete virtuali. Sebbene il bitcoin rimanga la moneta di riferimento nel mondo delle cripto-valute si deve considerare la presenza di altre blockchain sul mercato soggette a altri investimenti.

### 1.3.2 Altcoin: le altre cripto-valute

Il termine Altcoin, abbreviazione di “alternative-coin”, si riferisce in maniera generica a qualsiasi tipo di cripto-valuta che non sia il Bitcoin<sup>80</sup>. Nonostante quest'ultimo costituisce la moneta virtuale più popolare, nella sua tecnologia presenta alcune limitazioni che hanno portato alla creazione di altre blockchain con caratteristiche uniche generatrici di diversi tipi di cripto-valuta. La BCE già dal febbraio 2015 nel suo report “Virtual currency schemes –a further analysis”<sup>81</sup> ha registrato la presenza di oltre 500 valute digitali<sup>82</sup> diverse dai bitcoin. Le più note in circolazione sono **Etherum**, che aumenta la velocità della transazione (tra i 10 e i 15 secondi), **Ripple**, rete di pagamento digitale per le transazioni finanziarie, pensata per pagamenti *crossborder*, **Litecoin** e **IOTA** (famosa per la sua tecnologia intrinseca più che per il suo valore di mercato) ognuna con un proprio sistema di funzionamento indipendente.

#### 1.3.2.1 Le cripto-valute anonime

Ai fini del presente contributo è importante menzionare l'arrivo sul mercato di altre due cripto-valute, che offrono alti livelli di riservatezza: Z-Cash e Monero.

**Monero:** Il progetto viene lanciato nel 2014, dal suo principale sviluppatore Riccardo Spagni, e diviene sempre più popolare grazie alle garanzie di anonimato proposte rispetto ai bitcoin. Come visto in precedenza, sappiamo che una transazione di cripto-valuta ha tre aspetti: l'indirizzo del mittente (chiave pubblica del mittente), l'indirizzo del destinatario (chiave pubblica del destinatario)

---

<sup>78</sup> Si veda il link: <https://www.cnn.com/2017/12/06/bitcoin-tops-13000-surgings-1000-in-less-than-24-hours.html>

<sup>79</sup> Per trading si intende l'investimento e lo scambio di cripto-valuta, acquistare e vendere valuta virtuale attraverso determinati portali a disposizione come Coinbase, Poloniex, ecc.

<sup>80</sup> Si veda il link: <https://medium.com/@monetha/what-is-an-altcoin-heres-a-definitive-guide-442ef5a585c8>

<sup>81</sup> European Central Bank, Virtual currency schemes –a further analysis, 2015, si veda il link: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

<sup>82</sup> Ibid.

e l'importo inviato. Nel mondo dei bitcoin, tutti e tre questi aspetti sono pubblici e tracciabili attraverso riferimenti incrociati. Inoltre, grazie alla *blockchain*, tutte le monete trasferite dal mittente al destinatario vengono registrate e rese pubbliche. Le transazioni con Monero basate sul protocollo CryptoNote<sup>83</sup>, sono difficilmente tracciabili ( in quanto non appare né mittente, né destinatario, né cronologia delle transizioni) grazie alle *ring signatures* e al Ring CT, implementato più avanti. Per mascherare gli indirizzi vengono usate firme ad anello o *ring signature*, dove ogni transizione tra due parti viene inserita e raggruppata ad altre transazioni multiple che si verificano tra diverse parti non correlate. Ciò significa che il trasferimento di moneta da un utente A ad un utente B viene mescolato con le altre transazioni degli utenti Monero e spostato casualmente lungo l'elenco delle transazioni, il che rende esponenzialmente difficile risalire alla fonte o al destinatario. Agli inizi del 2017 è stato implementato il Ring CT: Ring Confidential Transactions (Ring CT), finalizzato a fornire un miglior anonimato per gli importi delle transazioni. Il sistema gestisce le transazioni dividendo l'importo trasferito in più importi, suddividendoli come fossero transazioni separate. Ad esempio, un utente che trasferisce 100 XMR (unità monetaria di Monero) a un acquirente dovrebbe suddividere l'importo in 22 XMR, 61 XMR e 17 XMR, per un totale di 100 XMR. Ognuno di queste viene trattata separatamente e viene creato un indirizzo univoco per ciascuna delle figure suddivise. Con la firma ad anello, ciascuno di questi importi suddivisi viene combinato con altre transazioni che, ovviamente, sono state divise, rendendo estremamente difficile identificare il mix esatto di 100 XMR che appartiene al destinatario.<sup>84</sup>

L'offerta di Monero attuale è in continua crescita, dato dovuto, specialmente negli ultimi due anni, all'uso che se ne fa sia per scopi legati al riciclaggio online che a quelli all'interno dei mercati illegali siti nelle Darknet. I criminali intenti ad operare nelle reti oscure cercano tecniche sempre più all'avanguardia per raggiungere il completo anonimato. Monero offre un sistema efficace che, attraverso la mescolanza di indirizzi e la suddivisione dell'importo rende molto difficile tracciare una transizione<sup>85</sup>.

**Z-cash:** utilizza uno strumento crittografico denominato *Zero-Knowledge-Proof* che consente a due utenti di effettuare transazioni senza che nessuna delle parti riveli il proprio indirizzo all'altro. Questa tecnica rende le transazioni Z-Cash non rintracciabili sulla blockchain offuscando gli indirizzi di entrambe le parti, così come l'ammontare coinvolto in ogni transazione, impedendo la ricostruzione dei passaggi dell'asset. Inoltre, Z-Cash è supportabile dalla maggior parte dei *wallet*, sia hardware che software, incentivandone l'uso. Essendo in circolazione dalla fine del 2016 ZEC

---

<sup>83</sup> CryptoNote è un protocollo che mira a risolvere i problemi delineati in Bitcoin Core, il protocollo dietro Bitcoin, alimentando diverse cripto-valute decentralizzate orientate ad una maggiore tutela della privacy nelle transazioni.

<sup>84</sup> Shen Noether, Adam Mackenzie, Monero Reserch Lab, *Ring Confidential Transaction*, 2016.

<sup>85</sup> Darknet Cryptocurrency: Zcash Vs. Monero, si veda il link: <https://darkwebnews.com/dark-web/darknet-cryptocurrency-zcash-vs-monero/>

(simbolo di valuta per Z-Cash), è utilizzata in seconda posizione rispetto a Monero, sulla rete da più anni e quindi ritenuta più affidabile, specialmente nelle Darknet. Nonostante questo, a partire dal luglio 2018, la moneta ha avuto un aumento progressivo che continua ancora oggi

## Capitolo II - Il Crimine Organizzato nel mondo della rete

### 2.1 Introduzione al crimine organizzato

Il termine "crimine organizzato", per come lo conosciamo oggi, sembra essere stato utilizzato per la prima volta a Chicago nel 1919<sup>86</sup>, in riferimento alle bande che gestivano il contrabbando in quell'epoca. Nonostante questa tarda collocazione terminologica, sappiamo che il fenomeno del crimine organizzato è un qualcosa che risale alle radici del percorso storico dell'essere umano. Secondo il criminologo Paul Lunde, "la pirateria e il banditismo erano, per il mondo preindustriale, ciò che il crimine organizzato è per la società moderna"<sup>87</sup>. L'Europa del diciannovesimo secolo vide il sorgere nelle diverse nazioni di vere e proprie società criminali organizzate in gruppi distinti, ranghi, a volte chiamate famiglie. Questi "gruppi" erano costituiti da membri provenienti da strati inferiori della società operanti nell'ambito di prostituzione, falso, contraffazione, furti, commerci illeciti e persino nell'ideazione di tecniche per il riciclaggio di denaro<sup>88</sup>. Nel 1761<sup>89</sup> in Cina nasce la prima società fraterna a stampo criminale, la Tiandihui (anche chiamata Hongmen, la vasta famiglia), mentre ancor prima in Giappone, durante la prima metà del quindicesimo secolo, viene riscontrata la nascita di gruppi organizzati di malviventi, *tekiya* e *bakuto*, gli affiliati originari dell'odierna Yakuza<sup>90</sup>. Sebbene la presenza costante di questo fenomeno nell'arco del tempo, solo di recente le nazioni hanno deciso di cooperare per dare una risposta collettiva. Come illustra Antonio Maria Costa, ex direttore esecutivo dell'UNODC<sup>91</sup>, dopo la fine della guerra fredda la governance globale non è riuscita a tenere passo alla globalizzazione economica. Pertanto, questa apertura senza precedenti al commercio, alla finanza, al modo di viaggiare, e alla comunicazione ha creato una crescita economica e un benessere diffuso che allo stesso tempo hanno contribuito a fornire un'enorme opportunità a società criminali in tutto il mondo di fare affari e prosperare come mai prima d'ora<sup>92</sup>.

La criminalità organizzata si è diversificata, è diventata globale e ha raggiunto proporzioni macroeconomiche: beni illeciti provengono da un continente, vengono trafficati in un altro, e

---

<sup>86</sup> UNODC, "the Studies and Threat Analysis Section, Policy Analysis and Research Branch, Division for Policy Analysis and Public Affairs, UNODC", *The Globalization of Crime - The threat of Transnational Organized Crime*, 2010.

<sup>87</sup> Lunde Paul, cit. in it. da: *Organized Crime: An Inside Guide to the World's Most Successful Industry*, 2004.

<sup>88</sup> Thomas, Donald. *The Victorian Roots of Organized Crime / Gangsters and career criminals flourished in 19th century London*, 3-01-1999, si veda il link: [www.sfgate.com/books/article/The-Victorian-Roots-of-Organized-Crime-2954000.php](http://www.sfgate.com/books/article/The-Victorian-Roots-of-Organized-Crime-2954000.php).

<sup>89</sup> Murray H. Dian, *The Origins of the Tiandihui, The Chinese Triads in Legend and History*, 1994,

<sup>90</sup> Arduini Giorgio, *Yakuza, un'altra mafia*. Luni editrice 2017

<sup>91</sup> L'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine

<sup>92</sup> Ibid. Lunde Paul, 2004.

commercializzati in un terzo. Le mafie sono oggi un problema transnazionale<sup>93</sup>; una minaccia alla sicurezza, specialmente nei paesi poveri e in conflitto. Il crimine sta alimentando la corruzione, infiltrandosi negli affari e nella politica, ostacolando lo sviluppo e la governance dando potere a coloro che operano al di fuori della legge. Nonostante la gravità della minaccia, il crimine organizzato non è sufficientemente compreso. C'è una mancanza di informazioni sulle tendenze dei mercati criminali transnazionali<sup>94</sup>. Senza una prospettiva globale non ci può essere una politica informata da prove obiettive, fedele a prassi scientifiche, rigorosamente stabilite. Nonostante le legislazioni interne abbiano definizioni a livello normativo di forme di crimine organizzato non esiste un significato condiviso del termine. In molti casi una poca comprensione a livello internazionale della terminologia può causare risposte legislative errate a livello nazionale, che limitano l'efficacia di misure di controllo e prevenzione del crimine.

Un primo tentativo di unificazione del concetto di crimine organizzato in senso transnazionale è stato fatto dalla “Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale”<sup>95</sup> e i protocolli associati ad essa. La Convenzione, redatta a Palermo nel 2000 ed entrata in vigore nel 2003, non contiene alcuna precisa definizione di “crimine organizzato transnazionale”, né contiene una lista dei tipi di crimini che potrebbero rientrare in questa rubrica. Tuttavia, in quanto il suo scopo è “combattere e prevenire la criminalità organizzata”, viene definito cosa sia un “gruppo criminale organizzato”, ovvero: “un gruppo strutturato, esistente per un periodo di tempo, composto da tre o più persone che agiscono di concerto al fine di commettere uno o più reati gravi<sup>96</sup> o reati stabiliti dalla presente Convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale”<sup>97</sup>.

Nonostante questo ritardo a livello internazionale, definizioni e precauzioni sono state adottate a livello nazionale<sup>98</sup>; come nel caso italiano che ha avuto modo di confrontarsi sin dall'unità nazionale con il fenomeno di criminalità organizzata più conosciuto al mondo: quello mafioso. Il modello mafioso è una tipologia di organizzazione criminale, riferita ad un variegato numero di

---

<sup>93</sup> In riferimento alla Convenzione di Palermo sul Crimine Organizzato Transnazionale indetta dalle Nazioni Unite nel 2000, nella quale si fa un chiaro riferimento ai “reati transnazionali” da parte di organizzazioni criminali che operano in più Stati.

<sup>94</sup> Costa Anotnio Maria, *preface by executive director p. iii*, “The Globalization of Crime - The threat of Transnational Organized Crime”, UNODC, 2010.

<sup>95</sup> Assemblea Generale delle Nazioni Unite *Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale*, sottoscritta nel corso della Conferenza di Palermo (12 - 15 dicembre 2000), si veda il link: [https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED\\_NATIONS\\_CONVENTION\\_AGAINST\\_TRANSNATIONAL\\_ORGANIZED\\_CRIME\\_AND\\_THE\\_PROTOCOLS\\_THEREO.pdf](https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THEREO.pdf)

<sup>96</sup> "Reato grave" indica la condotta che costituisce un reato sanzionabile con una pena privativa della libertà personale di almeno quattro anni nel massimo o con una pena più elevata.

<sup>97</sup> Assemblea Generale delle Nazioni Unite *Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale* sottoscritta nel corso della Conferenza di Palermo (12 - 15 dicembre 2000), *Articolo 2, a*).

<sup>98</sup> Si parlerà dell'approccio normativo sia europeo che italiano nel capitolo IV.

organizzazioni/società in tutto il mondo, che attraverso l'uso della violenza, esercita specifiche forme di pressione economica e politica al fine di ricavarne profitto. Come ci ricorda Giovanni Falcone, la mafia non va confusa con un'associazione a delinquere, ma rappresenta un'entità parallela ai pubblici poteri intenta a "sostituirli"<sup>99</sup>. Eppure, tale distinzione, esplicitata nell'articolo 416bis<sup>100</sup> del codice penale italiano, rimane ancora un *unicum* nel panorama legislativo europeo, nonostante le pressanti richieste di Europol ed Eurojust. Così organizzazioni criminali a stampo mafioso approfittano di legislazioni più morbide per trasferirvi i propri affari ed interessi.

Il pericolo messo in evidenza dagli investigatori, in tutta Europa, è il condizionamento che queste organizzazioni hanno sull'economia, sul mercato e sulla libera concorrenza<sup>101</sup>. Oltre ai tipici crimini molti dei reati commessi dalle organizzazioni criminali sono "senza vittime", nel senso che anche nel momento in cui ci fosse una chiara vittima, questa sarebbe riluttante a denunciare qualsiasi illecito per paura di rappresaglie<sup>102</sup>. "La strategia globale delle mafie italiane all'estero è tenere il basso profilo", osservava Europol nel rapporto riguardante il crimine organizzato italiano nel 2013<sup>103</sup>. Inoltre, per vendere qualsiasi materiale o servizio illecito, i mercati criminali devono essere sufficientemente aperti per attirare i clienti; mercati favoriti sempre di più dal processo di interconnessione delle nazioni nel mondo.

Si consideri l'arricchimento di un'organizzazione criminale e la sua conseguente influenza in un determinato paese, grazie al florido narcotraffico e alla compravendita di armi con più paesi. Queste attività influenzano la stabilità politica di una nazione aggravata dalla corruzione di politici, giudici, poliziotti e militari. L'organizzazione nell'arco del tempo si afferma in maniera sempre più incisiva, apre i propri mercati in altre nazioni, mentre controlla le attività in decine di carceri in tutto il paese e gestisce importanti vie e punti di vendita per il trasporto di cocaina<sup>104</sup>. L'intero scenario a sua volta porta ad una diminuzione del rating<sup>105</sup> da parte delle agenzie di credito e delle banche internazionali, con un conseguente crollo degli investimenti, infettando i prezzi nei mercati di capitali internazionali<sup>106</sup>.

---

<sup>99</sup> Falcone Giovanni, *Cose di Cosa Nostra*, ediz. Rizzoli 1991.

<sup>100</sup> Reato di associazione di tipo mafioso.

<sup>101</sup> Mafie unite d'Europa: tutti i "buchi" nella lotta al crimine in Ue Mappa interattiva: i clan Paese per Paese, [www.ilfattoquotidiano.it](http://www.ilfattoquotidiano.it)

<sup>102</sup> Nando dalla Chiesa, *Manifesto dell'Antimafia*, Einaudi 2014.

<sup>103</sup> SOCTA, *Eu Serious and Organized Crime Threat Assessment – Report 2013*.

<sup>104</sup> Nando dalla Chiesa, da *gli Scenari Internazionali della criminalità organizzata. Lineamenti teorici e di ricerca, Mafia Globale*, Laruna Editore, 2017.

<sup>105</sup> Al diminuire del rating aumenta il premio per il rischio richiesto e l'emittente deve quindi pagare uno spread maggiore – differenziale maggiore - rispetto al tasso che sarebbe richiesto in assenza di rischio, o risk-free rate.

<sup>106</sup> Ibid. Nando Dalla Chiesa 2017.

Il crimine organizzato è un'industria multimiliardaria<sup>107</sup> che è soggetta ad un incredibile livello di competizione, rischio mortale e massiccia pressione normativa; per questo richiede un alto livello di sofisticazione nelle pratiche di gestione, nella logistica, nella finanza e nell'istruzione.

L'espansione dei nuovi mezzi di comunicazione permessi dalle tecnologie di rete ha fatto sì di stabilire connessioni, alleanze e relazioni commerciali ottimizzando ed espandendo le operazioni delle organizzazioni criminali intorno al globo.

La rivoluzione digitale ha fatto sì che anche il crimine organizzato si evolvesse, adattandosi alle nuove tecnologie ed innovandosi. I gruppi criminali oggi sono decentrati e con l'aiuto delle tecnologie creano canali e relazionali in diversi paesi con più attori, più mezzi, sfruttando modalità di pagamento all'avanguardia. Le mafie in tutto il mondo sfruttano l'informazione e la comunicazione allo stesso modo delle imprese legittime e utilizzano il crimine informatico per finanziare le loro operazioni "tradizionali".

Il mondo del *cybercrime*, specialmente negli ultimi anni in crescita, ospita una molteplicità di attori di diverso genere: da cyberterroristi a singoli hacker, dalle vecchie organizzazioni criminali a nuovi gruppi specializzati che commettono illeciti sulla rete. Nei seguenti paragrafi si approfondirà il mondo del crimine organizzato in rete concentrandosi su le organizzazioni criminali a stampo tradizionale innovate dalle nuove tecnologie e quelle di nuovo stampo, operanti esclusivamente nello scenario della rete.

## 2.2 Criminalità informatica organizzata: vecchi e nuovi modelli.

I gruppi di criminalità organizzata operano nella rete con funzioni ed impatti sociali di diverso peso<sup>108</sup>. Un numero crescente di studi accademici e rapporti di aziende di cyber-sicurezza dimostrano le varietà di strutture organizzative che sono coinvolte in crimini informatici e hanno ampliato la nozione di crimine organizzato a fenomeni criminali legati al profitto che si verificano completamente o parzialmente nel cyberspazio<sup>109</sup>. Esistono infatti forme di criminalità che operano esclusivamente online, altre che operano in maniera mista ed altre ancora, principalmente offline<sup>110</sup>. Nel presente lavoro si indagheranno quei tipi di associazione criminale che svolgono attività oltre i confini nazionali e che sfruttano comunemente mezzi della rete, quali *onion routing* e cripto-valute, per portare a termine i propri scopi criminali. I gruppi in questione sono da un lato nuove forme di

---

<sup>107</sup> "Il fatturato della Ndrangheta spa è di 52,6 miliardi all'anno [...] Le stime sul giro d'affari - pari al 3,4% del Pil italiano" da Galullo Roberto *Ndrangheta spa, un'azienda da 53 miliardi di fatturato*, dal Sole24ore.

<sup>108</sup> McGuire, M., *Organised Crime in the Digital Age*. London: John Grieve Centre for Policing and Security, 2012.

<sup>109</sup> E. Rutger Leukfeldt & Anita Lavorgna & Edward R. Kleemans - *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, 2016.

<sup>110</sup> Ibid.

associazionismo operanti on-line, anche conosciute come *CyberGang*, e dall'altro le tradizionali forme di criminalità organizzata, presenti sul territorio, che operano sfruttando la rete per migliorare le proprie attività offline.

Prima di capire come queste due forme di criminalità hanno interagito tra loro e si sono evolute nel tempo è essenziale inquadrare l'ampio spettro della criminalità organizzata operante con il mezzo della rete.

### *2.2.1 Lo scenario del crimine organizzato in rete: il modello McGuire*

La complessa natura del crimine, come quella che si verifica nel cyberspazio, è aggravata dal crescente coinvolgimento di gruppi organizzati di nuovo e vecchio stampo che vanno evolvendo e mutando con il passare degli anni<sup>111</sup>. Tali gruppi, tuttavia, svolgono ruoli diversi all'interno della rete, con diversi obiettivi e sfaccettature.

Il criminologo britannico Michael McGuire del John Grieve Centre<sup>112</sup>, professore universitario e collaboratore di governo e di forze dell'ordine nel combattere i nuovi fenomeni di criminalità informatica, ha redatto uno degli studi più innovativi per quanto riguarda il coinvolgimento di gruppi di criminali organizzati sul web: "Organised Crime in the Digital Age"<sup>113</sup>. Nel documento egli espone le caratteristiche della criminalità organizzata operante in rete, smentendo molte delle convinzioni create nel mondo accademico in materia. Una di queste riguarda l'età degli utenti che agiscono illecitamente con l'aiuto delle reti computerizzate. Mentre ci si può aspettare che il crimine online sia riservato alle nuove generazioni, la ricerca rivela che quasi la metà (43%) dei membri, dei gruppi di criminalità digitale organizzata, ha più di 35 anni, mentre solo un terzo (29%) è sotto 25, di cui molti infatti hanno solo conoscenze informatiche di base. Grazie ai software standard<sup>114</sup> e all'adozione della tecnologia "inferiore" da parte dei criminali (come telefoni

---

<sup>111</sup> Europol, Internet Organised Crime Threat Assessment (IOCTA) 2018

<sup>112</sup> Il John Grieve Center (JGC) è un centro di studi (intento a creare una comunità di idee che abbraccia studenti, accademici, forze dell'ordine, professionisti e decisori politici) che contribuisce attivamente alle discipline accademiche emergenti dagli studi di polizia, promuovendo e diffondendo le competenze, la comprensione e le buone pratiche tra i professionisti. Il Centro gode di stretti collegamenti con varie organizzazioni di polizia e altre agenzie che non solo servono a migliorare la comprensione reciproca, ma anche a contribuire direttamente ai contenuti del corso per gli studenti.

<sup>113</sup> McGuire, M., *Organised Crime in the Digital Age*. London: John Grieve Centre for Policing and Security, 2012.

<sup>114</sup> Un software standard è un protocollo o un altro formato comune di un documento, file o trasferimento dati accettato e utilizzato da uno o più sviluppatori software mentre si lavora su uno o più programmi per computer. Ad esempio, per inviare un'e-mail da Outlook a Gmail, l'e-mail sarà inviata in protocollo HTML (ipertesti) che può analizzare correttamente il file per visualizzare l'e-mail. Senza una tecnica standardizzata per inviare un'e-mail, i due programmi diversi non sarebbero in grado di condividere e visualizzare accuratamente le informazioni fornite.

prepagati, smartphones e tablets), l'accessibilità e il fascino della criminalità digitale sono aumentati notevolmente<sup>115</sup>.

McGuire ha suggerito tre diversi tipi di gruppi criminali che agiscono in rete, ognuno diviso in due sottogruppi:

1. Il primo gruppo opera esclusivamente online e a sua volta può essere suddiviso in due sottogruppi: gli “sciami” e gli “hub”. Gli sciami, dall'inglese *swarm*, si presentano come grandi collettivi di rete, organizzazioni disordinate, senza leadership, in genere costituite da gruppi di individui attivi che sfruttano il web mossi da ideologie che conducono a crimini d'odio (come siti con contenuti neonazisti) e di resistenza politica (come Anonymous).

Gli “hub”, che letteralmente significa fulcro, elemento centrale, sono invece gruppi ben organizzati con una chiara e centrale struttura di comando. Coinvolgono un punto focale (hub) di criminali attorno al quale i membri periferici si riuniscono. I componenti in questo caso vanno da utenti esperti di informatica, a programmatori fino a veri e propri crakers<sup>116</sup> intenti in attività online di diverso genere, tra cui la pirateria, il phishing, le botnet<sup>117</sup> ed i reati sessuali in rete. McGuire riferisce che la distribuzione di scareware<sup>118</sup> o altri tipi di materiali illeciti sui *darkmarkets* coinvolge gruppi di questo tipo.

2. Il secondo gruppo è chiamato "ibrido" poiché esso combina attività online e offline. Anche in questo caso ci sono due tipi di sottogruppi all'interno dell'ibrido: uno è l'ibrido clusterizzato e l'altro l'ibrido esteso.

Per capire meglio di cosa si parla è importante chiarire il significato della parola cluster. Tradotto in italiano come “grappolo”, in informatica il cluster o meglio computer cluster viene definito<sup>119</sup> generalmente come un gruppo (o grappolo) di computer intento a condividere e scambiare informazioni. In questo senso quando l'autore parla di un gruppo ibrido clusterizzato intende soggetti che agiscono in maniera molto simile agli “hubs”, ma in maniera simultanea tra offline e online. Un esempio di questo genere è un gruppo di

---

<sup>115</sup> Berlatsky Noah, *Cybercrime*, 2013.

<sup>116</sup> Il termine craker o *hacker malicious* è stato coniato per distinguere gli hacker “cattivi” da quelli “buoni”. Un craker sfrutta la sua particolare abilità nel manipolare programmi e sistemi per fini nocivi (come innestare virus, far saltare server di rete o entrare abusivamente

<sup>117</sup> Una botnet è una rete controllata da un botmaster e composta da dispositivi infettati da malware specializzato, detti bot o zombie.

<sup>118</sup> Nel gergo informatico scareware individua una classe di software dannosi o comunque di limitata utilità la cui installazione viene suggerita agli utenti attraverso tecniche di marketing scorretto o mediante i metodi dell'ingegneria sociale.

<sup>119</sup> D.A. Bader and R. Pennington, *Cluster Computing: Applications*, The International Journal of High-Performance Computing, 15(2):181-185, May 2001.

individui, che ruba carte di credito con l'intento di utilizzare i dati per gli acquisti online o vendere i dati attraverso i *carding network* nel Dark Web.

I gruppi della forma ibrida estesa operano in modo simile agli ibridi cluster, ma sono molto meno centralizzati. In genere includono molti associati, sottogruppi e potranno svolgere una serie di attività criminali mantenendo comunque un livello di coordinamento sufficiente ad assicurare il successo delle loro operazioni.

3. Il terzo tipo di gruppo opera principalmente offline e sfrutta lo sviluppo della tecnologia per migliorare le proprie attività al di fuori della rete. L'autore sottolinea l'importanza che questi gruppi stanno avendo, contribuendo sempre di più al fenomeno della digitalizzazione del crimine. Come i precedenti tipi di gruppo, anche questo può essere suddiviso in base al loro grado di coesione e organizzazione tra "gerarchie" e "aggregati".

Le "gerarchie" o gruppi gerarchici sono meglio descritti come gruppi criminali tradizionali, come quelle a stampo mafioso. Tali organizzazioni esportano alcune delle loro attività attraverso la rete, molte volte sfruttando gruppi "hubs" o ibridi per portare a fine i propri obiettivi criminosi. Ad esempio, l'interesse tradizionale mafioso a riguardo della vendita di droghe si estende ora al mondo dei mercati di narcotici online; altri esempi includono gioco d'azzardo online, estorsione e ricatto attraverso minacce che possono esplicitarsi nell'arresto di sistemi computerizzati o nell'accesso ad informazioni private tramite attacchi malware o di hacking.

I gruppi "aggregati" sono liberamente organizzati, temporanei e spesso senza uno scopo chiaro usando le tecnologie digitali *ad hoc*<sup>120</sup>, cosa che tuttavia può infliggere danni. Gli esempi includono l'uso di *blackberry* o telefoni cellulari per coordinare attività di gruppo o disordine pubblico, come accaduto durante le rivolte a Londra nel 2011<sup>121</sup>.

Questo modello di suddivisione dei gruppi di criminalità informatica proposto da McGuire è fondamentale per capire come oggi i diversi attori criminali che si interfacciano con il mondo online, interagiscano tra loro.

I gruppi intenti ad utilizzare *onion routing* e cripto-valute possono essere identificati in maniera trasversale rispetto alla tripartizione precedentemente esposta. Nonostante questo, organizzazioni a

---

<sup>120</sup> Broadhurst R. - Grabosky P. - Alazab M. - Chon S., *Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology*. 06- 2014. p. 5-7.

<sup>121</sup> Si veda il link: <https://www.theguardian.com/media/2011/aug/08/london-riots-facebook-twitter-blackberry>

stampo tradizionale e *Cyber-Gang*<sup>122</sup>, sia in collaborazione che agenti separatamente, rappresentano oggi gli attori prevalenti e di maggiore preoccupazione nello scenario del crimine informatico<sup>123</sup>.

### 2.2.3 Incontro tra due culture criminali

Le organizzazioni criminali del vecchio secolo, per fare affari nel cyberspazio, si sono dovute servire di nuovi strumenti, piattaforme ed operatori intenti ad utilizzarli. Questo processo di evoluzione criminale era necessario, sia per aprire nuovi orizzonti di investimento e sia per proteggersi dai potenziali ostacoli provenienti dalle forze dell'ordine e dalla concorrenza di organizzazioni malavitose parallele.

Per mettere in atto questa serie di soluzioni, i membri delle organizzazioni si sono serviti, e si servono tutt'ora, delle nuove piattaforme: come i sistemi *.onion* o le reti VPN per comunicare tra loro, sfruttando inoltre i nuovi mezzi di pagamento, come le cripto-valute, per facilitare le transazioni.

Andrew Lewman, uno dei cofondatori di *TheTorProject*, in un'intervista, datata al maggio del 2017, afferma che l'uso delle e-mail criptate dai siti *onion routing* da parte dei criminali è imperante. Secondo lui il 95% del traffico su TOR è rappresentato da attività criminali<sup>124</sup>. In questo modo le organizzazioni malavitose sono proiettate a livello internazionale usando Internet per promuovere le stesse attività del mondo reale, come la compravendita di droga e armi fino al traffico sessuale. Inoltre, hanno anche appreso vantaggi dal mondo digitale per trovare nuovi sbocchi in attività criminali che includono programmi di frode collettiva, furto d'identità, e crimini bancari online.

Per organizzare questo insieme di attività in rete, si richiedono avanzate competenze informatiche che i "vecchi" modelli criminali, almeno nei primi anni della rivoluzione digitale, non potevano fornire. Così nel momento in cui i "vecchi" criminali organizzati cominciarono ad approcciarsi al mondo delle frodi bancarie nei primi anni Novanta, si resero conto che la tecnologia aveva trasformato questo particolare ramo di attività. Non serviva più corrompere cassieri al fine di ottenere informazioni da conti bancari dei clienti, ma bastava truffare gli stessi clienti, facendoli cadere in qualsivoglia "trappola" digitale, diminuendo così costi e rischi.

I membri dei nuovi gruppi organizzati si compongono di programmatori, hackers o semplicemente appassionati di informatica impegnati continuamente nel progettare nuove tecniche per commettere

---

<sup>122</sup> in riferimento ai gruppi organizzati in rete, come gli hub di McGuire.

<sup>123</sup> Report presentato da "the Studies and Threat Analysis Section, Policy Analysis and Research Branch, Division for Policy Analysis and Public Affairs, UNODC", "The Globalization of Crime - The threat of Transnational Organized Crime" 2010.

<sup>124</sup> Patrick Howell O'Neill - Tor's ex-director: *The criminal use of Tor has become overwhelming*, si veda il link: <https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop/>

atti criminali che generino profitti ricavati esclusivamente da condotte illecite online. Come ricorda Misha Glenny, giornalista e studioso di questi fenomeni criminali, il gruppo di giovani intenti a creare il primo sito DarkMarket si definiva una *gang*, ma in realtà rappresentava un “nuovo tipo di mafia”<sup>125</sup>. I gruppi cybercriminali sono oggi caratterizzati da una struttura organizzativa simile alle famiglie criminali ma sofisticate in tecniche di hacking, facendo così emergere un'economia di servizio altamente professionale nel crimine informatico cooperando con gruppi ideologici o veri e propri stati-nazione<sup>126</sup>.

Per molto tempo, i tradizionali gruppi mafiosi e i criminali informatici hanno avuto ben poco a che fare l'uno con l'altro<sup>127</sup> eppure come osserva Peter Grabosky, professore della Northwestern University, il crimine virtuale non è assolutamente diverso da quello reale, ha solo ottenuto nuovi mezzi<sup>128</sup>. Mentre la tecnologia di attuazione, e in particolare la sua efficienza, può essere senza precedenti, le attività perpetrate sono fundamentalmente familiari (truffa, contrabbando, rapina)<sup>129</sup>.

Con l'evoluzione del World Wide Web, l'e-commerce e l'uso massiccio della rete in crescita, tale scissione venne meno. Nell'arco degli anni la crescita dell'economia digitale ha causato inevitabilmente un aumento della criminalità digitale organizzata<sup>130</sup> e come afferma Kenny McKenzie, ex responsabile delle forze dell'ordine presso la BAE Systems<sup>131</sup>: “sempre più attività criminali fanno affidamento sul mondo online e una percentuale significativa, pari all'80% del volume dei reati gravi attualmente in rete, ha chiare associazioni con gruppi che mostrano vari livelli di coordinamento collettivo, scopo e capacità”<sup>132</sup>.

I nuovi boss delle organizzazioni criminali tradizionali nascono in contesti digitali e hanno una comprensione molto migliore, rispetto ai padri, dei vantaggi che le tecnologie informatiche possono offrire. Le reti criminali globali hanno nell'arco dell'ultimo decennio iniziato ad espandersi drammaticamente, grazie alla fusione delle due culture criminali.

Il punto di incontro tra “vecchio” e “nuovo” crimine ha fornito alle organizzazioni criminali nuovi mezzi per accrescere i guadagni ed espandere le proprie attività.

Un documento del 2014 scritto dalla *National Security Research Division* presso la *Rand Corporation*<sup>133</sup> afferma che il mercato nero online non è più un paesaggio composto da reti di

---

<sup>125</sup> Glenny Misha, *Mafia.com* 2012.

<sup>126</sup> Malawarebytes: *The new Mafia, Gangs and Vigilantes* – 2017.

<sup>127</sup> Ibid. Glenny Misha, 2012.

<sup>128</sup> Peter N. Grabosky, *Virtual Criminality: Old Wine in New Bottles?*, giugno 2001, si veda il link: <https://journals.sagepub.com/doi/10.1177/a017405>

<sup>129</sup> Ibid.

<sup>130</sup> Ibid. McGuire, 2012.

<sup>131</sup> BAE Systems Applied Intelligence (ex Detica) è una società internazionale di consulenza aziendale e tecnologica di proprietà di BAE Systems.

<sup>132</sup> Ibid. McGuire, 2012.

<sup>133</sup> Si veda il link: [www.rad.org](http://www.rad.org)

individui motivati dall'ego e dalla notorietà (come potevano essere gli hacker della prima generazione), ma è diventato un groviglio di elementi altamente centralizzato e organizzato, connesso con i gruppi criminali tradizionali (come cartelli della droga, mafie e cellule terroristiche)<sup>134</sup>.

Già dal marzo del 2017 Europol ha rivelato, nella sua relazione annuale riguardante la minaccia della criminalità, quale fosse il suo principale impiego: cercare di capire e combattere la digitalizzazione della criminalità organizzata<sup>135</sup>.

Le forze di polizia europee hanno individuato questa tendenza nell'evoluzione del riciclaggio di denaro connessa alle nuove forme di pagamento, nei mercati neri della rete sfruttati dalla criminalità per la vendita di prodotti e servizi illeciti e nelle molteplici altre azioni attraverso le quali i vecchi gruppi entrano in contatto con i nuovi.

Un esempio di questo genere è rappresentato da un caso del 2013, in cui la polizia belga ha arrestato membri di un'organizzazione turco-olandese impegnata nel commercio di stupefacenti che aveva reclutato (o costretto) due hacker a penetrare nel sistema informatico di un porto con un attacco di *phishing*<sup>136</sup>. Una volta dentro, la banda riuscì a rintracciare tutti i container in entrata e in uscita dal porto, avendo modo così di rilasciare i permessi necessari per appropriarsi dei contenitori che trasportavano cocaina dal Sud America<sup>137</sup>.

Il processo di digitalizzazione del crimine è andato rafforzandosi nel tempo. Qualche mese fa il procuratore aggiunto della Direzione Distrettuale Antimafia afferma che Camorra e Ndrangheta, ormai da diversi anni si sono notevolmente avvicinate al mondo delle cripto-valute per investire i propri proventi illeciti<sup>138</sup>.

Così i sistemi informatici e le tecniche di anonimato non sono più in mano esclusiva di hacker e programmatori, ma sono diventate d'uso comune per il crimine tradizionale con il fine di estorcere, spacciare droga o sponsorizzare il gioco illegale. La valuta non è più stampata solo dai governi, ma esiste nelle reti digitali, utilizzata per scopi illeciti e per il riciclaggio di denaro. Come le imprese di maggior successo oramai le organizzazioni criminali cavalcano la cresta dell'onda tecnologica investendo e impiegando ingenti somme di denaro in attività criminali in rete. Oggi più di 5.000 organizzazioni criminali in Europa, che operano su scala internazionale, sono attualmente sotto inchiesta<sup>139</sup>. Questo aumento, rispetto al 2013 (in cui Europol ne contava 3600), è principalmente

---

<sup>134</sup> Ibid., Malawarebytes, 2017.

<sup>135</sup> Europol, SOCTA 2017, si veda il link: [www.europol.europa.eu](http://www.europol.europa.eu)

<sup>136</sup> Glenny Misha, *Mafia.com* 2012.

<sup>137</sup> Ibid.

<sup>138</sup> Cipolla Alessandro, Antimafia: "Così la Camorra guadagna con la Borsa e i Bitcoin" L'allarme lanciato da Giuseppe Borrelli dell'Antimafia: "La Camorra investe in Borsa e Bitcoin perché meno accessibili alle indagini", 2 febbraio 2018, si veda il link: <https://www.money.it/antimafia-camorra-guadagna-borsa-bitcoin>

<sup>139</sup> Europol, SOCTA 2017.

dovuto a un modo di agire diverso rispetto al passato. L'aumento indica anche l'emergere di reti criminali più piccole, specialmente in mercati criminali che sono altamente dipendenti da Internet, come parte dei loro modi operandi o come veri e propri modelli di business (ad esempio i *darkmarkets*). Per il SOCTA 2017 (documento concernente lo studio sulla valutazione delle nuove minacce da parte delle organizzazioni criminali, di Europol), oltre il 45% delle organizzazioni criminali sono coinvolte in più attività illecite, per aumentare margini di profitto e mitigare rischi e costi operativi<sup>140</sup>. Il più grande campo d'investimento è il traffico di beni e servizi di più variegato genere, che possono andare dalla vendita di diversi tipi di droghe al commercio di armi.

L'integrazione dei sistemi di pagamento digitali e delle piattaforme di anonimato ha fatto sì che i mercati criminali online dilagassero in maniera prorompente dentro e fuori i confini UE.

Le classiche attività criminali si sono fortificate con l'uso della tecnologia, quindi non solo i mercati e traffici illeciti, ma anche diversi tipi frodi, lo sfruttamento sessuale di bambini, crimini relativi alla proprietà intellettuale, estorsioni, fino ad arrivare al contrabbando di essere umani e ai crimini ambientali. Così la tecnologia viene usata in ogni settore della criminalità: la tratta di persone in cui i rifugiati ricevono SIM per assistere il loro passaggio oltre confine; l'ascesa del bitcoin e di altre cripto-valute per il commercio di beni illeciti e per essere sfruttati quali nuovi mezzi di riciclaggio; l'uso onnipresente di servizi di messaggistica criptati nel commercio di specie selvatiche minacciate; e soprattutto, l'enorme distribuzione di droghe ricreative e da prescrizione<sup>141</sup>.

In questo contesto, l'interazione tra gruppi di esperti in tecniche informatiche e criminali tradizionali molte volte è necessario per commettere determinate azioni illecite, in altri casi questo incontro viene meno, grazie alla sofisticazione stessa delle vecchie organizzazioni.

Da questa analisi appare così un nuovo volto del crimine organizzato contemporaneo: da un lato i "gruppi gerarchici" di McGuire, vecchie mafie intente nel processo di digitalizzazione, e dall'altra vere e proprie associazioni per delinquere di esperti informatici<sup>142</sup>, talvolta connesse ad organizzazioni più grandi e centralizzate, talvolta agenti singolarmente.

### *2.3 I nuovi ruoli del crimine organizzato digitalizzato*

Per comprendere meglio come tali forme di gruppi criminali agiscono, in maniera specifica nel rapporto tra cripto-valute e reti anonime, si possono evidenziare tre ruoli chiave attraverso i quali vengono svolte le diverse attività illecite. Le organizzazioni criminali possono diventare:

1. fornitori di prodotti e servizi,

---

<sup>140</sup> Ibid.

<sup>141</sup> Ibid.

<sup>142</sup> In riferimento ai gruppi "hubs" di McGuire,

2. investitori,
3. agenti come mano guida.

### 2.3.1 Fornitori di prodotti e servizi

Nonostante esistano reti già fortemente strutturate sul territorio attraverso le quali le organizzazioni criminali hanno modo di scambiare prodotti e servizi, possiamo senza dubbio affermare che i siti *.onion* nelle Darknet si prestano ugualmente a proliferi commerci illeciti.

L'ex direttore di Europol Rob Wainwright afferma che il mercato del contrabbando online nell'Unione sia in forte crescita e acquisisca tra i 3 e i 5 miliardi di entrate annue<sup>143</sup>. I molteplici prodotti venduti vanno dai diversi tipi di droga fino ad armi, malware e dati ed informazioni personali illegalmente acquisiti e poi rivenduti sui mercati online. Altra attività tradizionale sotto influenza del crimine organizzato, è il gioco d'azzardo online che gestisce volumi enormi di transazioni e flussi di contante che purtroppo possono occultare e mascherare il riciclaggio di denaro<sup>144</sup>. Basti pensare che il numero dei siti non autorizzati supera di oltre dieci volte quello degli operatori che invece lo sono.<sup>145</sup> Molti di questi siti, se non la maggior parte<sup>146</sup>, operano nelle Darknet consentendo pagamenti attraverso cripto-valute. Queste modalità rendono così i portali del gioco illegale protetti da anonimato.

Come detto precedentemente, tutte le merci e i servizi messi a disposizione nelle Darknet sono acquistabili attraverso cripto – valuta ed è necessario quindi che le organizzazioni investano in bitcoin o in altri tipi di monete virtuali per dare il via a tali meccanismi.

### 2.3.2 Investitori in cripto-valute

Oltre per l'uso improprio che se ne fa nei *Darkmarkets*, esistono diversi motivi per cui il crimine organizzato voglia investire in cripto-valute. Non essendo supportate da alcun governo o autorità centrale, non sono soggette alle pressioni politiche o economiche che regolano le autorità bancarie centrali e private emittenti moneta<sup>147</sup>. La mancanza di controllo consolidato rende le cripto-valute attraenti sia per coloro che desiderano cimentarsi in attività illegali che per chi volesse sostenere

---

<sup>143</sup> Vitrais Benjamin, Europol: *The Dark Web Is The Heaven For Organized Criminals In The EU*, del 9 maggio 2017, si veda il link: [www.deepdotweb.com/2017/05/09/europol-dark-web-heaven-organized-criminals-eu](http://www.deepdotweb.com/2017/05/09/europol-dark-web-heaven-organized-criminals-eu)

<sup>144</sup> Romiti Maria Luisa, *Riciclaggio e gioco d'azzardo on line Il dark web sfrutta i "casinò" in rete*, 2014.

<sup>145</sup> Ibid.

<sup>146</sup> Choi Sinyong, *Illegal Gambling and Its Operation via the Darknet and Bitcoin: An Application of Routine Activity Theory* 2018.

<sup>147</sup> Matonis Jon, ECB: *Roots of Bitcoin Can Be Found in the Austrian School of Economics*, FORBES BLOG 3-11- 2012

organizzazioni dissidenti, come ad esempio nel caso di WikiLeaks<sup>148</sup>. L'ulteriore vantaggio è che tali transazioni possono essere eseguite oltre i confini senza i limiti che provengono dall'ampio processo di autorizzazione richiesto per l'uso delle carte di credito<sup>149</sup>. La mancanza di un verificatore di terze parti, l'anonimato, e la graduale applicazione delle cripto-valute in tutto il mondo apre una porzione più ampia di attività commerciali illecite ed ulteriori possibilità di effettuare transazioni senza passare per alcun istituto centralizzato.

Questo insieme di elementi fanno sì che la cripto-valuta sia un "bene" altamente appetibile per le organizzazioni criminali, non solo per far funzionare i mercati illeciti online ma come mezzo per altri scopi criminali ed investimenti.

Uno dei principali scopi delle organizzazioni criminali è quello di "allontanare" il denaro dalle relative origini illecite, ostacolando la tracciabilità delle origini dei proventi. Le cripto-valute sono un nuovo modo di nascondere la vera identità dei proventi ricavati illegalmente, ed anche un modo di nascondere la vera identità dell'utente.

L'uso delle cripto-valute nell'ambito del cybericiclaggio è un'attività entrata nella prassi di molte organizzazioni criminali<sup>150</sup>; il denaro può essere riciclato più velocemente tramite le monete virtuali rispetto ai mezzi tradizionali, avendo la possibilità di suddividere il capitale in più conti, equivalentemente al numero di *wallet* che si desidera possedere<sup>151</sup>. Nel 2016, un pagamento effettuato su un conto in Bulgaria è stato rintracciato per essere ulteriormente suddiviso in dodici diversi conti, biforcando tutti i soldi in diverse città della Russia rintracciando il segnale della chiave pubblica da qualche parte in Germania<sup>152</sup>.

Giuseppe Borrelli, procuratore aggiunto della Direzione distrettuale Antimafia (DDA), ha osservato come la criminalità organizzata starebbe, specialmente negli ultimi anni, investendo in Borsa e in particolare nei Bitcoin<sup>153</sup>, proprio per perseguire scopi legati al riciclaggio; un tema che si approfondirà nel corso dello svolgimento del seguente lavoro.

---

<sup>148</sup>Matonis Jon, WikiLeaks Bypasses Financial Blockade with Bitcoin, FORBES BLOG 20-08-2012. si veda il link: <http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin>

<sup>149</sup>J.P. & G.T., Bits and Bob, "The Economist": *Babbage* 13-06-2011, si veda il link: <http://www.economist.com/blogs/babbage/2011/06/virtual-currency>.

<sup>150</sup>Milad George, Irwin S.M. Angela: *The use of crypto-currencies in funding violent jihad*, *Journal of Money Laundering Control*, Ottobre 2016.

<sup>151</sup>Nel Capitolo III, se ne approfondiranno gli aspetti.

<sup>152</sup>Rhyme Upadhyaya, Aruna Jain, *Cyber ethics and cyber crime: A deep dwelled study into legality, ransomware, underground web and bitcoin wallet*, 2016.

<sup>153</sup>Ibid. Cipolla Alessandro, 2018.

### 2.3.3 Mano Guida:

Il terzo ruolo attraverso il quale il crimine organizzato si interfaccia con l'*onion routing* e le cripto-valute è quello di essere coinvolto direttamente in un'azione cyber ed agire come mano guida in determinate operazioni. Queste azioni sono perpetrate attraverso il reclutamento di personale qualificato nell'uso di tecniche informatiche oppure da veri e propri gruppi cybercriminali che agiscono esclusivamente online (come gli "hub" di McGuire).

Le forme di cybercriminalità organizzata colgono l'opportunità per eseguire numerosi attacchi intenti a distruggere, abusare o bloccare i sistemi informatici<sup>154</sup>. Oltre i virus o i malware che causano seri danni a database, software o a siti web, un crimine particolarmente perpetrato dai cybercriminali è rappresentato dall'estorsione attraverso reti informatiche<sup>155</sup>. Questi crimini vengono commessi attraverso minacce telematiche, annunciando di bloccare un sistema o cancellare i dati di un database con l'uso di determinati cyber-attacchi. L'estorsione sulle reti informatiche è diventata una pratica regolare in questi anni e ci sono molti gruppi organizzati che seguono questo esempio attraverso l'aiuto di DoS<sup>156</sup> o malware<sup>157</sup>, utilizzando cripto-valute ed anonimato per far perdere le tracce del proprio operato. Attraverso lo *skimming*, il *phishing*, i *trojan* bancari<sup>158</sup> o altre frodi online i *carders* acquisiscono numeri di carte di credito, o violano sistemi bancari per poi rivendere tutto il materiale sul Darkweb. La spiegazione a queste condotte è che appare più semplice vendere carte di credito rubate che usarle<sup>159</sup>. I mercati delle *darknet* infatti assicurano l'anonimato delle transazioni permettendo ai *carders* di rimanere al sicuro. Ad esempio, se un *carder* russo ha hackerato o frodato un sistema bancario nel Regno Unito, non può usare la carta di credito a causa delle leggi internazionali sulla protezione dalle frodi<sup>160</sup>. Le banche, responsabili della tutela dei clienti e della sicurezza interna, se si accorgessero di un movimento insolito bloccherebbero il conto o metterebbero in allerta le forze dell'ordine. A questo punto il *carder* si opererà per mettere in vendita su un mercato in lingua inglese i dati della carta, così se un cittadino

---

<sup>154</sup> EUROPOL - (IOCTA) 2016. p. 45-46.

<sup>155</sup> Ibid.

<sup>156</sup> Uno degli attacchi lanciati più spesso, nella consumazione di questi crimini, è il Denial-of-Service (DoS- negazione del servizio) che persiste nel tentativo di impedire agli utenti legittimi di accedere ad informazioni o servizi all'interno del proprio sistema. Prendendo di mira un computer o la connessione di rete dei siti che si sta tentando di utilizzare, un malintenzionato può essere in grado di impedire l'accesso alle e-mail, a siti web, ai conti online (bancari, ecc.), o ad altri servizi sul computer interessato. Tale tipo di attacco può essere fatto anche su larga scala, come nel caso del DDoS (Distributed Denial-of-Service), coinvolgendo più reti computerizzate e più sistemi, permettendo di bloccare intere società o uffici statali. Attraverso l'uso delle botnet, questi attacchi possono essere lanciati a sistemi aziendali anche se protetti in maniera efficace.

<sup>157</sup> Si veda il link: <https://www.cardschat.com/news/pokerstars-ddos-attackers-arrested-by-europol-extortiongroup-also-alleged-to-have-targeted-betfair-neteller-18629>

<sup>158</sup> programma intento a spiare all'interno di un computer bancario.

<sup>159</sup> Si veda il link: <https://deep-weblinks.com/deep-web-credit-card-numbers/>

<sup>160</sup> Come le leggi per la tutela del consumatore ecc... si veda il link: <https://www.cibc.com/en/privacy-security/debit-and-credit-card-fraud.html>

britannico volesse acquistarla sarebbe più al sicuro nell'utilizzarla, trasferendo ad esempio attraverso bonifico dei soldi su altri conti<sup>161</sup>. Nel novembre 2017, quattro membri chiave di una rete criminale internazionale responsabile della compromissione di dati di carte di pagamento e di transazioni illecite ai danni di cittadini europei, sono stati arrestati durante l'operazione *Neptune*<sup>162</sup>. L'operazione congiunta, guidata dalle autorità italiane, in cooperazione con le forze dell'ordine bulgare e ceche, sostenuta dall'Europol (EC3), è culminata nell'arresto dei leader del gruppo criminale che agiva su base transnazionale supervisionando attivamente tutte le fasi delle attività criminali, compresa l'installazione di attrezzature tecniche sugli sportelli automatici in aree centrali delle città europee, producendo carte di credito contraffatte, rivendendole sul Darkweb e successivamente incassando denaro dagli sportelli automatici nei paesi extraeuropei<sup>163</sup>.

---

<sup>161</sup> Si veda il link: <https://www.theguardian.com/money/2018/jul/07/heres-how-scammers-get-away-with-it>

<sup>162</sup> Si veda il link: <https://www.europol.europa.eu/newsroom/news/organised-criminals-dealing-electronic-payments-disrupted-in-italy-bulgaria-and-czech-republic>

<sup>163</sup> Europol, IOCTA 2018.

## Capitolo III - L'economia sotterranea del crimine: dalle Darknet al Cybericiclaggio

### 3.1 Il mondo delle reti oscure: i cripto-mercati

Nelle Darknet sono presenti forum esplicitati attraverso *chat room* e servizi di comunicazione, per pianificare e coordinare i crimini. Esempi di questo genere sono le segnalazioni secondo cui alcuni di coloro che si occupano di frodi a rimborso fiscale hanno discusso metodi e tecniche sul Dark Web<sup>164</sup>. Questi forum infatti possono essere divisi in appositi spazi dedicati all'hacking, al *carding* e ad altri argomenti che coprono una vasta gamma di prodotti e servizi che servono all'intero spettro della criminalità informatica.

L'anonimato che garantisce la *onion routing* rende l'uso delle e-mail anonime molto frequente, compreso lo scambio di file in p2p. Altre pagine presenti sono correlate a siti di truffa, *phishing*, e altri servizi di frode. Tra i contenuti di queste reti sono incluse pagine talvolta molto regolamentate o illegali nelle *clearnet*, come quelle pornografiche e pedopornografiche. La natura dello sfruttamento sessuale dei minori sui forum della Darknet promuove l'abuso di nuove vittime con il fine di fornire nuovo materiale<sup>165</sup>. L'ambito della pedopornografia online tocca moltissimi aspetti che vanno dagli abusi, al traffico di bambini per scopi sessuali, alla produzione di pornografia infantile fino alla sua messa in commercio<sup>166</sup>. Nel più dei casi gli attori coinvolti in questi crimini partecipano alla commissione del reato in maniera diversa e con ruoli differenti<sup>167</sup>. Le forme di criminalità organizzata in relazione all'ambito d'interesse di questo lavoro<sup>168</sup>, si impegnano parzialmente nel commercio del materiale pedopornografico<sup>169</sup> che rappresenta solo uno degli aspetti di un più ampio settore criminale. Per questo motivo si accenneranno alcune delle caratteristiche legate alla vendita di tale materiale nelle Darknet, senza indagare l'interezza dell'argomento al quale sarebbe più proprio dedicarvi un lavoro a parte.

Senza dubbio il mezzo attraverso il quale è aumentata la conoscibilità delle reti oscure, sono i mercati e le iniziative commerciali che si specializzano nella vendita di prodotti illeciti o pesantemente regolamentati, attraverso i quali il crimine organizzato ha avuto modo di creare una vera e propria economia sotterranea.

---

<sup>164</sup> Krebs Brian, *Tax Fraud Advice, Straight From the Scammers*, Krebs on Security, 24 Marzo 2015.

<sup>165</sup> Europol, *The Internet Organised Crime Threat Assessment (IOCTA)*, 2014.

<sup>166</sup> UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, 2015, p.8-13.

<sup>167</sup> Ibid.

<sup>168</sup> da un lato organizzazioni criminali di vecchio stampo (che usano internet per rafforzare le attività al di fuori della rete) e dall'altro i gruppi cybercriminali che operano esclusivamente nell'ambito digitale (in riferimento ai *carder*, *hacker*. gli hub di McGuire).

<sup>169</sup> Ibid., UNODC, 2015, p. 33.

I cripto-mercati facilitano la vendita di droghe, armi da fuoco e beni digitali come le informazioni sulle carte di credito rubate o falsi documenti di identità<sup>170</sup>. Questi mercati sono costituiti da siti Web, in molti modi simili ad altre piattaforme online che facilitano il commercio, come eBay o Amazon. La differenza fondamentale è l'anonimato offerto dall'accesso a tali mercati<sup>171</sup> che può essere raggiunto in diversi modi. Esistono siti web “di superficie”<sup>172</sup> che forniscono elenchi di indirizzi .onion per i mercati oscuri, abilitando così l'accesso immediato; ci sono anche dei siti specchio sulla superficie del web che forniscono collegamenti ipertestuali a siti nascosti corrispondenti ed infine ci sono mercati “solo su invito” nei quali solo gli utenti correnti hanno modo di far accedere utenti esterni interessati<sup>173</sup>. Questi domini nascosti applicano compravendite in cripto-valute per massimizzare l'anonimato<sup>174</sup>. In questo scenario, domanda e offerta si autoregolano attraverso norme sociali più o meno formali, valori e credenze culturali che hanno alimentato la crescita di un mercato nero su una scala senza precedenti<sup>175</sup>.

Interfacce *user-friendly*<sup>176</sup> e funzionalità d'offerta sono simili a quelle fornite da aziende di e-commerce sul web di superficie, come sistemi di *feedback* che consentono ai clienti di valutare i venditori e rivedere i prodotti. Allo stesso tempo, un sistema del genere aiuta a creare fiducia tra venditori e compratori che non si conoscono<sup>177</sup>. I clienti possono scegliere tra vari *marketplace* e venditori, creando così un elevato livello di concorrenza tra venditori e tra piattaforme; dando vita ad una delle reti commerciali illecite più grandi al mondo<sup>178</sup>.

La diffusione degli smartphones ha portato molti dei mercati neri della rete ad evolversi, creando delle *Photo-sharing applications platform*, applicazioni per la condivisione di foto e video sui prodotti illeciti venduti nei *darkmarkets*<sup>179</sup>. Questi servizi consentono agli utenti di creare comunità “sotterranee” con l'interesse primario di poter discutere, scambiare informazioni ed acquistare prodotti illeciti (principalmente droga), usando inoltre degli *hashtags* in modo da facilitare la ricerca interna. I clienti hanno la possibilità di scorrere le foto di prodotti pubblicizzati e quindi contattare il

---

<sup>170</sup> Ibid. IOCTA 2014.

<sup>171</sup> European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) ed Europol, *Drugs and the darknet: Perspectives for enforcement, research and policy*, 2017.

<sup>172</sup> Siti presenti nelle Clearnet.

<sup>173</sup> Ibid. EMCDDA, 2017.

<sup>174</sup> Abdulmajeed Alhagbani, *Going Dark: Scratching the Surface of Government Surveillance*, 2015.

<sup>175</sup> Meropi Tzanetakis, *Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time*, 2018.

<sup>176</sup> Tipo di software di facile usabilità. Prende l'utente “per mano” e, anche grazie ad una interfaccia grafica (GUI) accattivante e all'uso di menu, pulsanti, icone, mouse, lo accompagna amichevolmente alla finalizzazione del compito prefisso.

<sup>177</sup> Bakken, Silje; Møller, Kim & Sandberg, Sveinung. *Coordination problems in dark net drug markets: Changes in cooperation, competition and valuation*. European Journal of Criminology. 2017.

<sup>178</sup> Meropi Tzanetakis, *Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time*, 2018.

<sup>179</sup> SOCTA, 2017.

rivenditore privato utilizzando le funzionalità di messaggistica istantanea<sup>180</sup>. L'eventuale transazione si svolge o faccia a faccia o direttamente online in cripto-valuta, con la conseguente consegna per posta.

Le ricerche su questi mercati hanno dimostrato l'esistenza di più di un centinaio di siti oscuri in lingua inglese, senza contare quelli stranieri sparsi in tutto il mondo e quelli con una portata geografica limitata, come quella nazionale<sup>181</sup>. Una ricerca dell'Osservatorio europeo delle droghe e delle tossicodipendenze (OEDT) in cooperazione con Europol datata al maggio del 2017 ha riportato un'indagine sui mercati delle Darknet presenti nei 28 paesi membri dell'Unione. Due terzi dei paesi contattati hanno risposto alla richiesta dati, tra questi, quattro paesi hanno riferito un totale di nove mercati nazionali Darknet: cinque in Francia, due in Finlandia, uno in Svezia e uno in Norvegia<sup>182</sup>.

Una ricerca aggiuntiva ne ha identificati altri quattro francesi, tre italiani e quattro russi (esclusivamente operanti in Russia) portando così il totale della ricerca a 20 mercati nazionali in sei paesi<sup>183</sup>. Le diverse entità presenti in questa vasta rete commerciale collaborano tra loro scambiando tecniche di anonimato e modalità attraverso le quali rendere sempre più sicure le transazioni. Il processo che ha portato lo sviluppo di questo sistema mette le proprie radici nel periodo concomitante alla nascita del world wide web<sup>184</sup>.

### 3.1.1 Modelli di mercati neri della rete

L'economia sotterranea del crimine informatico è estremamente vasta e spesso la sua dimensione e struttura è difficile da comprendere. Oggi i *darkmarkets* ospitano una molteplicità di partecipanti e sono costantemente in cambiamento a causa della loro natura illegale. Nonostante ciò nell'arco del tempo i mercati neri della rete si sono affermati, creando una loro clientela in continua crescita. A partire dal gennaio 2016, si stima che i cripto-mercati abbiano generato un volume di denaro mensile che si attesta tra 14,2 e i 25 milioni di dollari americani<sup>185</sup>.

Un mercato di questo genere, come abbiamo avuto modo di sottolineare in precedenza, non è altro che un servizio nascosto<sup>186</sup> implementato da un software anonimo, come TOR che rende non rintracciabili gli indirizzi IP degli utenti. Il commercio illegale è abilitato dai siti caricati su tali

---

<sup>180</sup> Ibid.

<sup>181</sup> Ibid. EMCDDA 2017.

<sup>182</sup> Ibid.

<sup>183</sup> Ibid.

<sup>184</sup> Nel dicembre del 1990 viene implementato il sistema di comunicazione basato sui servizi forniti dalla Internet, il world wide web.

<sup>185</sup> Kruithof Kristy, *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*, Rand Corporation, 2016.

<sup>186</sup> In riferimento al Capitolo I.

servizi che consentono ad acquirenti e venditori di interagire e negoziare in anonimato. I mercati delle Darknet consentono i pagamenti attraverso cripto-valute offuscando le transazioni, specialmente con l'uso negli ultimi anni di Monero e Zcash<sup>187</sup>.

Esistono attualmente due tipi di entità commerciali del web oscuro: i cripto-mercati e i così detti *vendor shop*<sup>188</sup>, singoli venditori, connessi o legati ai mercati.

I cripto-mercati riuniscono molteplici venditori gestiti da un gruppo di amministratori del mercato (ovvero della pagina web) in cambio di una commissione sulle vendite, attività speculare a ciò che avviene nelle *clearnet* con Amazon ed Ebay. Al pari delle realtà legali in rete, esistono forti strutture gerarchiche per ogni mercato, intente nel gestire l'architettura di questi sistemi. Gruppi o individui all'apice dell'amministrazione richiedono un compenso più elevato rispetto ai medi intermediari che si occupano di funzioni di hosting o di servizi di tesoreria e di cassa. I servizi offrono modalità di scambio che consentono di fare transazioni, con uso di cripto-valuta, seguite da *feedback* (su una scala da 0 a 5 stelle) collegate ad ogni acquisto, con punteggi aggregati e visualizzabili sul *marketplace* con il fine di guidare i clienti nella selezione di fornitori affidabili e di prodotti altamente qualificati<sup>189</sup>. Proprio questo sistema rende i cripto-mercati unici nella loro specie, andando ad offrire un meccanismo di reputazione bilaterale che infonda fiducia sia nei commercianti che negli acquirenti, proteggendo l'anonimato di entrambi ed andando a facilitare transazioni ripetute<sup>190</sup>.

Una homepage classica fornisce link legati ad informazioni e ai servizi supportati dal mercato che includono le categorie dei prodotti offerti, un sistema di messaggistica istantanea per permettere comunicazioni dirette e forum di discussioni riguardante le attività del mercato. I cripto-mercati tendono a specializzarsi soprattutto nella vendita di droghe illegali<sup>191</sup> o dei prodotti correlati, ma offrono anche elenchi collegati ad altre attività fraudolente, tra cui carte di credito rubate, informazioni sull'identità, e armi da fuoco, meno comunemente disponibili alla vendita rispetto alle altre categorie<sup>192</sup>.

L'altro tipo di attività disponibile nelle reti oscure è il così detto *vendor shop*, noto anche come “negozio a venditore singolo”, pagine create direttamente dal fornitore del prodotto o del servizio, che in molti casi commercia parallelamente su un cripto-mercato. Questi negozi digitali vendono

---

<sup>187</sup> In riferimento al Capitolo I.

<sup>188</sup> Persi Paoli Giacomo, Judith Aldridge, Nathan Ryan, Richard Warnes, Behind the Curtain, *the illicit trade of firearms, explosives and ammunitions on the dark web*, © Copyright 2017 RAND Corporation.

<sup>189</sup> Van Houta, Tim Bingham, *Silk Road', the virtual drug marketplace: A single case study of user experiences*, 2013.

<sup>190</sup> Hardy Robert August, Julia R. Norgaard, *Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web*, 2015.

<sup>191</sup> Aldridge & Décary-Héту Not an 'Ebay for Drugs': *The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation*, 2014.

<sup>192</sup> Giacomo Persi Paoli, Ibid. 2017.

direttamente ai clienti, disposti ad acquistare il prodotto senza alcuna terza parte o intermediario, rendendo così le transazioni più rischiose e soggette a truffa, disincentivando la clientela ad entravi. Dall'altra parte queste pagine, legandosi ai cripto-mercanti, possono sfruttare quest'ultimi come punto di lancio per mettere a conoscenza i clienti delle proprie attività. I *vendor shop* nel web oscuro si pongono come punti in cui vengono venduti prodotti specializzati, con una particolare attenzione al commercio di armi<sup>193</sup>, al contrario dei cripto-mercanti che offrono una gran quantità di prodotti e servizi.

Tale economia sotterranea non deve essere intesa come un sistema unitario, al contrario, i *darkmarkets* si differenziano tra loro soprattutto in relazione al paese di provenienza<sup>194</sup>.

I mercati neri online di origine russa si caratterizzano per essere altamente specializzati nella vendita di nuovi malware sofisticati, di servizi di *carding* ed offrono inoltre numerose opzioni di riciclaggio di denaro<sup>195</sup>. In questi mercati, con struttura fortemente gerarchica, i venditori non offrono tutto, commercializzano solo ciò in cui sono maggiormente specializzati e tra loro esiste un'altissima competizione sia nel raffinare le modalità di pagamento che nel migliorare la spedizione dei prodotti<sup>196</sup>. Sulla stessa linea i mercati giapponesi e ancor di più quelli cinesi che tendono ad usare canali di accesso altamente ricercati, specializzandosi anche loro nella creazione di nuove tecniche d'innovazione per la criminalità informatica, vendendo oltre che software, hardware adattabili alle pratiche criminali<sup>197</sup>. A differenza dei precedenti altri mercati, quelli nord/sud americani ed europei hanno un'impostazione nettamente più aperta, incoraggiando clienti e cyber-criminali ad entrare<sup>198</sup>. I cybercriminali in Brasile che, al pari dei russi e cinesi, si specializzano nella produzione e vendita di *malaware* come Trojan bancari e altri software dannosi, usano piattaforme popolari come Facebook, Twitter, Skype e WhatsApp per comunicare e mettere a conoscenza colleghi e clienti della presenza dei prodotti nel mercato sotterraneo, incuranti dei controlli da parte governativa<sup>199</sup>. In questo tipo di mercati le categorie a disposizione sulla homepage sono centinaia, mettendo in commercio molteplici prodotti e servizi di diverso genere e tipologia.

*Dreammarket*, il più vecchio e vasto dei mercati occidentali esistenti<sup>200</sup>, esclusivamente in lingua inglese, si pone apertamente al pari delle altre piattaforme di e-commerce nelle *clearnet*. La

---

<sup>193</sup> Ibid.

<sup>194</sup> Trend Micro, *Cybercrime and the Deep Web - Forward-Looking Threat Research* (FTR) Team, 2016.

<sup>195</sup> Trend Micro, *Russian Underground 2.0*, 2015.

<sup>196</sup> Ibid.

<sup>197</sup> Trend Micro, Ibid. 2016.

<sup>198</sup> Ibid.

<sup>199</sup> Mercedes, Fernando. *The Brazilian Underground Market* 2014, Si veda il link:

<https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/whitepapers/wp-the-brazilian-underground-market.pdf>.

<sup>200</sup> Si veda il link: <https://www.darknetmarkets.com/dream-market/>

categoria prescelta dai clienti è la droga, con ben 61'457 inserzioni<sup>201</sup> tra cui cannabis, ecstasy oppioidi e cocaina tra le più vendute, seguita poi da beni digitali (dati personali, dati relativi a frodi, mezzi di frode, software ecc..) e servizi (da servizi di hacking a banconote contraffatte, fino a passaporti e carte di identità falsificate)<sup>202</sup>.

Su impostazione simile si basano gli altri mercati occidentali tra cui i più famosi: Wall st Market, il più moderno e innovativo in rete per le sue tecniche tese ad evitare qualsiasi tipo di frode; il mercato di Tochka, ora rinominato mercato libero Point / T • chka, che garantisce a sua volta attraverso un sistema di segnalazione di truffe la sicurezza negli acquisti; il Berlusconi Market, di origine italiana emerso nell'estate del 2017 che nell'arco dell'ultimo anno si è posizionato tra i migliori mercati esistenti; ed Empire Market nato nei primi mesi del 2018 in risposta alla chiusura del più famoso Aphabay<sup>203</sup>. Oggi l'espansione del fenomeno dei *darkmarkets* in rete è di enorme portata e tende sempre più attraverso l'uso di nuove tecnologie a raffinarsi.

Essendo realtà in continuo mutamento in un mondo vasto come quello della rete, nonostante le differenze che intercorrono tra i diversi mercati, i cybercriminali collaborano tra loro, condividendo strumenti, informazioni, *know-how* e le migliori pratiche tese al miglioramento del commercio illegale in rete.

### 3.1.2 Prodotti e servizi

Come si è potuto notare dall'evoluzione che hanno subito i cripto-mercati nell'arco degli ultimi venti anni e dallo sviluppo che hanno avuto in occidente, oggi nelle reti oscure si vendono plurimi prodotti e servizi. Le categorie di prodotti più selezionati nei *darkmarkets* sono droga, falso documentale, banconote contraffatte, dati di carte di credito o di account bancari, armi ed esplosivi fino ad arrivare a malware ed altri strumenti di hacking.

Per far sì che i prodotti materiali arrivino al destinatario i venditori devono fare affidamento ai servizi postali ordinari, esponendo così gli acquisti ai controlli di funzionari doganali, dell'ufficio postale e talvolta delle forze dell'ordine. Esistono così, per prevenire eventuali rischi associati ai controlli, variegate tecniche di occultamento dei prodotti, discusse ed implementate sui forum dedicati, sia nel dark web che sulle *clearnet*<sup>204</sup>. Usando i forum dei mercati, i venditori possono discutere delle tecniche di spedizione ed accordarsi con i clienti su quale sia il modo migliore per ricevere il prodotto. Una delle tecniche più utilizzate è quella di spedire i prodotti insieme ad altri, come ad esempio quelli associati all'elettronica di consumo: stampanti, smartphones, televisori, o in

<sup>201</sup> Si veda il link: <https://darkwebnews.com/dark-web-market-list/>

<sup>202</sup> Si veda il link: <https://dreammarketdrugs.com/product-listing-of-dream-market/>

<sup>203</sup> Si veda il link: <https://darkwebnews.com/darkwebmarkets/empire-market-guide/>

<sup>204</sup> Ibid. Giacomo Persi Paoli, 2017.

custodie per strumenti con un doppio fondo<sup>205</sup>. I venditori possono inoltre inviare il prodotto in diverse spedizioni, come nei molteplici casi della compravendita di armi<sup>206</sup>, inviate in pacchi separati consentendo al destinatario di riassemblare le parti in un'arma funzionante senza comprometterne la qualità. In molti casi gli ordini avvengono all'ingrosso ed esistono delle vere e proprie promozioni che includono la diminuzione dei costi di spedizione<sup>207</sup>. Questo insieme di tecniche unite, ad esempio, all'inserimento di un indirizzo di una persona totalmente estranea allo scambio, permette al ricevente di andare a ritirare il pacco una volta inviato senza particolari rischi. Il sistema commerciale dei cripto-mercati si assicura così oltre che la garanzia di qualità del prodotto attraverso i *feedback*, qualità e sicurezza nella spedizione o attraverso previ accordi o attraverso regole prestabilite, andando a creare un modello strutturato con un fatturato mensile di decine di milioni di euro<sup>208</sup>.

### 3.1.2.1 Droga

Il commercio online di droghe rappresenta l'attività più diffusa nei mercati online illeciti, con una crescita progressiva del fenomeno nell'arco degli ultimi quattro anni<sup>209</sup>. Nell'era dei cripto-mercati, avere un buon servizio clienti, capacità di scrittura e una buona reputazione tramite *feedback* può essere per fornitori e acquirenti un buon modo di interfacciarsi<sup>210</sup>. I mercati della Darknet fungono così da intermediari virtuali che collegano venditori di livello superiore, medio e al dettaglio con i consumatori.

Questi mercati online offrono una gamma di narcotici differenti che vanno dalle droghe comuni fino a sostanze chimiche utilizzate per la fabbricazione di nuove o per altri scopi illeciti, dando una vastissima scelta al cliente. Per tutte le droghe più note l'unità più venduta in Europa è un grammo, solo nel caso della cannabis o dell'MDMA le vendite vanno da uno ai dieci grammi<sup>211</sup>. Tale minimizzazione dei prodotti può far pensare all'uso esclusivamente personale degli acquisti; tuttavia una percentuale significativa dello spaccio online è destinato ad un secondo ciclo di vendita, attraverso acquisti raggruppati<sup>212</sup>. Molte delle pagine esistenti offrono una sorta di "promozione" all'ingrosso intorno ai mille dollari o più<sup>213</sup> per prodotto. Inoltre, le droghe

---

<sup>205</sup> Ibid.

<sup>206</sup> Si veda il link: <https://www.telegraph.co.uk/news/2016/04/12/how-criminals-on-the-dark-web-are-smuggling-weapons-into-britain/>

<sup>207</sup> Giacomo Persi Paoli, Ibid. 2017.

<sup>208</sup> EMCDDA, 2016.

<sup>209</sup> Europol, IOCTA 2018.

<sup>210</sup> EMCDDA, 2016.

<sup>211</sup> Ibid.

<sup>212</sup> Ibid.

<sup>213</sup> <https://www.theguardian.com/world/2016/feb/11/online-market-turning-drug-dealers-goons-geeks-darknet>

disponibili online tendono ad essere di purezza più elevata di quelle distribuite nelle strade<sup>214</sup>, attirando in rete una sempre crescente fetta di clientela, intenta in parte a diluire il prodotto per poi rivenderlo in quantità maggiori. Dai diversi studi ufficiali riportati a livello internazionale ed europeo<sup>215</sup> si mostra come i mercati online della droga fatturino milioni di euro annui al passo con i mercati offline, ed in continua evoluzione, contribuendo alle entrate delle organizzazioni criminali che sfruttano questi canali principalmente per la vendita al dettaglio.

### 3.1.2.2 Falso Documentale

Una delle attività maggiormente perpetrate nei *dark markets*, solitamente subito dopo la compravendita di droga, è la fornitura di documenti falsi<sup>216</sup>, come passaporti, documenti d'identità, patenti di guida, certificati di nascita ecc.

Un business in crescita in Italia, come dimostrano gli arresti effettuati dalle forze dell'ordine nell'ambito dei controlli antiterrorismo<sup>217</sup>. Da anni a questa parte il dark web è diventato luogo attraverso il quale criminali e terroristi si appropriano di documenti di identità fraudolenti o falsi documenti di viaggio per svolgere le loro attività illegali<sup>218</sup>. Tramite gli indirizzi indicizzati e il motore di ricerca TOR è facile trovare siti come FakeID, che offrono documenti finti a prezzi stracciati, da 400 euro per un passaporto brasiliano fino ad 850 euro per il set completo di passaporto, carta d'identità e patente norvegese<sup>219</sup>. Inoltre, per sovrapprezzi non specificati si offrono di affrancare i documenti con vari timbri aeroportuali per dargli verosimiglianza e di aggiungere il numero del documento al database centrale o nazionale<sup>220</sup>.

### 3.1.2.3 Banconote false e carte di credito

La proliferazione delle banconote contraffatte negli ultimi anni è stata una conseguenza del dilagare delle vendite sul dark web<sup>221</sup>. Sono disponibili tutte le valute principali, ma la qualità e la quantità

---

<sup>214</sup> Ibid.

<sup>215</sup> In riferimento ai documenti UNDOC citati, EMCDDA, Europol IOCTA (sia 2014 che 2018).

<sup>216</sup> Ramacciotti Stefano, CISSP–Pierluigi Paganini del G.d.L. *Educazione alla Sicurezza Informatica, Deep e Dark Web*, 2018.

<sup>217</sup> Si veda il link: [https://www.repubblica.it/tecnologia/sicurezza/2015/11/30/news/passaporti\\_falsi\\_a\\_400\\_euro\\_al\\_mercato\\_del\\_deep\\_web-128497342/](https://www.repubblica.it/tecnologia/sicurezza/2015/11/30/news/passaporti_falsi_a_400_euro_al_mercato_del_deep_web-128497342/)

<sup>218</sup> Si veda il link: <https://www.interpol.int/es/Criminalidad/Delincuencia-financiera/Counterfeit-currency-and-security-documents/Identity-and-travel-document-fraud>

<sup>219</sup> Ibid.

<sup>220</sup> Si veda il link: <https://www.analidifesa.it/2015/11/come-ho-trovato-documenti-siriani-armi-e-denaro-sul-deep-web/>

<sup>221</sup> Si veda il link: <https://www.europol.europa.eu/newsroom/news/eu-wide-action-against-buyers-of-counterfeit-money-darknet>

varia. In questi tipi di transazioni è comune ottenere 2000 euro contraffatti per una somma di 500 euro, il cui valore sarà traslato in cripto-valute<sup>222</sup>. Tutte le transazioni vengono eseguite con la promessa che le banconote acquistate possano essere sottoposte a controlli standard, compreso quello della luce ultravioletta.

Sui *darkmarket* continua, dalla loro creazione ai giorni d'oggi, la compravendita di informazioni di account, conti bancari e numeri di carte di credito rubate. Dati personali e bancari sono spesso la seconda o la terza categoria di “materie prime” elencate nei mercati oscuri ed uno dei prodotti più comuni posti in evidenza dalle forze dell'ordine<sup>223</sup>.

#### 3.1.2.4 Armi

La disponibilità di armi da fuoco ed esplosivi sui mercati *Darknet* rimane una preoccupazione chiave per le forze dell'ordine. Mentre tipicamente è una delle merci meno comuni trovate sui *darkmarkets*, è quella che rappresenta il più grande potenziale di pericolo per la sicurezza pubblica<sup>224</sup>. Nei grandi cripto-mercati il numero degli annunci supera i 60000, mentre in altre homepage presenti in rete non è presente la categoria “armi da fuoco” e per trovarne si deve cliccare o sulla categoria “altri prodotti” oppure sui forum dove si indicano gli URL dei *vendor shop*, ovvero dei negozi specializzati nella vendita di armi ed esplosivi<sup>225</sup>. A giugno 2018, il Berlusconi Market<sup>226</sup> ha oltre 700 elenchi nella categoria delle "armi", tra cui munizioni, pistole, fucili di precisione a lunga gittata, esplosivi e armi bianche<sup>227</sup>. Da numerosi studi si riscontra come generalmente la vendita di pistole sia la più numerosa seguita successivamente da fucili e mitragliatrici<sup>228</sup>. Unite a questi vengono vendute munizioni, coltelli, attrezzature per ordigni e prodotti digitali per il supporto, come eBook che forniscono istruzioni per la fabbricazione e l'assemblaggio di esplosivi e armi<sup>229</sup>.

#### 3.1.2.5 Malware

Altro tipo di armi, particolarmente di moda nell'era del digitale, vendute nelle reti oscure sono i *malware*: programmi maligni che vanno da semplici software di registrazione di frequenze per

---

<sup>222</sup> Zaklina Spalevic, Milos Ilic, *The Use of Dark Web for the purpose of illegal activity spending* 2017.

<sup>223</sup> Europol, IOCTA 2018.

<sup>224</sup> Ibid.

<sup>225</sup> Ibid. Giacomo Persi Paoli 2017.

<sup>226</sup> Un mercato italiano innominato come l'ex presidente del consiglio italiano, gestito dal proprietario e fondatore con nickname “Angelino Alfano”. (da [www.darkweb.com](http://www.darkweb.com))

<sup>227</sup> Europol, IOCTA 2018.

<sup>228</sup> Ibid.

<sup>229</sup> Ibid.

rubare all'utente dati sensibili, a sofisticati e professionali *software* che possono intercettare, alterare o dirottare i dati della vittima<sup>230</sup>. Le ricerche sul tema evidenziano la distribuzione di questi strumenti digitali in crescita, tra i maggiori più venduti ci sono i *ransomware*<sup>231</sup>, programma che disabilita il dispositivo di una vittima fino a che non viene pagato un riscatto che libera il sistema dal blocco. Oltre a questi troviamo la distribuzione di Trojan o virus come gli *exploit e botnet*<sup>232</sup> in grado portare attacchi Dos o i correlati DDoS, particolarmente dannosi<sup>233</sup>. L'insieme di questi strumenti nella società odierna rappresenta un enorme pericolo. Ogni istituto bancario, azienda o amministrazione pubblica utilizza sistemi computerizzati che possono essere un facile bersaglio da parte di malintenzionati intenti nel bloccare un sistema ai fini non solo di estorcere informazioni sensibili ma di destabilizzare intere strutture informatiche dedite all'erogazione di servizi essenziali<sup>234</sup>.

### 3.2 Gli altri illeciti nelle darknet

Un'altra attività in crescita, specialmente negli ultimi cinque anni, è l'industria del gioco d'azzardo online che stima nel 2017 una valutazione di mercato pari a 49,64 miliardi di dollari americani<sup>235</sup>. Questa crescita, dovuta anche allo spropositato aumento degli strumenti digitali come smartphones e tablets, è stata notata dai governi in tutto il mondo che nell'arco del tempo hanno cominciato a limitarne le imprese che investivano in questo settore, dal restringere il rilascio delle licenze al circoscrivere i pagamenti<sup>236</sup>. Dalla Russia alla Cina fino alla Turchia il gioco d'azzardo online è totalmente illegale, mentre nei Paesi Bassi e in Polonia è permesso solo ai portali d'origine e licenza nazionale, mentre ancora in Francia e nel Regno Unito, specialmente negli ultimi anni, le pratiche del gioco d'azzardo online sono pesantemente regolate. Il dipartimento di giustizia degli Stati Uniti

---

<sup>230</sup> Europl, IOCTA 2014.

<sup>231</sup> Roderic G. Broadhurst, *Malware Trends on 'Darknet' Crypto-markets: Research Review* 2018.

<sup>232</sup> Si veda Capitolo II, sotto-par. Mano Guida.

<sup>233</sup> Si veda Capitolo II.

<sup>234</sup> In riferimento agli "Operatori di servizi essenziali" (Ose), ovvero chi fornisce servizi chiave per la vita del Paese, per ciascuno dei settori previsti: energia, trasporti, bancario, infrastrutture dei mercati finanziari, sanitario, fornitura e distribuzione di acqua potabile e infrastrutture digitali.

<sup>235</sup> Sinyong Choi, *Illegal Gambling and Its Operation via the Darknet and Bitcoin: An Application of Routine Activity Theory*, 2018.

<sup>236</sup> Un riferimento in particolare alla legislazione americana che già dal 2006 ha cominciato a limitare il gioco d'azzardo online con Unlawful Internet Gambling Enforcement Act, che si può consultare alla pagina riportata nel seguente link: <https://www.govinfo.gov/content/pkg/STATUTE-120/pdf/STATUTE-120-Pg1884.pdf>

ha dichiarato nelle prime settimane del 2019 che, ai sensi dello *U.S.Wire Act*<sup>237</sup>, tutti i giochi d'azzardo su Internet che comportano transazioni interstatali non siano più permesse<sup>238</sup>.

Tale tendenza proibizionista ha fatto sì che, dopo la nascita del bitcoin e delle reti *.onion*, molte pagine di gioco d'azzardo si spostassero nelle reti oscure, rendendo le transazioni più semplici e scevre dalle leggi imposte<sup>239</sup>. Nonostante la maggior parte degli illeciti riguardanti quest'ambito è ancora forte nella parte in superficie del web nelle quali, il gioco d'azzardo online, con l'uso di cripto valute, viene sfruttato per scopi di riciclaggio di denaro<sup>240</sup>, oggi le Darknet ospitano casino, siti di poker online e centri scommesse che usano i sistemi più conosciuti di cripto-valute, dal Bitcoin ad Ethereum fino a Monero e Zcash, per eseguire le proprie transazioni. Il sistema di gioco d'azzardo sotterraneo è apparso agli occhi del pubblico internazionale con la chiusura, da parte delle autorità cinesi, nel 2018 di un giro di scommesse nel dark web, relative alla coppa del mondo, pari a 1,5 miliardi di dollari americani<sup>241</sup>. Dalle dichiarazioni provenienti dalle indagini appare che durante gli otto mesi di esistenza della piattaforma di gioco, questa abbia visto la registrazione di centinaia di migliaia di utenti, creando un giro di scommesse controllato da un gruppo criminale vasto e ben organizzato<sup>242</sup>.

Tra gli ambiti pesantemente regolamentati nelle *clearnet* c'è la pedopornografia online che in maniera ben più ingente del gioco d'azzardo è dilagata nelle reti oscure.

Nel 2017 l'Internet Watch Foundation (IWF), un'organizzazione no-profit con sede nel Regno Unito che lavora per ridurre al minimo la quantità di materiale pedopornografico online, ha dichiarato un aumento del 57% dei nomi di dominio<sup>243</sup> che ospitano tali materiali e un aumento dell'86% dell'uso di siti presenti nel web oscuro<sup>244</sup>. Lo sfruttamento sessuale dei minori online non è un fenomeno tipico della criminalità organizzata nel senso tradizionale del termine. I trasgressori sono spesso attori solitari e il coinvolgimento delle mafie è scarso se non nullo<sup>245</sup>. Tuttavia, nell'arco degli ultimi anni, sono venute alla luce delle vere e proprie forme organizzative<sup>246</sup>. Nel

---

<sup>237</sup> Legge risalente al 1961, che vietava il gioco d'azzardo sportivo è stata reinterpretata dal Dipartimento di Giustizia. La legge originale può essere consultata al sito: <https://www.govinfo.gov/content/pkg/STATUTE-75/pdf/STATUTE-75-Pg491.pdf>

<sup>238</sup> Si veda il link: <https://www.bloomberg.com/news/articles/2019-01-15/u-s-now-says-all-online-gambling-illegal-not-just-sports-bets>

<sup>239</sup> Ibid. Choi.

<sup>240</sup> Fiedler Ingo, *Online Gambling as a Game Changer to Money Laundering?* 2013.

<sup>241</sup> Si veda il link: <https://www.digitaltrends.com/cool-tech/china-world-cup-gambling-ring/>

<sup>242</sup> Ibid.

<sup>243</sup> Un nome di dominio, in informatica, è costituito da una serie di stringhe separate da punti, che identifica il dominio dell'autonomia amministrativa, dell'autorità o del controllo all'interno di internet. I nomi di dominio sono formati dalle regole e dalle procedure del Domain Name System (DNS). Qualsiasi nome registrato nel DNS (ad esempio it.wikipedia.org) è un nome di dominio. Essi vengono utilizzati in diversi contesti di rete e in ambito specifico per la denominazione o l'indirizzamento.

<sup>244</sup> Internet Watch Foundation, *Annual Report 2017*, 2017, pp. 5.

<sup>245</sup> Europol, IOCTA 2018.

<sup>246</sup> Ibid.

maggio 2018, l'operazione SKY, guidata dalla polizia nazionale spagnola e sostenuta da Europol, ha portato all'arresto di otto sospetti in Canada, Francia, Ungheria, Italia e Spagna. La complessa indagine ha preso di mira un gruppo coinvolto nella distribuzione di materiale di sfruttamento sessuale dei bambini attraverso piattaforme *Darknet* e Skype. L'indagine si è concentrata dapprima sulla rete TOR, ma in seguito gli investigatori hanno scoperto i collegamenti per deviare gli utenti verso un gruppo privato accessibile solo su invito su Skype<sup>247</sup>. Un altro esempio è del luglio del 2018, nel quale le forze di polizia bulgare hanno arrestato otto sospetti coinvolti nella diffusione di pornografia minorile. I criminali in questione hanno usato bitcoin per pagare l'hosting di un sito web creato appositamente per caricare foto e video di abusi sessuali su minori<sup>248</sup>. L'insieme di documenti d'indagine delle forze dell'ordine europee dello scorso anno hanno dimostrato la presenza, nei mercati online delle *darknet*, di materiale pedopornografico, proveniente da mercati dell'Est Europa o russi.

L'uso delle tecnologie come reti VPN e TOR, hanno reso agevole a tutti in maniera semplice l'accesso al mondo dell'anonimato, criptando comunicazioni e transazioni tra individui. Questo ha fatto sì che piccole e grandi entità criminali usassero questi mezzi per delinquere in molteplici ambiti. Il crimine attraverso diversi metodi ha trovato nuovi mezzi per dare ai propri proventi illeciti una parvenza di legalità attraverso nuovi sistemi di riciclaggio di denaro.

### 3.3 Il Cybericiclaggio

Milioni di transazioni avvengono quotidianamente su Internet e le organizzazioni criminali da più di due decenni ne approfittano per riciclare fondi acquisiti illegalmente tramite transazioni online segrete e anonime<sup>249</sup>.

Molte delle nuove caratteristiche di Internet si prestano ai bisogni dei criminali che operano a livello internazionale in particolare: l'anonimato delle varie parti della transazione, la rapidità dei collegamenti in rete, la connessione, se pure virtuale, fra gli individui attivi nell'operazione, che gli dà modo di trovarsi in punti opposti del pianeta. A differenza dei metodi "tradizionali" di riciclaggio di denaro, che si basano sul sistema bancario, il cybericiclaggio dipende dall'uso di vari tipi di transazioni e fornitori di servizi finanziari, che vanno dai bonifici bancari, al deposito/prelievo di

---

<sup>247</sup> Europol, Eight arrested for distribution of child sexual abuse material through Skype and the darknet, Si veda il link: [www.europol.europa.eu/newsroom/news/eight-arrested-for-distribution-of-child-sexual-abuse-material-through-skype-and-darknet](http://www.europol.europa.eu/newsroom/news/eight-arrested-for-distribution-of-child-sexual-abuse-material-through-skype-and-darknet), 2018.

<sup>248</sup> Europol, IOCTA, 2018.

<sup>249</sup> Jean-Loup Richet, *Laundering Money Online: a review of cybercriminals' methods*, 2013.

contante fino a alle transazioni di moneta elettronica e cripto-valuta<sup>250</sup>. Il cybericiclaggio è oggi una minaccia gravissima per la sicurezza delle transazioni monetarie telematiche se si considera il fatto che esse sono sempre più difficili da individuare in Internet, a causa della frammentazione degli scambi e della molteplicità degli itinerari percorsi dal denaro veicolato.

Secondo l'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine, i flussi di denaro riciclato ogni anno oscillano tra il 2% e il 5% del Pil globale, quasi duemila miliardi di dollari<sup>251</sup>. In Italia tali flussi corrispondono al 10% del Pil<sup>252</sup>.

La maggior parte di queste operazioni, se non quasi la totalità, sfruttano i sistemi computerizzati per realizzarsi<sup>253</sup>.

Ulteriore rivoluzione che ha dato una spinta incisiva verso il processo di digitalizzazione del riciclaggio di denaro è stata l'introduzione delle monete virtuali prima e delle cripto-valute dopo. Nell'ultimo anno in Italia sono stati evidenziati diversi casi, che hanno coinvolto associazioni per delinquere, nel riciclaggio di denaro con l'uso delle monete virtuali<sup>254</sup>.

Inoltre, molte delle tecniche utilizzate per ripulire i proventi illeciti online sono discusse all'interno dei forum delle Darknet mettendo in collaborazione diversi metodi utilizzati da più entità criminali<sup>255</sup>.

Per capire come tale fenomeno oggi sia in crescita è essenziale indagare come funzioni il riciclaggio al di fuori di internet e come si sia sviluppato nella rete grazie alla nascita di nuove tecnologie.

### 3.3.1 Il riciclaggio di denaro: verso nuove frontiere

“Il riciclaggio di denaro è il processo attraverso il quale vengono sostituiti, trasferiti o occultati tramite varie operazioni proventi o altre utilità provenienti da delitto non colposo, in modo da ostacolare l'identificazione della provenienza illecita”<sup>256</sup>. Nonostante le pratiche di legittimazione di fondi illegali esistano da tempo nella prassi di gruppi criminali, il termine riciclaggio di denaro entra nella terminologia giuridica tra il 1973/74, dopo lo scandalo Watergate<sup>257</sup>.

---

<sup>250</sup> Eurasian Group on Combating *Money Laundering and Financing of Terrorism, Cybercrime and Money Laundering* 2014.

<sup>251</sup> UNODC, *The Global Programme against Money Laundering, Proceeds of Crime and the Financing of Terrorism 2011-2017*. Si veda inoltre il link: <https://www.unodc.org/unodc/en/money-laundering/globalization.html>

<sup>252</sup> Si veda il link: [https://www.corriere.it/economia/11\\_maggio\\_10/bankitalia-riciclaggio-tarantola\\_93891902-7b24-11e0-be08-e42815e8b082.shtml](https://www.corriere.it/economia/11_maggio_10/bankitalia-riciclaggio-tarantola_93891902-7b24-11e0-be08-e42815e8b082.shtml)

<sup>253</sup> Financial Action Task Force. FATF Report, 2014.

<sup>254</sup> UIF, *Quaderni dell'antiriciclaggio, Casistiche di riciclaggio e di finanziamento del terrorismo*, 2018.

<sup>255</sup> Max Goncharov Trend Micro, *Russian Underground 2.0*, 2015.

<sup>256</sup> Razzante Ranieri, *par. 4.2 il riciclaggio di denaro, reale e/o virtuale, p.64*. Bitcoin e Criptovalute profili fiscali, giuridici e finanziari, 2018

<sup>257</sup> Shams Heba, *Legal Globalization: Money Laundering Law and Other Cases, International Financial Law Series*, 2004.

In accordo con il report annuale del Gruppo di Azione Finanziaria Internazionale (GAFI)<sup>258</sup>, sebbene ci siano molti modi per cui le organizzazioni criminali riciclino denaro, la maggior parte delle tipiche operazioni di riciclaggio seguono uno schema tripartito ben preciso: collocamento, stratificazione e integrazione<sup>259</sup>.

La prima fase di **collocamento o posizionamento** si esplicita nel momento in cui il riciclatore inserisce i proventi illeciti nel sistema finanziario depositando il denaro in una banca o nell'economia al dettaglio attraverso l'acquisto di beni di valore elevato, proprietà o beni aziendali<sup>260</sup>, che possono essere successivamente rivenduti sotto forma di bonifici o assegni bancari. È in questa fase che le autorità possono avere le migliori possibilità di catturare il riciclatore<sup>261</sup>. Proprio per evitare che questo accada i criminali effettuano versamenti o operazioni di cambio regolari ripetute al disotto delle soglie fissate per l'identificazione. Questa operazione chiamata *smurfing* tenta di evitare qualsiasi tipo di monitoraggio, dividendo una grande somma di denaro in tanti pezzi in modo da non apparire sospetta all'occhio delle autorità. Ovviamente tali operazioni possono essere favorite da banche, intermediari finanziari, commercianti o professionisti<sup>262</sup>. Dopo aver collocato i fondi in un'istituzione legittima, il riciclatore tenterà di nascondere la fonte e la proprietà dei fondi attraverso **il processo di stratificazione**<sup>263</sup> nel quale creerà complesse transazioni finanziarie, come i bonifici internazionali o il collocamento di fondi in una banca offshore, effettuando numerosi trasferimenti da un conto all'altro nel tentativo di allontanare i proventi dalla loro origine criminale e confondere chiunque cerchi di tracciare la pista del denaro. Dato il gran numero di transazioni effettuate ogni giorno, è improbabile che le autorità riescano ad intercettare il segnale a questo stadio.

Nell'ultima fase nota come **integrazione**, il riciclatore reintroduce, ovvero reintegra, i fondi nell'economia legittima<sup>264</sup>. Le organizzazioni criminali impegnate nel riciclaggio solitamente istituiscono società anonime fittizie, investendo nel settore immobiliare, o si cimenteranno in qualsiasi altra pratica che porterà alla legittimità dei fondi<sup>265</sup>. Le attività commerciali che fanno un grande volume di vendite in contanti sono adatte per questo scopo, proprio per la minore tracciabilità del contante. Esempi di tali attività variano ampiamente includendo casino, centri

---

<sup>258</sup> Si veda il link: [https://italiarapparigi.esteri.it/rapp\\_ocse/it/ocse/enti-con-segretariati-preso-l/fatf](https://italiarapparigi.esteri.it/rapp_ocse/it/ocse/enti-con-segretariati-preso-l/fatf)

<sup>259</sup> Financial Action Task Force, *Report on Money Laundering Typologies 2000–2001* 19 (February 1, 2001), si veda inoltre See Nicholas Clark. *The Impact of Recent Money Laundering Legislation On Financial Intermediaries*, 14 DICK. J. INT'L L. 467, 469 (1996); si veda anche Fletcher N. Baldwin, Jr., *Money Laundering and Wire Transfers: When the New Regulations Take Effect Will They Help?*, 1996).

<sup>260</sup> Angela Veng Mei Leong, *Chasing dirty money: domestic and international measures against money laundering*, *Journal of Money Laundering Control*, 2007.

<sup>261</sup> Ibid.

<sup>262</sup> A. Stile, *Riciclaggio e reimpiego di proventi illeciti*, 2009.

<sup>263</sup> Ibid. Leong.

<sup>264</sup> Ibid.

<sup>265</sup> Ibid.

scommesse, club, ristoranti, distributori di benzina, negozi di noleggio auto, parcheggi e altri percorsi di vendita costituendo condizione di sviluppo delle economie criminali<sup>266</sup>. Oltre che con lo scopo di nascondere i proventi illeciti quindi, le organizzazioni criminali investono nell'economia legale con l'intento di allargare il proprio capitale mentendo allo stesso tempo il controllo territoriale<sup>267</sup>. Anche in quest'ultima fase, nonostante il capitale risieda al sicuro<sup>268</sup>, la criminalità deve far sì che gli investimenti appaiano ordinari, sfruttando così i sistemi di globalizzazione finanziaria odierni. Tali operazioni a livello internazionale possono partire dai paradisi fiscali e passare per più istituti finanziari sparsi nel mondo attraverso molteplici fidejussioni, così da confondere maggiormente le autorità, finendo poi in un determinato investimento che rappresenti la definitiva "purificazione" del guadagno illecito.

Quest'insieme di passaggi, oggi parte integrante dei sistemi di riciclaggio, non sarebbero possibili senza l'uso delle tecnologie di rete che permettono trasferimenti di grandi quantità di denaro da una parte all'altra del mondo.

Possiamo affermare che il crimine organizzato impegnato nel riciclaggio di proventi illeciti oggi è avvantaggiato da tre motivi principali:

I sistemi informatici e i nuovi mezzi elettronici hanno contribuito a favorire l'evoluzione del *money transfer*, esigenza imprescindibile di tutti i tipi di traffico mercantile<sup>269</sup>. L'evoluzione delle tecnologie di rete ha offerto numerose modalità attraverso le quali il crimine possa trasferire, ritirare, depositare o occultare i propri guadagni. La diffusione dell'utilizzo dell'*e-cash* va di pari passo con lo sviluppo dell'*home banking* e del *trading on line*, i quali strumenti hanno fatto sì che i tradizionali sportelli diventassero alla portata di tutti, tramite computer, smartphone e app, consentendo ad operatori non bancari di immettere denaro nel circuito creditizio, di effettuare pagamenti e di muovere ingenti somme di capitali<sup>270</sup>. L'*internet banking* ha rivoluzionato il vecchio sistema bancario permettendo di trasferire grandi somme di denaro con un solo clic senza il coinvolgimento di alcuna interazione tra persone. Metodi che consentono di sfruttare i vantaggi dell'elettronica sono l'uso di carte prepagate o *smart cards*, nelle quali l'utente può immagazzinare grandi quantità di denaro e svolgere trasferimenti online grazie ai servizi di pagamento digitale<sup>271</sup>. Oltre all'uso delle carte di credito/prepagate ci sono molti altri servizi di pagamento online disponibili su Internet che, come abbiamo avuto modo di affrontare nel primo capitolo, sono noti

---

<sup>266</sup> L. Fornari, *Criminalità del profitto e tecniche sanzionatorie* 1997.

<sup>267</sup> Transcrimine, *Primo rapporto nazionale sulla mafia – Progetto PON Sicurezza 2007 – 2013*.

Gli investimenti delle mafie, in [www.investimentioc.it](http://www.investimentioc.it), 2013.

<sup>268</sup> Come ad esempio in un conto offshore.

<sup>269</sup> Palana Maurizio *Il riciclaggio nell'ambito dell'attività degli "Agenti Money Transfer"*, 2008.

<sup>270</sup> U. Rapetto, *Cyberlaundering – il riciclaggio del terzo millennio*, citazione disponibile su: <http://gnosis.aisi.gov.it/sito%5CRivista14.nsf/servnavig/6>

<sup>271</sup> Come può essere Paypal.

come denaro digitale, denaro elettronico e, dal 2009, un sistema di pagamento decentralizzato come quello permesso dalle cripto-valute. Con l'introduzione delle cripto-valute le organizzazioni criminali hanno trovato un ulteriore modo per commettere riciclaggio in maniera efficiente<sup>272</sup>, avendo la possibilità di trasferire ingenti somme di denaro in pochi secondi da una parte all'altra del mondo in maniera anonima e senza passare per alcun istituto centralizzato.

### 3.3.2 Il nesso con le cripto-valute

Passare per le tre fasi del riciclaggio attraverso l'uso dello pseudo-anonimato che le cripto-valute offrono, può permettere ai criminali di trarne vantaggio senza dover preoccuparsi inoltre di passare per sistemi centralizzati come quelli bancari.

Il bilanciamento tra trasparenza delle transazioni e anonimato dell'utente è al centro del dibattito sull'uso criminoso delle cripto-valute. I singoli indirizzi degli utenti che scambiano cripto-valute non possono essere legati in alcun modo alle identità individuali nel mondo reale grazie al complesso sistema crittografico che vi è alla base, come il rapporto che intercorre tra chiave pubblica e chiave privata. Tuttavia, i registri delle singole transazioni vengono trasmessi sul "libro pubblico distribuito", ovvero la *blockchain*, che in particolare nel caso dei bitcoin registra tutte le transazioni effettuate all'incirca ogni dieci minuti e le raggruppa nei "blocchi della catena". Per questo le cripto-valute più utilizzate, ad eccezione di Monero e Z-cash, vengono definite come quasi anonime, essendo il loro percorso tracciabile ma il destinatario sconosciuto<sup>273</sup>. Nonostante tutto già il requisito della quasi anonimità basta alle organizzazioni criminali a scampare dalle operazioni di antiriciclaggio globale<sup>274</sup>. L'anonimato dell'utente rende vano il processo di *know your customer*<sup>275</sup>, requisito essenziale che banche e altri istituti finanziari utilizzano per valutare i potenziali rischi che possono nascondersi dietro un cliente. Specialmente nelle transazioni iniziali le forze dell'ordine e di antiriciclaggio cercano di sfruttare questo fattore per identificare il riciclatore o gli eventuali concorrenti. L'affidarsi ad istituzioni finanziarie centralizzate con l'arrivo delle cripto-valute, basate su un sistema altamente decentralizzato, si è rivelato inadatto alle nuove tecnologie che hanno sconvolto tecniche e regolamenti antiriciclaggio sviluppati negli ultimi decenni<sup>276</sup>. Le cripto-valute aumentano le sfide dell'antiriciclaggio essendo molto difficile, se non impossibile, come afferma il presidente di *Deloitte US Anti-Money Laundering* (AML), Fred Curry, che i professionisti possano

---

<sup>272</sup> Sarah N. Welling, Andy G. Rickman, *Cyberlaundering: The Risks, the Responses*, 1998.

<sup>273</sup> Si veda Capitolo I.

<sup>274</sup> Campbell-Verduyn, Malcolm. *Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance*. Crime, Law and Social Change 2017.

<sup>275</sup> In italiano: conosci il tuo cliente.

<sup>276</sup> Stokes, R. *Anti-Money Laundering Regulation and Emerging Payment Technologies*. *Banking & Financial Services Policy Report* 2013.

monitorare le transazioni senza conoscere chi sono le parti<sup>277</sup>. Questo insieme di caratteristiche rendono le cripto-valute un mezzo efficace per “pulire” il denaro dallo “sporco” delle attività illecite<sup>278</sup>.

Ritornando a questo punto allo schema tripartito del riciclaggio: nella **fase di collocamento** i criminali possono depositare denaro contante e scambiarlo con cripto-valute attraverso i servizi di *LocalBitcoin Exchanges*<sup>279</sup>, pronti ad accettare grandi quantità di capitale attraverso il deposito del contante presso l’account del venditore (operazione che non richiede alcun rilascio di identità personale). In alternativa i criminali potrebbero direttamente eseguire transazioni di cripto-valute già in loro possesso, acquisite in rete da clienti o consumatori disposti a pagare in moneta virtuale per l’acquisizione di beni e servizi. Un esempio in questo senso è rappresentato dalle organizzazioni criminali impegnate nella vendita di droga nelle *darknet* che, attraverso l’uso dei *darkmarkets*, richiedono cripto-valuta al fine di nascondere l’identità delle parti<sup>280</sup>. Dai numerosi casi che riscontrano il legame tra riciclaggio e cripto-valute si osserva come solo una piccola parte siano esenti dal legame con il traffico di droga in rete<sup>281</sup>. **Nella fase di stratificazione**, i criminali potrebbero dare vita a diversi account di cripto-valuta, dividendo l’ammontare originale in tante piccole parti che comunicano tra loro, confondendo la tracciabilità delle transazioni e bypassando il problema della blockchain. Questo spostamento da un account all’altro, unito al mantenimento dell’anonimato, va definitivamente a cancellare le prove della provenienza illecita del denaro. Tali operazioni vengono eseguite dalla figura del *money mule*<sup>282</sup>, ovvero persone che, spesso senza saperlo, sono state reclutate come intermediari di riciclaggio di denaro per conto di organizzazioni criminali<sup>283</sup>. Il “mulo” ha il compito infatti di trasferire somme di denaro ricevute a terzi e, sull’importo trasferito riceve una percentuale<sup>284</sup>. Le organizzazioni criminali, al fine di reclutare nuovi *mules*, utilizzano spesso annunci di lavoro fasulli o creano post sui social media con la promessa di ottenere soldi in maniera facile e veloce<sup>285</sup>. Nonostante le persone coinvolte non siano consapevoli che il denaro trasferito possa essere il frutto di un illecito, queste svolgono comunque

---

<sup>277</sup> Rubinfeld, S. *FATF Pushes Risk-Based Approach Toward Virtual Currencies, Services*. Wall Street Journal, 2 luglio 2015.

<sup>278</sup> Christopher, C.M. *Wack-a-mole: Why prosecuting digital currency exchanges won't stop online money laundering*. Lewis and Clarke Review, 2014.

<sup>279</sup> Si veda il link: <https://www.buybitcoinworldwide.com/en/buy-bitcoins-with-cash/>

<sup>280</sup> Sarah Durrant, *Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations*, City University of New York CUNY Academic Works, 2018.

<sup>281</sup> Ibid.

<sup>282</sup> Money mule è il termine inglese utilizzato ufficialmente in materia per descrivere i corrieri (ovvero i muli) di denaro delle organizzazioni criminali.

<sup>283</sup> Europol, Money Muling, si veda il link: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/money-muling>

<sup>284</sup> Feola Raffaella, *Il reato di "money muling" Analisi del fenomeno legato al crimine informatico*, 21/09/2017, disponibile sul seguente link: <https://www.studiocataldi.it/articoli/27498-il-reato-di-quotmoney-muling-quot.asp>

<sup>285</sup> Ibid, Europol, Money Muling.

un ruolo cruciale nel processo di riciclaggio, diventando soggetti imputabili dal punto di vista penale<sup>286</sup>. Altra tecnica per “ripulire” le cripto-valute può essere quella di scambiarle un certo numero di volte attraverso vari mercati online<sup>287</sup>. Ogni volta che un utente scambia cripto-valuta con un altro, “salta” tra gli indirizzi di *wallet* diversi, aggiungendo gradi di crittografia e quindi aumentando lo stato di privacy della transazione.

Infine, nella fase di integrazione, i riciclatori potrebbero mantenere i loro guadagni illeciti in cripto-valute per investire in future transazioni, come nel caso della creazione di siti o compagnie di facciata online. Una delle possibilità utilizzate in rete è la creazione di società di e-commerce, siano esse vere o false o che possano offrire servizi o commerciare beni in maniera fraudolenta e non<sup>288</sup>.

Altro metodo molto utilizzato è quello di aprire, acquistando in cripto-valuta, un sito legittimo di gioco d'azzardo online trasferendo i fondi utilizzando una falsa identità o un prestanome. Una volta investito il denaro, qualsiasi ricavato del nuovo sito di gioco d'azzardo apparirebbe totalmente legittimo alle autorità<sup>289</sup>.

In alternativa, una delle pratiche più diffuse tra i criminali in rete in questa fase è quella di “incassare”<sup>290</sup>, molte volte tornando presso i servizi dove originariamente avevano scambiato contante per cripto-valuta, facendo il contrario in cambio di qualsiasi valuta esistente. In altri casi i riciclatori di denaro si rivolgono ai mercati *peer-to-peer* nelle *darknet* per trasformare le proprie cripto-valute in contanti<sup>291</sup>.

La convergenza di diversi campi come il gioco d'azzardo online e cripto-valute; le comunicazioni anonime in rete e i forum criptati; il mondo dell'e-commerce e i pagamenti elettronici; i servizi di telecomunicazione e quelli bancari rende l'ecosistema estremamente complicato in termini di regolamentazione e controllo.

### 3.3.2.1 Il caso riportato dalla UIF

Ai fini di questo lavoro è interessante menzionare un caso, riportato dall'Unità di Informazione Finanziaria della Banca d'Italia, di raccolta di fondi illeciti e successivo investimento in valute virtuali<sup>292</sup>. Il caso interessa una rete di soggetti, “punto di raccolta di fondi provenienti da varie zone

---

<sup>286</sup> Ibid.

<sup>287</sup> Si veda il link: <https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2/>

<sup>288</sup> Weaver, S.: *Modern day money laundering: does the solution exist in an expansive system of monitoring and record keeping regulations?* Annu. Rev. Bank. Law Financ. Law 24, 443–465 (2005).

<sup>289</sup> Ibid.

<sup>290</sup> Ibid. Durrant 2018.

<sup>291</sup> Si veda il link: <https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2/>

<sup>292</sup> UIF, *caso n. 6*, p. 33/34, Quaderni dell'antiriciclaggio, Casistiche di riciclaggio e di finanziamento del terrorismo, 2018, si veda il link: [https://uif.bancaditalia.it/pubblicazioni/quaderni/2018/quaderni-11-2018/Quaderno\\_11\\_luglio\\_2018.pdf](https://uif.bancaditalia.it/pubblicazioni/quaderni/2018/quaderni-11-2018/Quaderno_11_luglio_2018.pdf)

del territorio nazionale con la finalità di trasferire le somme ricevute verso piattaforme di scambio e di investimento di valute virtuali”<sup>293</sup>.

Tale gruppo di persone riceveva delle ricariche su conti prepagati, attestati ai singoli membri del gruppo, per poi inviare dei bonifici esteri a favore di determinate società “operanti come piattaforme di investimento e compravendita di valute virtuali con rapporti bancari incardinati in vari Stati esteri, alcuni off-shore, anche diversi da quelli in cui risultavano localizzate le rispettive sedi legali”<sup>294</sup>.

Le ricerche su le persone che si celavano dietro alle ricariche, ha portato a conoscenza dell’Ufficio, che tra questi vi erano “nominativi indagati o condannati per traffico di stupefacenti e affiliazione ad associazioni mafiose” ed altri ancora già segnalati alla UIF “per l’utilizzo di fondi derivanti da frodi informatiche (c.d. phishing)”<sup>295</sup>.

Le indagini hanno portato al risultato che il gruppo che riceveva le ricariche “agiva come punto di raccolta di fondi provenienti da diversi comuni del territorio nazionale con lo scopo di inviare le somme stesse verso piattaforme di scambio e di investimento di valute virtuali”. Inoltre, dalle ricerche approfondite sui portali di rete e sulle piattaforme di discussione riguardante lo scambio di cripto-valuta, si è rivelato che i soggetti interessati offrivano servizi di *exchange* su queste pagine.

L’autorità giudiziaria ha rivelato che uno di questi *exchanger* era anche coinvolto “in reati di falsificazione di documenti di identità e riciclaggio di denaro proveniente da traffico di sostanze stupefacenti, con conversione in euro della valuta digitale Bitcoin (...). Le relative risorse finanziarie sono state sottoposte a provvedimento di sequestro preventivo”<sup>296</sup>.

---

<sup>293</sup> Ibid.

<sup>294</sup> Ibid.

<sup>295</sup> Ibid.

<sup>296</sup> Ibid.

## Capitolo IV- Aspetti di regolamentazione e controllo

### 4.1 Approccio penalistico alle sfide del Crimine Informatico

La criminalità informatica solleva numerose sfide per il diritto penale tradizionale e per i sistemi di giustizia criminale in tutto il mondo. La prima sfida riguarda la sua definizione<sup>297</sup>. Nel momento in cui si parla di crimine informatico o *cybercrime*, si fa riferimento ad un insieme di reati<sup>298</sup>. Si possono dividere questo insieme di reati in tre macro-categorie<sup>299</sup>:

- Nel momento in cui si usi il computer come obiettivo (ad es. accesso abusivo ad un computer al fine di raccogliere o eliminare dati<sup>300</sup>, disseminazione di virus e malware per bloccare il sistema o altre funzioni di hacking).
- Nel momento in cui si usi il computer come mezzo o strumento usato per commettere una qualsivoglia condotta criminale (ad es. i diversi tipi di frode telematica<sup>301</sup> o molestie online).
- Nel momento in cui si usi il computer come accessorio per il crimine, ovvero tutte quell'insieme di attività che sarebbero state compiute ugualmente ma che possono essere aidate dall'uso del computer (ad es. pedopornografia, riciclaggio di denaro o il commercio online<sup>302</sup>).

Una seconda sfida è rappresentata dalla complessità delle tecnologie dell'informazione e della comunicazione (ICT) spesso non alla portata di tutti e non familiari al tradizionale mondo della giustizia criminale. Dal momento che le ICT costituiscono un settore in rapida crescita e in evoluzione, gli operatori devono costantemente riquilibrare il settore richiedono personale ben addestrato alle nuove tecniche, nella fase di indagine, durante il procedimento penale e nei tribunali<sup>303</sup>.

---

<sup>297</sup> McQuade III, Samuel C. *Understanding and Managing Cybercrime*. 2006,

<sup>298</sup> Pubblicazione del Consiglio D'Europa, 2005. *Organised Crime in Europe: The Threat of Cybercrime., Situation Report 2004*.

<sup>299</sup> Tafazzoli, *Cyber Crime Legislation, ICT Research Institute*, maggio 2018, si veda il link: [www.itrc.ac.ir](http://www.itrc.ac.ir)

<sup>300</sup> Come ad esempio Dos o DDoS.

<sup>301</sup> Come possono essere il carding, il phishing ecc..

<sup>302</sup> Si veda il link: <https://www.coursehero.com/file/p7q2k3c/The-computer-as-incidental-to-the-crime-becomes-a-crime-when-the-computer/> oppure <http://riverdelfin.blogspot.com/2013/07/types-of-computer-crimes.html>

<sup>303</sup> Chaikin, David.. *Network investigations of cyber-attacks: The limits of digital evidence*.

La terza sfida è rappresentata dalla natura virtuale dei crimini informatici caratteristica che spesso si scontra con i principali criteri operativi dei sistemi di giustizia penale, in particolare sovranità e il principio di territorialità. Tale natura richiede che non solo le singole istituzioni nazionali si rendano operative ma anche gli altri paesi a livello regionale e internazionale stabiliscano regole chiare sulla giurisdizione di un sistema giuridico riguardante questi reati<sup>304</sup>. Di conseguenza, c'è un forte bisogno di chiarezza di norme che stabiliscano le priorità e le competenze di ciascun paese coinvolto. Si deve considerare inoltre le difficoltà legate alla velocità attraverso la quale molti di questi crimini vengono commessi. I crimini informatici si verificano in una frazione di secondo e possono diffondersi con sorprendente velocità<sup>305</sup>. Le prove della criminalità informatica sono spesso costituite da informazioni digitali, che sono effimere per natura e possono essere modificate o cancellate<sup>306</sup>. Le forze dell'ordine e le agenzie di sicurezza devono quindi agire rapidamente e essere in grado di raccogliere e conservare le prove digitali per utilizzarle nei procedimenti penali.

Al fine di affrontare efficacemente i problemi relativi alla repressione della criminalità informatica, i diversi sistemi nazionali di giustizia criminale devono aggiornare la loro legislazione e i sistemi di applicazione della legge nel momento in cui questi non sono in grado di far fronte alle indagini e al perseguimento del fenomeno.

Esistono una serie di accordi internazionali tra cui la Convenzione di Budapest o la Decisione Quadro 2013/40 UE<sup>307</sup> connessi ad organi operativi complementari (come forze di polizia che agiscono a livello nazionale e sovranazionale), che cercano di andare a fornire nuovi strumenti e a migliorare la cooperazione internazionale.

#### 4.2 Normativa e istituti di contrasto al crimine informatico

Trovare strategie e soluzioni di risposta alla minaccia del crimine informatico è di fondamentale importanza, specialmente per i paesi occidentali. I rischi associati a deboli misure di protezione in alcuni paesi, potrebbero infatti incidere maggiormente sui paesi in via di sviluppo, a causa di misure di protezione meno rigorose e talvolta inesistenti. È necessario così che governi ed istituti

---

*Crime, Law and Social Change* 2006.

<sup>304</sup> Brenner, Susan W., and Leo L. Clarke. *Distributed Security: Preventing Cybercrime*. *John Marshall Journal of Computer & Information Law*, 2005.

<sup>305</sup> Ibid.

<sup>306</sup> Carlo Blengino, *Informatica forense da pag257 a 281* del Manuale di Informatica Giuridica e diritto delle nuove tecnologie (Massimo Durante – Ugo Pagallo) 2017.

<sup>307</sup> Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio.

internazionali collaborino per regolare le tre categorie sopracitate del *cybercrime*, fenomeno oramai in continua espansione<sup>308</sup>.

Reti oscure, cybericlaggio o altri usi impropri della rete da parte dei criminali organizzati rappresentano solo un determinato tipo di condotte all'interno del più vasto mondo del crimine informatico; condotte che possono riconoscersi nella categoria relativa all'uso dei computer come accessorio. Nonostante questo, per arrivare a commettere attività illecite come quelle sui *darkmarkets* molte volte si deve passare per diverse fasi, commettendo più reati sfruttando diversamente i sistemi informatici. Ad esempio, per vendere dati di carte di credito nelle Darknet è necessario commettere un qualche tipo di frode telematica prima, oppure nel caso dell'apertura di una piattaforma fraudolenta online frutto di guadagno illecito, i responsabili saranno imputati sia di frode<sup>309</sup> che di riciclaggio o autoriciclaggio di denaro<sup>310</sup>, commesso con il mezzo della rete.

Prima di andare ad approfondire nello specifico il ruolo di governi e istituzioni nel mondo delle reti oscure e del cybericlaggio, è importante dare una visione della normativa, riguardante il crimine informatico a tre livelli: quello internazionale; europeo e nazionale.

#### 4.2.1 Il Livello Internazionale

Dall'inizio degli anni '90, a partire dall'ottavo Congresso delle Nazioni Unite (ONU) su la prevenzione del crimine e il trattamento dei criminali (1990)<sup>311</sup>, le Nazioni Unite, con la propria rete di istituti per la prevenzione della criminalità e la giustizia penale, cominciano ad essere attivamente coinvolti nell'affrontare i problemi della criminalità transnazionale e della criminalità informatica<sup>312</sup>. La portata della criminalità informatica colpisce tutti i paesi dell'ONU e l'Assemblea Generale delle Nazioni Unite dal 2001 ha promosso nuovi sforzi internazionali per aiutare gli stati membri ad affrontare la criminalità informatica. Un esempio è rappresentato da: “l'incontro su le sfide del XXI secolo” (risoluzione 56/261 della GA)<sup>313</sup> nella quale si è dedicata una sezione speciale “sull'Azione contro l'alta tecnologia e la criminalità informatica”<sup>314</sup>, in cui si trovano

---

<sup>308</sup> Gercke Marco, ITU - *Understanding cybercrime: phenomena, challenges and legal response*, 2012.

<sup>309</sup> Art 640 c.p.

<sup>310</sup> Art. 648 bis e art. 648 ter, c.p.

<sup>311</sup> United Nation, Eight Congress on the Prevention of Crime and the Treatment of Offenders Havana, Cuba, dal 27 agosto al 7 settembre 1990, si veda il link: <https://digitallibrary.un.org/record/1296532/files/a-conf-144-28-rev-1-e.pdf>

<sup>312</sup> Ibid.

<sup>313</sup> Assembla Genenrale delle Nazioni Unite, *Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century*, 2001, si veda il link: [https://www.unodc.org/documents/commissions/CCPCJ/Crime\\_Resolutions/2000-2009/2000/General\\_Assembly/A-RES-55-59.pdf](https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2000/General_Assembly/A-RES-55-59.pdf)

<sup>314</sup> “Action against high-technology and computer-related crime”.

raccomandazioni politiche orientate all'azione per la prevenzione e il controllo di questi nuovi crimini<sup>315</sup>.

Nel 2001 Kofi Annan, ex Segretario Generale delle Nazioni Unite, ha esaminato varie opzioni per incentivare lavori sull'*high-technology* e sulla criminalità informatica, tra cui l'opzione di un "trattato" globale legalmente vincolante riguardante argomenti relativi alla privacy, alla libertà di espressione e ad altri diritti umani e interessi commerciali<sup>316</sup>.

L' Undicesimo Congresso ha rinviato l'azione sullo sviluppo di un trattato sulla criminalità informatica delle Nazioni Unite.

Sebbene non specificamente diretto alla criminalità informatica, il ruolo complementare della **Convenzione Contro la Criminalità Organizzata Transnazionale**<sup>317</sup> (in vigore dal 2003) è uno strumento globale pertinente per affrontare alcuni degli aspetti più cruciali del crimine informatico. La Convenzione, introdotta nel dicembre 2000 a Palermo, consente l'assistenza giudiziaria reciproca (MLA, *mutual legal assistance*) e stabilisce diverse categorie di reato, tra cui: la partecipazione ad un gruppo criminale organizzato e la natura di un reato transnazionale<sup>318</sup>, riciclaggio di denaro sporco, corruzione, ostruzione della giustizia, produzione illecita e traffico di armi da fuoco<sup>319</sup>. Si stabiliscono anche una serie di principi e disposizioni per la cooperazione internazionale, introducendo la responsabilità aziendale e limitando la regola della doppia incriminazione ai fini della mutua assistenza<sup>320</sup>. L'articolo 27 riguarda la cooperazione tra i diversi corpi di polizia e descrive i tipi di assistenza sistematicamente forniti tra i funzionari delle forze dell'ordine in assenza di un accordo formale per quanto riguarda le diverse forme di criminalità transnazionale<sup>321</sup>. La Convenzione amplia infine la gamma dei reati estraibili<sup>322</sup>.

Il primo trattato internazionale riguardante il crimine informatico è "La Convenzione sul Cybercrime", meglio conosciuta come "**Convenzione di Budapest**"<sup>323</sup>.

---

<sup>315</sup> Economic and Social Council, *Effective measures to prevent and control computer-related crime*, 2002, <https://www.unodc.org/pdf/crime/commissions/11comm/8e.pdf>

<sup>316</sup> Redo, S. 'The UN in Broadhurst, R. Ed, *Proceedings of the 2nd Asia Cyber Crime Summit*, Centre for Criminology: University of Hong Kong, 2004.

<sup>317</sup> Assemblea Generale delle Nazioni Unite, *Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale* Palermo, 12 - 15 dicembre 2000, si veda il link: [https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED\\_NATIONS\\_CONVENTION\\_AGAINST\\_TRANSNATIONAL\\_ORGANIZED\\_CRIME\\_AND\\_THE\\_PROTOCOLS\\_THERE TO.pdf](https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERE TO.pdf)

<sup>318</sup> Si veda Capitolo II.

<sup>319</sup> Ibid. Convenzione di Palermo 2001.

<sup>320</sup> Ibid.

<sup>321</sup> Ibid.

<sup>322</sup> Bullwinkel, J. 'International Cooperation in Combating Cyber-Crime in Asia: Existing Mechanisms and New approaches', in R. Broadhurst and P. Grabosky, eds. *Cyber-Crime: The Challenge in Asia*, University of Hong Press, 2005.

<sup>323</sup> Si veda il link: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

Nel 1996, il Consiglio d'Europa stabilisce un comitato per i problemi relativi alla criminalità che a sua volta istituisce un gruppo di esperti per affrontare il crimine informatico, il quale completò i suoi lavori alla fine del 2001.

La Convenzione sulla criminalità informatica che risultò da questo lavoro si pone tre obiettivi:

- In primo luogo, stabilire una base comune su le definizioni di alcuni reati, obbligando i firmatari a criminalizzare un elenco minimo di reati specifici, e quindi consentire l'armonizzazione della legislazione pertinente a livello nazionale<sup>324</sup>.

Il titolo primo riguarda i reati contro la riservatezza, l'integrità e la disponibilità dei dati informatici come ad esempio l'accesso illegale a un sistema informatico<sup>325</sup> o l'uso improprio di dispositivi informatici<sup>326</sup> (ad esempio "strumenti hacker"). In particolare, la Convenzione, all'articolo 6, afferma che le parti contraenti devono criminalizzare la produzione, la vendita, l'acquisto, l'importazione e la distribuzione di codici o altri apparecchi destinati ad azioni di hacking.

Il titolo secondo riguarda i reati tradizionali di frode e falsificazione effettuati attraverso un sistema informatico, mentre il titolo terzo riguarda i crimini relativi al contenuto (come la distribuzione di materiale pedo-pornografico online). Infine, il titolo quarto incrimina le violazioni del diritto d'autore e dei diritti connessi quando tali infrazioni sono state commesse per mezzo di un sistema informatico.

- Il secondo obiettivo della Convenzione è quello di definire una base comune relativa ai poteri e ai mezzi investigativi adatti all'ambiente della tecnologia dell'informazione, cercando di allineare le procedure penali dei diversi paesi in materia. Questo punto viene descritto nella seconda sezione della Convenzione<sup>327</sup> che rappresenta la parte procedurale nella quale si mira a stabilire regole e procedure comuni, adattando le misure tradizionali, come la ricerca o il sequestro, con la creazione di nuove, come la conservazione rapida dei dati<sup>328</sup> (c.d. *quick freeze*), con il fine che rimangano efficaci nel volatile mondo tecnologico. Proprio tale dinamicità dei dati nell'ambiente IT, ha fatto sì che nuovi mezzi potessero rilevarsi utili nel processo di indagine come la raccolta in tempo reale di dati sul traffico<sup>329</sup> e

---

<sup>324</sup> Consiglio d'Europa, *Convenzione sul Crimine Informatico*, 2001, disponibile su: [http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest\\_/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

<sup>325</sup> Consiglio d'Europa, Article 2, Section I – *Substantive Criminal Law, Chapter 2 Measures to be taken at the national level*, *ibid.* 2001.

<sup>326</sup> Consiglio D'Europa, *The misuse of computer-related devices*, *Ibid.* 2001.

<sup>327</sup> Consiglio D'Europa, *Section 2 – Procedural law*, *Ibid.* 2001.

<sup>328</sup> Consiglio D'Europa, *Title 2 – Expedited preservation of stored computer data*, *ibid.* 2001.

<sup>329</sup> Consiglio D'Europa *Title 5 – Real-time collection of computer data*, *Ibid.* 2001.

l'intercettazione dei dati di contenuto<sup>330</sup>. Nonostante ciò, la Convenzione non richiede né giustifica la sorveglianza di comunicazioni personali o contatti, da parte di fornitori di servizi o di forze dell'ordine, a meno che non vi sia un'indagine penale ufficiale<sup>331</sup>.

- Infine, come terzo obiettivo quello di determinare tradizionali e nuovi tipi di cooperazione internazionale, consentendo ai paesi cooperanti di attuare rapidamente le modalità di indagine e accusa promosse dalla Convenzione in concreto. Esempi di questo genere riguardano gli obblighi di proteggere tale Convenzione da parte della legislazione nazionale e di applicare i criteri stabiliti per quanto riguarda la giurisdizione sui reati in questione<sup>332</sup>. Inoltre, si sostiene che prima di applicare i poteri elencati, gli Stati debbano garantire che questi siano proporzionati alla natura e alle circostanze del reato sotto inchiesta<sup>333</sup>. La Convenzione chiarisce che la cooperazione internazionale deve essere fornita tra Stati contraenti “nella misura più ampia possibile<sup>334</sup>”, principio che richiede di ridurre al minimo gli ostacoli al rapido flusso di informazioni e prove.

La Convenzione rappresentò in quegli anni una forte presa di consapevolezza da parte degli Stati nel percepire le nuove minacce provenienti dalla rete, facendo sì che anche altri organi a livello globale e regionale si muovessero in tal senso.

Prendendo atto del lavoro iniziato dal Consiglio d'Europa, l'Assemblea Generale delle Nazioni Unite cominciò inizialmente a conformarsi alla suddetta Convenzione (Risoluzione 55/63<sup>335</sup>), per poi istituire un gruppo intergovernativo di esperti (sotto gestione UNODC) con il fine di condurre uno studio completo sul fenomeno della criminalità informatica ed i legami con il crimine organizzato, andando ad assistere gli Stati e il settore privato, in collaborazione l'uno con l'altro, nella ricerca di migliori risposte al fenomeno (Risoluzione 65/230<sup>336</sup>). Oggi tale programma, implementato negli stati membri attraverso il lavoro dell'UNODC, ed ulteriormente sostenuto dalle

---

<sup>330</sup> Consiglio D'Europa, *Sempre al titolo quinto, Articolo 21 – Interception of content data*, Ibid. 2001.

<sup>331</sup> In riferimento agli articoli 14 e 15 che aprono la sezione procedurale.

<sup>332</sup> Consiglio D'Europa, *Section 3 – Jurisdiction, in particolare Article 22 – Jurisdiction*, Ibid. 2001.

<sup>333</sup> Consiglio D'Europa, *Capitolo III, International co-operation*, Ibid. 2001.

<sup>334</sup> Consiglio D'Europa, *Capitolo III – International co-operation, Section 1 – General principles, Title 1 – General principles relating to international co-operation, Article 23 – General principles relating to international co-operation*, 2001.

<sup>335</sup> Assemblea Generale delle Nazioni Unite, *Combating the criminal misuse of information technologies* 22 gennaio 2001, disponibile su: [https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN\\_resolution\\_55\\_63.pdf](https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf)

<sup>336</sup> Assemblea Generale delle Nazioni Unite, *Resolution adopted by the General Assembly on 21 December 2010, 65/230*. Twelfth United Nations Congress on Crime Prevention and Criminal Justice disponibile: [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/RES/65/230](http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/230)

altre risoluzioni<sup>337</sup>, fornisce assistenza tecnica mirata per lo sviluppo delle capacità, per la prevenzione, la sensibilizzazione, la cooperazione internazionale e l'analisi del fenomeno del crimine informatico.

Da questi esempi, gruppi di nazioni ed organizzazioni internazionali hanno agito per migliorare i propri apparati interni, creando nuovi istituti e legislazioni improntate per combattere le minacce provenienti dal mondo cibernetico.

L'Organizzazione internazionale di polizia criminale, l'**Interpol**, si impegna a essere un organismo di coordinamento globale per l'individuazione e la prevenzione dei crimini digitali. L'Interpol attraverso il *Global Complex for Innovation (IGCI)*<sup>338</sup> mira a condividere le competenze e ad evitare la duplicazione di attività già in corso, in modo che gli organi di polizia possano concentrare efficacemente le proprie risorse sulla lotta alla criminalità informatica, collaborando con altre parti interessate a sviluppare una risposta coordinata a questa crescente minaccia<sup>339</sup>.

I paesi del G8 nell'arco dei diversi incontri sono andati a sottolineare sempre più il pericolo rappresentato dal crimine informatico<sup>340</sup>, mentre l'**OCSE**<sup>341</sup> ospita al suo interno una delle organizzazioni più efficaci al coordinamento intergovernativo delle forze dell'ordine offrendo modelli per la cooperazione transnazionale contro la criminalità informatica: il **GAFI**, Gruppo di Azione Finanziaria Internazionale<sup>342</sup>. Il GAFI è un'organizzazione intergovernativa il cui obiettivo è l'attuazione di riforme legislative e regolamentari necessarie per combattere il riciclaggio di denaro. Il Gruppo ogni anno mette sotto un processo di valutazione i propri stati membri, verificando che abbiano implementato regolamenti e norme dediti alla sicurezza di transazioni finanziarie online<sup>343</sup>.

Anche gli sforzi regionali sono in corso grazie all'iniziativa di OAS (Organizzazione degli Stati americani), ASEAN (Associazione delle Nazioni del Sud-est asiatico) e dell'APEC (Cooperazione Economica Asiatico-Pacifica).

---

<sup>337</sup> UNODC, *Strengthening international cooperation to combat cybercrime*, 2010, disponibile su: [https://www.unodc.org/documents/commissions/CCPCJ/Crime\\_Resolutions/2010-2019/2013/CCPCJ/Resolution\\_22-7.pdf](https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-7.pdf)

<sup>337</sup> UNODC, *Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime*, 2013, disponibile su: [https://www.unodc.org/documents/commissions/CCPCJ/Crime\\_Resolutions/2010-2019/2013/CCPCJ/Resolution\\_22-8.pdf](https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf)

<sup>338</sup> Si veda il link: <https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation>

<sup>339</sup> Si veda il link: [file:///C:/Users/owner/Downloads/IGCI\\_CIO\\_strategy%20and%20outreach\\_projectsheet\\_2017-03\\_EN\\_web.pdf](file:///C:/Users/owner/Downloads/IGCI_CIO_strategy%20and%20outreach_projectsheet_2017-03_EN_web.pdf)

<sup>340</sup> Si veda il link: <http://www.cybercrimelaw.net/G8.html>

<sup>341</sup> Organizzazione per la cooperazione e lo sviluppo economico, mira a promuovere il benessere economico e sociale aiutando gli Stati membri a coordinare i loro sforzi per aiutare le nazioni meno sviluppate, conta attualmente 36 membri attivi, tra cui la maggior parte membri dell'Unione Europea.

<sup>342</sup> Si veda: <http://www.fatf-gafi.org/>

<sup>343</sup> GAFI Report, *Money Laundering Using New Payment Methods*, ottobre 2010.

Durante l'assemblea generale dell'OAS del 2004, gli Stati membri hanno approvato la risoluzione AG/RES.2004 (XXXIV-O/04)<sup>344</sup>, intitolata "La strategia integrale interamericana per combattere le minacce alla sicurezza informatica", incaricando in questo modo il Segretariato di cominciare a lavorare su le relative risposte al crimine informatico. La conseguenza fu la creazione di un gruppo teso al supporto tecnico degli stati membri in caso di attacco: il *Computer Security Incident Response Teams (CSIRTs)* che ancora oggi promuove una cultura tesa alla consapevolezza delle nuove minacce<sup>345</sup>.

Durante il comunicato congiunto della quarta riunione ministeriale dell'ASEAN sulle forme del crimine transnazionale del 2004<sup>346</sup>, i ministri hanno riconosciuto il crimine informatico come fonte di accrescimento della criminalità transnazionale che incide sulla sicurezza dei paesi membri e sollecita un'efficace cooperazione giudiziaria nella lotta a questo tipo di crimine<sup>347</sup>. Negli anni successivi si sono cercate di creare diverse forme di cooperazione in materia grazie all'*ASEAN Regional Forum*, importante piattaforma di dialogo sul tema della sicurezza informatica, nel quale operano gruppi di esperti che tengono riunioni periodiche, workshop e seminari su argomenti relativi al terrorismo cibernetico e al *cybercrime*<sup>348</sup>.

Per quanto riguarda l'APEC invece, l'assemblea unanime, già dal 2003, ha dato vita al *The e-Security Task Group*<sup>349</sup>, progetto per la creazione di capacità legislative tese al rafforzamento delle norme in materia di criminalità informatica. L'anno seguente venne deciso di attuare una legislazione nazionale dei paesi membri coerente con le disposizioni degli strumenti giuridici internazionali, compresa la Convenzione di Budapest (2001) e le seguenti risoluzioni dell'Assemblea generale delle Nazioni Unite<sup>350</sup>. Oggi anche grazie all'aiuto dell'APEC *Telecommunications and Information Working Group (TEL)*<sup>351</sup>, gli Stati Membri sono periodicamente aggiornati su le nuove tecniche e metodi messi in atto dal crimine informatico<sup>352</sup>.

Sebbene passi avanti in materia siano stati fatti da un punto di vista regionale, le attività portate avanti dagli organi europei per quanto riguarda il crimine informatico rimangono un esempio per le altre legislazioni di questo genere<sup>353</sup>.

---

<sup>344</sup> Si veda il link: [http://www.oas.org/en/sms/cicte/documents/oas\\_ag/ag-res\\_2004\\_\(xxxiv-o-04\)\\_en.pdf](http://www.oas.org/en/sms/cicte/documents/oas_ag/ag-res_2004_(xxxiv-o-04)_en.pdf)

<sup>345</sup> Si veda il sito: [www.csirt.org/](http://www.csirt.org/)

<sup>346</sup> Si veda il link: <https://www.asean.org/uploads/archive/5187-9.pdf>

<sup>347</sup> Lennon Y.C. Chang, *Cybercrime and Cyber Security in ASEAN*, luglio 2017.

<sup>348</sup> Ibid.

<sup>349</sup> Si veda il link: <http://www.oecd.org/sti/ieconomy/2492761.pdf>

<sup>350</sup> Informazioni ricavate dal sito: <http://www.cybercrimelaw.net/APEC.html>

<sup>351</sup> Si veda al link: <https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information>

<sup>352</sup> Si veda il link: <http://www.apectel28.com.tw/document/webword/estg/telwg28-ESTG-07.doc>

<sup>353</sup> Khoo, B. H. *Police Cooperation in Fighting Transnational Organised Crime: An Asian Perspective*, in R. Broadhurst (Ed.) *Bridging the GAP: A Global alliance on Transnational Organised Crime*, Hong Kong Police: Printing Department HKSAR, 2003.

#### 4.2.2 Il livello Europeo

L'Unione Europea include al suo interno diversi istituti sovranazionali che affrontano le sfide poste dalla cyber-criminalità internazionale adottando posizioni comuni, direttive e altri strumenti per combattere una vasta gamma di attività criminali. Uno dei primi esempi è l'istituzione di una "Rete Giudiziaria Europea" (European Judicial Network), fondata nel '97, che consente di mettere in contatto magistrati e rappresentanti incaricati di assistenza giudiziaria internazionale, facilitando la cooperazione transfrontaliera<sup>354</sup>. Un ulteriore rafforzamento alla mutua assistenza in ambito giudiziario è contenuto nella proposta del 19 aprile 2002, una decisione quadro del Consiglio relativa agli attacchi contro i sistemi di informazione<sup>355</sup>. La decisione, successiva alla ratifica della Convenzione di Budapest, è l'inizio di un percorso di armonizzazione della normativa tesa alla lotta del crimine informatico nei diversi Stati membri dell'Unione. Proprio nell'intento di aumentare una cooperazione in senso giudiziario, che vada oltre una rete di contatti, sempre nel 2002, viene istituita dal Consiglio dei Ministri dell'Unione, l'Eurojust un organo che mette in collaborazione gli istituti giudiziari dei diversi paesi con il fine della cooperazione penale<sup>356</sup>. Uno dei risultati degli incontri di Eurojust è stato la fondazione, nel 2016, dell'Eurojust European Judicial Cybercrime Network (EJCN) rete intenta a favorire contatti tra professionisti e specialisti nel contrastare le sfide poste dalla criminalità informatica<sup>357</sup>.

Pienamente integrato nell'Unione con la decisione del Consiglio 2009/371/JHA<sup>358</sup> il 6 aprile del 2009, l'Europol, l'ufficio di polizia dell'UE, oggi rappresenta uno degli organi di riferimento per la lotta al crimine informatico. La Decisione andava inoltre a rafforzare l'impegno europeo contro gravi forme di criminalità organizzata<sup>359</sup>.

Il nuovo ufficio di polizia europeo è composto da funzionari di collegamento (che rappresentano la legislazione nazionale attraverso le agenzie di controllo in tutta l'UE, compresi organi di polizia, funzionari doganali e d'immigrazione) e dallo staff interno. La funzione principale dell'Europol è di sostenere le attività operative dei funzionari nazionali incaricati nell'applicare le leggi relative al combattere diverse forme di crimine, compresa la criminalità informatica<sup>360</sup>. Si cerca così di

---

<sup>354</sup> Si veda il link: <http://www.europa.eu.int/scadplus/leg/en/lvb/133055.htm>

<sup>355</sup> Si veda il link: <http://www.cybercrimelaw.net/EU.html>

<sup>356</sup> Si veda il link: [http://www.eurojust.europa.eu/press/PressReleases/Documents/2018-04-26\\_Eurojust-FactSheet.pdf](http://www.eurojust.europa.eu/press/PressReleases/Documents/2018-04-26_Eurojust-FactSheet.pdf)

<sup>357</sup> Si veda il link: <http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx>

<sup>358</sup> Si veda il link: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32009D0371> abrogata nel 2016, oggi in forza: "Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and abrogata dalla "Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA" si veda al link: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0794>

<sup>359</sup> Parlamento Europeo, *Documento di Lavoro sulla Criminalità Organizzata*. Commissione speciale sulla criminalità organizzata, la corruzione e il riciclaggio di denaro, 1.10.2012

<sup>360</sup> Si veda il link: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

facilitare lo scambio di informazioni, fornire analisi, relazioni strategiche su tendenze e modelli di attività criminale, scambiando competenze tecniche per le indagini in corso all'interno dell'UE.

Nel 2013 l'*Eruopol* istituisce lo *European Cybercrime Centre* (EC3) corpo operativo che si occupa di crimine informatico, improntando il suo lavoro sul supporto operativo, tecnico e analitico alle indagini degli Stati Membri<sup>361</sup>. Il centro, frutto della Direttiva 2013/40 / UE<sup>362</sup> promulgata dal Parlamento e dal Consiglio, ha come compito la lotta ai crimini informatici commessi da gruppi organizzati, in particolare quelli che generano grandi profitti quali frode on-line; lo sfruttamento sessuale di minori online; attacchi informatici che colpiscono i sistemi critici di infrastrutture europee ed il commercio nelle reti oscure, compreso il cybericclaggio. Il gruppo è impegnato ogni anno inoltre nello stilare un rapporto strategico di punta sulle scoperte chiave, le minacce emergenti e gli sviluppi del cybercrime: lo *Internet Organised Crime Threat Assessment* (IOCTA). Il documento fornisce raccomandazioni chiave destinate alle forze dell'ordine e ai responsabili politici per consentire loro di rispondere alle minacce informatiche in modo efficace e concertato<sup>363</sup>.

Nel 2014, in collaborazione con Eurojust, EC3 guida l'operazione *Onymous*, mettendo fine ai commerci in ben 410 piattaforme delle Draknet<sup>364</sup> tra cui Pandora, Cannabis Road, Black Market e Silk Road 2.0<sup>365</sup>, sequestrando un milione di euro in Bitcoin, insieme al valore pari a 180.000 euro di contanti, oro, argento e droghe<sup>366</sup>. In occasione dell'operazione viene lanciato all'interno dell'EC3 il *Joint Cybercrime Action Taskforce* (J-CAT), creato per servire come piattaforma per le operazioni mirate contro le reti criminali globali e le infrastrutture dei mercati di rete dentro e fuori i confini europei<sup>367</sup>. L'iniziativa, prima nel suo genere, è tesa alla collaborazione su più frontiere, coordinando le indagini internazionali con i partner, massimizzando l'efficacia delle azioni congiunte contro le principali minacce informatiche<sup>368</sup>. Questo alto livello dal punto di vista collaborativo ha portato fin dall'inizio degli ottimi risultati, facendo chiudere decine di siti online e sequestrando grandi quantità di materiale pedo-pornografico<sup>369</sup>.

Il ruolo fondamentale svolto da questo insieme d'istituti rimane però fortemente limitato, mancando una previsione di un autonomo potere d'iniziativa in ambito penale. Questo può essere dovuto ad una certa riluttanza degli Stati Membri a privarsi di una parte di sovranità così importante e legata al

---

<sup>361</sup> Ashford, Warwick *European Cybercrime Centre opens in The Hague*, 2013, disponibile sul sito: <https://www.computerweekly.com/news/2240175936/European-Cyber-Crime-Centre-opens-in-The-Hague>

<sup>362</sup> Si veda il link: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF>

<sup>363</sup> Si veda il link: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment>

<sup>364</sup> Si veda il link: <https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network>

<sup>365</sup> Si veda il link: <https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/>

<sup>366</sup> Si veda il link: <https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network>

<sup>367</sup> Si veda il link: <https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce>

<sup>368</sup> Marcena Hunter, *Innovation in international Cooperation to counter cybercrime: The joint cybercrime Action Task force (J-CAT)*, 2018.

<sup>369</sup> Ibid.

territorio come quella derivante dagli esercizi delle forze di polizia. Il coordinamento sovranazionale è di fondamentale importanza proprio per mettere in contatto e condividere indagini ed informazioni perpetrate dai singoli organi nazionali impegnati nella lotta al crimine informatico.

#### 4.2.3 Il livello italiano

La disciplina normativa italiana riguardante le minacce provenienti dal cyberspazio anticipa le regolamentazioni internazionali in materia con l'elaborazione della legge n. 547 del 1993<sup>370</sup>, intitolata "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"<sup>371</sup>. La legge aggiunge al codice penale diverse fattispecie inquadrabili in quattro macro aree di intervento:

- 1) Frode Informatica;
- 2) Falsificazione;
- 3) Integrità dei dati e dei sistemi informatici;
- 4) Riservatezza dei dati e delle comunicazioni informatiche.

La legge del '93 rimane ancora oggi la base normativa di rilievo nella lotta alle nuove minacce legate al crimine informatico.

Altro passo in avanti fu fatto dal Decreto del Ministro dell'Interno del 28 aprile 2006<sup>372</sup>, avente titolo "Riassetto dei comparti di specialità delle Forze di polizia"<sup>373</sup>. Il Decreto ha determinato la Polizia Postale quale organo specializzato nel contrasto dei crimini perpetrati attraverso Internet e l'uso di mezzi elettronici computerizzati<sup>374</sup>, rendendo così l'organo il maggiore attore di contrasto nazionale al crimine informatico.

Con un ulteriore decreto ministeriale datato il 9 gennaio del 2008, viene istituito ufficialmente il CNAIP, il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche, un "unità organizzativa di livello non dirigenziale, incardinata nel servizio di polizia postale"<sup>375</sup>.

Qualche mese dopo viene ufficialmente ratificata la Convenzione di Budapest del 2001, con la legge del 18 marzo 2008, n. 48<sup>376</sup>, tra le cui principali modifiche aggiunte al codice penale c'è l'art. 615 - quinquies "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a

---

<sup>370</sup> Si veda il link: [http://www.gazzettaufficiale.it/atto/serie\\_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=1993-12-30&atto.codiceRedazionale=093G0633&elenco30giorni=false](http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=1993-12-30&atto.codiceRedazionale=093G0633&elenco30giorni=false)

<sup>371</sup> Ibid.

<sup>372</sup> Si veda il link: <http://gazzette.comune.jesi.an.it/2006/193/1.htm>

<sup>373</sup> Ibid.

<sup>374</sup> specialmente nel caso di frode e falsificazione in materia di diritto d'autore.

<sup>375</sup> Decreto del Ministero dell'Interno, 9 gennaio 2008, si veda il link: <http://www.poliziadistato.it/statics/44/d.m.-9-gennaio-2008-istituzione-cnaipic.pdf>

<sup>376</sup> Si veda il link: <http://www.parlamento.it/parlam/leggi/080481.htm>

danneggiare o interrompere un sistema informatico o telematico” ( in riferimento anche a coloro che volessero diffondere attraverso il dark web diversi tipi di malware o programmi tesi a commettere reato in Internet).

Le modifiche alla procedura penale rispecchiano i miglioramenti apportati dalla Convenzione in ambito procedurale<sup>377</sup>, come descritto precedentemente<sup>378</sup>. Volendo questo lavoro dare una visione d’insieme dello scenario normativo non se ne entrerà nel merito. Nonostante ciò è importante ricordare che tale modifica resta mancante nell’avvicinare scienza e diritto, in un ambito così specifico come quello informatico<sup>379</sup>. L’assenza di un rimando ad espressi organi più tecnici in materia, il mancato riferimento ad una catena di custodia e l’assenza di sanzioni penali processuali hanno portato tale ratifica ad apparire incompleta nella pratica attuativa<sup>380</sup>.

#### *4.2.3.1 Legame tra aspetto normativo ed operativo nel contrasto ai reati nelle Darknet*

Ulteriori mancanze si manifestano nelle operazioni di contrasto al crimine informatico delle forze dell’ordine nel momento in cui queste si occupano di reati commessi per mezzo di tecniche di anonimato in rete o attraverso transazioni in cripto-valuta. Considerando la parziale assenza di un corpo normativo che possa limitare gli illeciti commessi nelle Darknet, l’unico modo di condurre le indagini è rappresentato dall’intercettare le transazioni illecite e ricollegarle ad un indirizzo che a sua volta porti gli operatori di sicurezza ad individuare chi si cela dietro alle compravendite “sotterranee” ( operazioni sempre più complesse visto il sofisticato livello di sviluppo di tali tecniche); in modo da poter imputare i colpevoli dei reati di volta in volta commessi in rete. Tra questi si possono menzionare i reati connessi alla vendita, immissione in commercio e trasporto di sostanze stupefacenti e psicotrope specificamente sanzionati nel "Testo unico sugli stupefacenti", il d.p.r. 309 del 1990<sup>381</sup>; il reato di "Fabbricazione o commercio non autorizzato di armi" riportato nell’art. 695 c.p.; fino ai reati di "Pornografia minorile" e di "Detenzione di materiale pedopornografico" di cui agli artt. 600-ter e 600-quater del Codice Penale.

Nell’arco del tempo la Polizia Postale ha cercato di limitare le attività nelle Darknet, specialmente nell’ambito della pedopornografia, contribuendo ad affinare modalità e strumenti condivisi nell’ambito della collaborazione internazionale di polizia con le varie agenzie investigative estere

---

<sup>377</sup> Si interviene in ambito di ispezioni, perquisizioni, sequestri, intercettazioni, sottolineando il carattere fondamentale della prova digitale.

<sup>378</sup> Si veda la descrizione in punti della Convenzione di Budapest riportata a pagina 59/60 di questo lavoro.

<sup>379</sup> Carlo Blengino, *Informatica forense da pag257 a 281*, Manuale di Informatica Giuridica e diritto delle nuove tecnologie (Massimo Durante – Ugo Pagallo) 2017.

<sup>380</sup> Ibid. Blengino, 2017.

<sup>381</sup> Si veda il link: [http://www.federserd.it/files/download/dr\\_p\\_309\\_9-10-90\\_aggiornato.pdf](http://www.federserd.it/files/download/dr_p_309_9-10-90_aggiornato.pdf)

ed avvalendosi del coordinamento dell'EC3 di Europol<sup>382</sup>. Il problema centrale a riguardo delle indagini in materia rimane l'anonimato, che nella sua evoluzione sta mostrando sempre più impermeabilità ai tentativi di intrusione degli organi di sicurezza. Non permettendo la rintracciabilità dei criminali che operano nelle Darknet, si è di fronte all'impossibilità per le forze giudiziarie di imputare i responsabili.

Tali considerazioni portano a riflettere su nuovi strumenti e forme di contrasto.

Da pochi anni a questa parte c'è stato qualche movimento da parte degli uffici Interpol nel cercare di individuare nuovi metodi d'indagine che potessero porsi come prime forme di risposta a tali problematiche.

### 4.3 Attività di contrasto dell'Interpol

L'*Interpol Global Complex for Innovation* mira a costruire relazioni tra le forze di polizia, cercando di aumentare la comprensione delle questioni di sicurezza digitale e facilitare la creazione di capacità operative tra gli organi di sicurezza dei paesi Membri.

Attraverso summit, corsi intensivi, mezzi e incontri formativi, l'Interpol cerca di superare le difficoltà di molte forze di polizia locali e nazionali nell'affrontare le nuove sfide poste dal crimine informatico.

Nel luglio del 2015, l'Interpol ha fornito cinque giorni di formazione specializzata sul mondo delle Darknet, in collaborazione con l'Organizzazione per la ricerca scientifica applicata dei Paesi Bassi (Netherlands Organisation for Applied Scientific Research, TNO)<sup>383</sup>. Tale formazione, ospitata dal *Gloabl Complex* a Singapore e gestita dal Laboratorio di cyber-ricerca<sup>384</sup>, consisteva in una simulazione basata su la riproduzione di un insieme di mercati del dark web, ricreando l'ambiente virtuale "sotterraneo" utilizzato dai criminali<sup>385</sup>. Durante i cinque giorni i partecipanti<sup>386</sup> hanno svolto il ruolo di venditori, acquirenti e amministratori con simulazioni di "take down"<sup>387</sup> da parte delle forze dell'ordine<sup>388</sup>. Questi esercizi hanno aiutato i partecipanti a migliorare la loro comprensione delle infrastrutture tecniche e il funzionamento di queste tecnologie<sup>389</sup>.

---

<sup>382</sup> Polizia Postale e delle Comunicazioni, doc. 2016, si veda il link: <https://www.commissariatodips.it/fileadmin/src/doc/pdf/PoliziaPostale.pdf>

<sup>383</sup> Si veda il link: <https://www.interpol.int/News-and-media/News/2015/N2015-108>

<sup>384</sup> Cyber Research Lab.

<sup>385</sup> Si veda nota 614.

<sup>386</sup> I rappresentanti presenti di Australia, Finlandia, Francia, Ghana, Hong Kong, Indonesia, Giappone, Paesi Bassi, Singapore, Sri Lanka e Svezia hanno partecipato alla prima sessione di formazione.

<sup>387</sup> *Take down* è l'espressione che si usa in materia relativa alla chiusura di un sito maligno un di un servizio nascosto con contenuti illeciti.

<sup>388</sup> Butler Eamonn, *Cryptocurrencies: Threats and Investigative Opportunities for Law Enforcement*, Charles University 31-07-2018.

<sup>389</sup> Ibid.

L'anno seguente Interpol, Europol e Basel Institute of Governance<sup>390</sup> hanno stabilito una partnership tripartita a condurre un gruppo di lavoro incentrato sul riciclaggio di denaro e sull'uso improprio delle valute digitali<sup>391</sup>. Gli obiettivi principali del gruppo di lavoro erano:

1. Raccogliere, analizzare e scambiare informazioni non operative riguardanti l'uso di cripto-valute come mezzo di riciclaggio di denaro, e il recupero dei procedimenti di indagini;
2. Organizzare workshop e incontri annuali per i rappresentanti delle forze dell'ordine e delle istituzioni per aumentare la capacità di indagare con successo sui crimini in cui sono coinvolte le cripto-valute;
3. Creare una rete di professionisti ed esperti in questo campo, che potessero collettivamente stabilire le migliori pratiche al fine di aiutare e creare raccomandazioni sia all'interno che all'esterno del gruppo di lavoro<sup>392</sup>.

Continuando con questa collaborazione, negli anni successivi si sono tenuti due ulteriori workshop globali<sup>393</sup>. Nel Gennaio 2017, oltre 400 investigatori finanziari accanto a rappresentanti del settore privato sono stati direttamente coinvolti nella scoperta del legame tra cyber-criminalità e riciclaggio di denaro sporco<sup>394</sup>.

Nel marzo del 2018, in collaborazione con il *German Bavarian Ministry of Justice*, l'Interpol ha reclutato 39 esperti in rappresentanza di 18 paesi membri di Europol (l'ufficio di polizia europeo), con il fine di consultarsi sulla minaccia crescente delle Darknet e del mondo delle cripto-valute<sup>395</sup>. Durante l'incontro sono stati condivisi esempi di indagini di transazioni in cripto-valuta nei diversi paesi, considerando sfide legali e tecniche che le rispettive giurisdizioni hanno affrontato. Come risultato di tale consultazione il 3 aprile viene fondato il *Working Group on Darknet and Cryptocurrencies*, il primo gruppo di lavoro che si occupa dei fenomeni relativi alle attività commerciali nelle reti oscure e delle relative transazioni in cripto-valute<sup>396</sup>.

Come prima osservazione, il *Working Group* ha rivelato l'ascesa degli Altcoin quale "crescente minaccia" al lavoro svolto dalle forze dell'ordine nel cercare di combattere l'anonimato delle transazioni illecite<sup>397</sup>. Una delle problematiche emergenti è relativa alla mancanza di strumenti per la tracciabilità delle monete che usano tecniche di anonimizzazione, come Monero o Zcash. Inoltre,

---

<sup>390</sup> Si veda il link: <https://www.baselgovernance.org/>

<sup>391</sup> Si veda il link: <https://new.baselgovernance.org/news-publications/news/basel-institute-europol-and-interpol-establish-working-group-money>

<sup>392</sup> Ibid.

<sup>393</sup> Ibid.

<sup>394</sup> Ibid.

<sup>395</sup> Si veda il link: <https://www.deepdotweb.com/2018/04/20/interpol-holds-first-darknet-and-cryptocurrency-working-group/>

<sup>396</sup> Si veda il link: <https://www.interpol.int/News-and-media/News/2018/N2018-022>

<sup>397</sup> Chohan, U.W. *The Licentious Blockchains: Outlining an Altcoin Subgenre*. SSRN, 2018.

i diversi membri presenti hanno comunemente osservato il rapido incremento di molte delle pagine illecite presenti su le Darknet, asserendo alla pericolosità di queste attività nel coinvolgere entità criminali di diverso genere.

Le conclusioni raggiunte alla fine dell'evento sono state in primo luogo, quelle di condividere informazioni tecniche, ed in secondo luogo la necessità di aggiungere nel quadro giuridico UE le definizioni di "cripto-valute", "valuta digitale" "exchanger" e "wallet provider"<sup>398</sup>.

Nella discussione riguardante la promozione e la sensibilizzazione in tema di sicurezza delle transazioni in cripto-valute, l'Europol, come partner di Interpol, ha un ruolo di primo piano, riunendo una varietà di esperti di diverse discipline e professionisti del diritto contribuendo così allo sviluppo della comunità di esperti di investigatori e pubblici ministeri.

Il terzo incontro del gruppo di lavoro dell'Interpol su le Darknet e le cripto-valute, segnato per luglio 2019, affronterà il problema relativo alla de-anonimizzazione, finalizzato a fornire agli investigatori in materia spunti pratici su come attribuire le attività criminali svolte nelle Darknet ad individui specifici<sup>399</sup>. L'obiettivo è condurre uno studio empirico sulle strategie, le metodologie e gli strumenti esistenti per la de-anonimizzazione degli attori criminali che sfruttano l'anonimato ereditato delle cripto-valute e dai servizi .onion. L'intenzione è quella di sviluppare un documento analitico che illustri le migliori pratiche utilizzate a riguardo dalle forze dell'ordine in tutto il mondo<sup>400</sup>.

L'obbiettivo che si cercherà di raggiungere nei prossimi incontri è quello di andare a rafforzare la cooperazione con le istituzioni europee per sensibilizzare maggiormente le legislazioni nazionali dei paesi più sviluppati, che soffrono maggiormente della presenza delle reti oscure.

Specialmente Europol ed Eurojust svolgono un ruolo centrale in questo processo, presentando pareri, report e indagini<sup>401</sup> per aggiornare la comunità e i responsabili delle decisioni presso gli altri organi dell'Unione sugli sviluppi della criminalità organizzata attraverso le nuove tecnologie di rete.

#### *4.4 Prospettive normative e politiche pubbliche nel contrasto all'economia sotterranea del crimine organizzato*

Nel quadro normativo riguardante il crimine informatico non appare alcuna definizione né di Darknet, né di anonimato della rete e neppure di cripto-mercati (o *darkmarkets*). Questo perché

---

<sup>398</sup> Ibid. Butler, 2018.

<sup>399</sup> INTERPOL Working Groups @ INTERPOL World 2019 Si veda il link: <https://www.interpol-world.com/working-groups/>

<sup>400</sup> Ibid.

<sup>401</sup> Si fa riferimento a report come IOCTA e SOCTA.

nell'arco degli anni le legislazioni dei diversi paesi hanno cercato di adattare le leggi penali esistenti ai reati commessi all'interno di questi spazi nascosti della rete.

Questo tipo di operazione oggi risulta marginale ad un quadro normativo che ha bisogno di rafforzare le proprie basi in relazione alla nuova società digitale, nella quale le attività commerciali "sotterranee" del crimine rappresentano un mercato da miliardi di euro annui.

Nei seguenti sotto-paragrafi si cercherà di delineare, alla luce della normativa vigente riguardante i crimini informatici, quali possano essere le politiche pubbliche applicabili e le iniziative di riforma percorribili nella lotta al legame tra crimine organizzato e reti oscure. Si cercherà dapprima di evidenziare quali delle norme, già descritte nel paragrafo precedente, possano essere applicabili a tale contesto, per poi fare una serie di considerazioni riguardanti il tema del contrasto all'anonimato in rete.

Il lavoro di tesi, nella parte finale di questo paragrafo, cercherà di fornire un contributo in materia su quelle che possano essere le scelte da intraprendere nella lotta all'uso improprio dell'*onion routing* e delle cripto-valute da parte del crimine organizzato.

#### 4.4.1 La normativa applicabile

Il Consiglio d'Europa e le Nazioni Unite hanno fornito due importanti strumenti normativi quali punti di partenza necessaria per condurre lo sviluppo di una legislazione propria nel combattere i commerci illeciti da parte delle organizzazioni criminali all'interno delle Darknet.

Nella Convenzione sul Crimine Informatico (2001) si possono evidenziare due principali disposizioni riadattabili al contesto di nostro interesse: in primo luogo l'art. 6 della Convenzione, in secondo luogo i principi di mutua assistenza.

Nell'art.6, "Abuso di apparecchiature"<sup>402</sup>, si dichiara che ogni parte contraente deve usare misure legislative coercitive nei confronti della vendita di apparecchiature, malware, password o codici d'accesso privati ai fini di hackeraggio (inglobata dall'ordinamento italiano dalla modifica dell'art.615 quinquies c.p.). L'articolo nella pratica, anche se redatto ben prima della nascita di veri e propri mercati del crimine online, vieta qualsiasi tipo di compravendita riguardante una delle categorie presenti nei *darkmarkets*.

Il secondo contributo all'interno della Convenzione è presente nel terzo capitolo, al titolo terzo che riguarda i principi generali della mutua assistenza e della condivisione di informazioni e prove tra i paesi contraenti; operazione fondamentale per lo svolgimento delle indagini. Le restanti

---

<sup>402</sup> Per consultare l'articolo originale si veda il link: <https://www.poliziadistato.it/statics/14/convenzione-cybercrime.pdf>

disposizioni dalla frode alla falsificazione informatica<sup>403</sup>, dai reati relativi alla pornografia infantile a quelli contro la proprietà intellettuale<sup>404</sup> vanno a completare un quadro parzialmente adattabile all'ambito dei commerci sotterranei di rete, ma non sufficiente. Questo anche perché l'applicabilità di questi crimini non erano stati pensati per una rete anonima come quella permessa dall'*onion routing* e conseguentemente non esistono delle disposizioni destinate agli organi giudiziari per limitare tali condotte correttamente nel dark web. Inoltre, all'epoca non si era realizzata ancora l'idea che veri e propri gruppi organizzati potessero agire in rete.

Il 19 aprile del 2010 le Nazioni Unite inaugurando il dodicesimo Congresso sulla prevenzione del crimine e della giustizia criminale a Salvador in Brasile<sup>405</sup> hanno adottato una dichiarazione che invita gli Stati ad un cambiamento della propria giustizia penale per quanto riguarda le leggi sul cyberspazio e sul crimine cibernetico. Si è sottolineata la necessità di fare un uso più efficace della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, adottata a Palermo nel 2000, nella quale si evidenzia il contrasto alle diverse forme di commercio illecito, specialmente di armi da fuoco ed esplosivi<sup>406</sup>. Il richiamo alla Convenzione viene fatto nell'intento di sensibilizzare i paesi per quanto riguarda l'incontro tra il fenomeno del crimine organizzato transnazionale e il mondo dei reati commessi in rete<sup>407</sup>.

La Convenzione di Palermo, come ricordato in precedenza, rappresenta uno strumento normativo eccezionale nella lotta alle diverse forme di criminalità a livello internazionale<sup>408</sup>; questo anche grazie all'istituzione di importanti disposizioni attribuite ad un vastissimo numero di Stati.

Sono presenti nella Convenzione l'assistenza giudiziaria reciproca (art. 18); la cooperazione internazionale di polizia (art.27), quella ai fini della confisca (art.13) e numerose definizioni sconosciute a molti ordinamenti giuridici<sup>409</sup>. Di estrema importanza risulta l'obbligo di incriminazione (art.34c.2), ovvero l'obbligo per le diverse legislature di criminalizzare determinate condotte tra cui: i reati di partecipazione ad un gruppo criminale organizzato (art. 5) il reato di riciclaggio di denaro (art.6) ed il reato di corruzione (art.8)<sup>410</sup>.

Questo panorama normativo può essere l'origine da cui sviluppare una regolamentazione propria compatibile alla realtà delle Darknet.

---

<sup>403</sup> Titolo secondo, reati informatici art.7 e 8.

<sup>404</sup> Rispettivamente titolo secondo e quarto, art. 9 e 10.

<sup>405</sup> Si veda paragrafo 2

<sup>406</sup> UNODC, *The Protocol against the Illicit Manufacturing and Trafficking in Firearms*, 2001.

<sup>407</sup> UNODC, *Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World*, 2010, Si veda il link: [https://www.unodc.org/documents/crime-congress/12th-CrimeCongress/Documents/Salvador\\_Declaration/Salvador\\_Declaration\\_E.pdf](https://www.unodc.org/documents/crime-congress/12th-CrimeCongress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf)

<sup>408</sup> Ibid.

<sup>409</sup> Reato grave, gruppo strutturato, provento del reato, congelamento o sequestro ecc..

<sup>410</sup> Assemblea Generale delle Nazioni Unite, *Risoluzione 55/25 del 15 novembre 2000*, Ibid. Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale” Palermo, 12 - 15 dicembre 2000.

Il primo punto da affrontare in vista di ulteriori regolamentazioni è il tema dell'anonimato in rete, fonte di discussione all'interno degli apparati istituzionali impegnati nella lotta ai crimini informatici nelle reti oscure.

#### 4.4.2 Politiche pubbliche nella lotta contro l'anonimato del crimine in rete

Il Dark Web è un argomento nuovo per molti responsabili delle politiche pubbliche<sup>411</sup>, ed è essenziale comprenderne in principio le modalità attraverso le quali poter regolare questo particolare ambito della rete.

Come abbiamo potuto osservare, le attuali leggi sul crimine informatico, sia a livello nazionale che internazionale, sono largamente applicabili al Dark Web che risulta difficilmente inseribile in un quadro normativo. Tale difficoltà è rappresentata dal fatto che regolare le reti oscure significherebbe regolare TOR<sup>412</sup>.

L'anonimato è ciò che rende il mondo delle Darknet diverso da tutto ciò che c'è in superficie della rete e limitarlo vorrebbe dire limitare tutti i sistemi basati su protocolli di rete di *onion routing*, come TOR.

Esistono così due sfide centrali delle politiche pubbliche riguardanti il Dark Web:

- 1) lasciare la possibilità agli utenti di poter anonimizzare le proprie comunicazioni
- 2) collaborare a livello internazionale e trovare soluzioni per sconfiggere i soggetti che delinquono con l'uso della crittografia e dell'anonimato<sup>413</sup>.

La prima questione è rappresentata dal fatto che non esiste alcun motivo per cui è intrinsecamente criminale usare TOR per rendere anonima la propria identità in rete. Come si è descritto nel primo capitolo, i sistemi di anonimato sono utilizzati anche da persone che vivono sotto regimi repressivi nei quali TOR può rappresentare l'unico modo di dare voce a chi non ne ha la possibilità.

Considerando la questione da un'altra prospettiva si può affermare senza dubbio che, essendo l'anonimato offerto a chiunque, non esiste un modo chiaro per ordinare e dividere i criminali dagli utenti innocenti.

Per quanto sia difficile per le forze dell'ordine ritenere qualcuno responsabile delle proprie azioni senza conoscerne l'identità, è allo stesso modo difficile smascherare una singola persona in rete senza dover de-anonimizzare tutti gli altri utenti di TOR<sup>414</sup>.

---

<sup>411</sup> Chertoff Micheal, *A public policy perspective of the Dark Web*, Journal of Cyber Policy, 2017.

<sup>412</sup> Ibid.

<sup>413</sup> Ibid.

<sup>414</sup> Ibid.

Da qui si sono sviluppate discussioni sull'uso di strumenti disciplinari riguardanti le reti anonime che appaiono decisamente orientate verso posizioni contrastanti<sup>415</sup>.

Uno dei ragionamenti affrontati per cercare di dare una risposta al problema riguarda il bilanciamento dei costi-benefici delle reti anonime<sup>416</sup>.

L'uso di TOR in occidente negli ultimi anni è aumentato specialmente dopo le vicende legate a Cambridge Analytica e alla compravendita dei dati relative alle ricerche online degli utenti per scopi commerciali<sup>417</sup>. Nonostante ciò, chi volesse navigare in maniera anonima può sfruttare reti VPN e altri motori di ricerca privati che offrono la possibilità di farlo in maniera semplice e sicura; senza imbattersi in lati della rete accessibili solo attraverso i siti *.onion*. Pertanto, la necessità di utilizzare un sistema di anonimato completo come TOR, nei paesi liberaldemocratici, è limitata. Questo anche grazie alla presenza di costituzioni e di diritti fondamentali del cittadino che, malgrado le ingerenze nelle banche dati avvenute negli Stati Uniti lo scorso anno<sup>418</sup>, proteggono la salvaguardia delle ricerche in rete e la privacy degli utenti.

Specialmente le democrazie occidentali, che hanno voluto sviluppare ed ospitare gran parte della rete TOR, stanno avendo a che fare con la maggior parte delle conseguenze negative della *onion routing*, rispetto ad altre parti del mondo<sup>419</sup>. Tali negatività, descritte abbondantemente nel capitolo precedente, vanno dal proliferare di materiale pedopornografico in rete, ai commerci illeciti fino alle attività di riciclaggio di denaro online che rappresentano fonti importanti di guadagno per le organizzazioni criminali presenti sul territorio.

Se il quadro di riferimento viene spostato sui costi-benefici netti di TOR in un paese con leggi altamente repressive il risultato finale cambia radicalmente<sup>420</sup>. Le reti di anonimato come TOR, in regimi privi di diritti politici, sono decisamente più vantaggiose non solo per i dissidenti ma anche per giornalisti, attivisti per i diritti umani e semplici cittadini.

Da tali ragionamenti viene alla luce che i costi-benefici non sono distribuiti uniformemente a livello globale.

La decisione delle politiche pubbliche occidentali potrebbe essere quella di limitare l'uso di TOR nei propri paesi, andando così a danneggiarne l'utilizzo in altre zone del mondo, essendo la maggior parte dell'infrastruttura (computer e server) residente nelle democrazie liberali<sup>421</sup>. Inoltre, anche se

---

<sup>415</sup> Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, Paper of The Global Commission for Internet Governance 2015.

<sup>416</sup> Ibid.

<sup>417</sup> Si veda il link: [https://motherboard.vice.com/en\\_us/article/538kqn/heres-the-data-republicans-just-allowed-isps-to-sell-without-your-consent](https://motherboard.vice.com/en_us/article/538kqn/heres-the-data-republicans-just-allowed-isps-to-sell-without-your-consent)

<sup>418</sup> Ibid., a tal riferimento si vedano le considerazioni affrontate nel par. 1 Capitolo I di questo lavoro.

<sup>419</sup> Ibid. Eric Jardine, 2015.

<sup>420</sup> Ibid.

<sup>421</sup> Ibid.

ci fosse un accordo per bloccare le reti di TOR, proprio per la sua tecnologia intrinseca basata su più server, l'operazione sarebbe impossibile ed accrescerebbe comunque la possibile creazione di piattaforme alternative basate sul protocollo di *onion routing*<sup>422</sup>.

In un periodo storico nel quale ci si accinge verso la protezione dei dati personali<sup>423</sup>, piuttosto che cercare correzioni rapide e definitive (come quelle sopra accennate) un altro modo realistico di procedere è quello di concentrarsi attivamente sia sul rafforzamento della normativa in materia che sul migliorare la vigilanza in rete, nel rispetto dei diritti fondamentali del cittadino.

Nonostante il lavoro svolto dalle forze dell'ordine nei diversi paesi per limitare il proliferare del crimine in rete, esistono dei limiti all'efficacia delle operazioni di polizia che azioni politiche, finalizzate a regolamentare, possono senza dubbio superare. Uno dei limiti è rappresentato dal fatto che le organizzazioni criminali agenti in rete possono essere globali, mentre la maggior parte delle forze dell'ordine (tranne l'Interpol, che non ha veri poteri operativi) sono locali. Se un criminale agisce in una giurisdizione nella quale le azioni da lui perpetrate non vengono considerate rilevanti da un punto di vista penale, sarà complesso agire contro quest'ultimo, specialmente se utilizza TOR che fa rimbalzare il segnale in più parti del mondo, coinvolgendo così più giurisdizioni.

L'auspicio delle Nazioni Unite a Salvador ha avuto scarsi risultati dal punto di vista dell'applicazione pratica e nonostante il lavoro dell'EC3 di Europol nel cercare di informare gli Stati sullo sviluppo di forme di criminalità organizzata in rete oggi esistono delle lacune normative in materia che non permettono la corretta applicabilità della legge al mondo del crimine informatico.

#### *4.4.3 Possibili strategie d'intervento in tema di diritto penale sostanziale: Unione Europea e Italia*

Oltre alle diverse iniziative intraprese<sup>424</sup>, si deve pensare ad una risposta normativa in senso coercitivo che sappia porre un margine sia all'uso spropositato fatto dai servizi nascosti delle reti oscure che al diffondersi di organizzazioni criminali, tradizionali o meno, nello scenario di rete.

Questo lavoro di tesi pone L'Unione Europea come punto di partenza nella risoluzione di queste problematiche, proponendo un possibile percorso a più livelli attraverso il quale gli Stati membri possano migliorare le proprie legislazioni interne.

Il processo di armonizzazione delle legislazioni nazionali, proveniente dalle istituzioni UE, è lo strumento ideale del diritto comunitario per tracciare tale percorso.

---

<sup>422</sup> Ibid.

<sup>423</sup> In riferimento al Regolamento (UE) 2016/679 e al GDPR, (Regolamento generale sulla protezione dei dati)

<sup>424</sup> Dal Global Complex for Innovation e EC3 di Europol.

Le legislazioni degli Stati membri sono diverse e queste differenze possono ostacolare la realizzazione degli obiettivi previsti dai Trattati. L'armonizzazione è il mezzo attraverso il quale eliminare o ridurre tali disparità<sup>425</sup>.

Fin dal Trattato di Maastricht i temi di giustizia criminale sono stati considerati di dominio esclusivo degli Stati membri, ritenendo marginale il bisogno di armonizzazione del diritto penale.

Dopo più di dieci anni di distanza, per affrontare la sfida della criminalità transfrontaliera, con il Trattato di Lisbona del 2007<sup>426</sup> si è introdotta la possibilità per l'Unione Europea di legiferare in materia penale attraverso l'uso della direttiva; strumento che vincola gli Stati membri al raggiungimento di un determinato risultato, lasciando la possibilità agli organi nazionali di scegliere forma e mezzi con i quali metterla in atto<sup>427</sup>.

L'abolizione della struttura a pilastri del Trattato di Amsterdam ha conferito la possibilità al Parlamento e al Consiglio di diventare decisori anche in materia penale, facendo inoltre rientrare l'Europol nel quadro giuridico dell'Unione. In particolare, al quarto capo del Trattato sul Funzionamento dell'Unione Europea<sup>428</sup>, intitolato "Cooperazione Giudiziaria in Materia Penale", l'art. 82 traccia il quadro di competenze dell'Unione nel campo della procedura penale (come l'ammissibilità reciproca delle prove tra gli Stati membri) e l'art. 83 svolge un compito analogo nel campo del diritto penale sostanziale. Quest'ultimo prevede che l'Unione possa, mediante direttive, dettare "norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni"<sup>429</sup>.

Tra le sfere di criminalità considerate sono presenti nell'articolo: "sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata"<sup>430</sup>.

Fino ad oggi, l'influenza attuale del modello di integrazione europeo per quanto riguarda l'ambito penale è stata limitata e ben al di sotto del potenziale offerto dall'articolo 83 del TFEU<sup>431</sup>. Questo perché ancora manca una vera volontà di armonizzazione giudiziaria in senso ampio estesa a tutti gli Stati membri dell'Unione.

---

<sup>425</sup> Si veda il link: <http://www.dizie.eu/dizionario/armonizzazione/>

<sup>426</sup> Si veda il link: [https://www.ecb.europa.eu/ecb/legal/pdf/it\\_lisbon\\_treaty.pdf](https://www.ecb.europa.eu/ecb/legal/pdf/it_lisbon_treaty.pdf)

<sup>427</sup> TFUE, Trattato sul Funzionamento dell'Unione europea, art. 288 par. 3, Lisbona 2007.

<sup>428</sup> Rinominato e modificato dall'articolo 2 del Trattato di Lisbona del 13 dicembre 2007, si veda il link: <http://www.isaonline.it/mag/UE-Funzionamento.html>

<sup>429</sup> Art. 83 par.1 TFEU, Trattato sul Funzionamento dell'Unione europea, Lisbona 2007.

<sup>430</sup> Ibid.

<sup>431</sup> A. KLIP, European Criminal Law, 3rd Ed., Intersentia 2016.

Oltre il muto riconoscimento, la cooperazione tra forze giudiziarie e di polizia è necessario che a problemi comuni si reagisca con soluzioni comuni, specialmente nell'era del digitale, nella quale i confini nazionali non bastano a contenere le nuove minacce provenienti dalla rete.

In questo lavoro si propongono due ambiti attraverso cui gli organi legislativi dell'Unione possono limitare i problemi di nostro interesse:

- 1) Criminalizzare l'accesso ad alcune aree di TOR, scoraggiando l'accesso della clientela ai *darkmarkets*
- 2) Partendo dalla soluzione italiana dell'art. 416 c.p., armonizzare la legislazione europea in tema di associazioni a delinquere: sia in rete che quando si parli organizzazioni criminali a stampo mafioso.

#### 4.4.3.1 Criminalizzare l'accesso di alcune aree di TOR

Come si è descritto nel primo capitolo, TOR consente agli utenti di creare siti, esattamente al pari di quelli presenti nel web in superficie, funzionando da *server*<sup>432</sup>. Tali servizi nascosti( gli *hidden services*) sono la tecnologia alla base dei *darkmarkets* e delle altre attività commerciali attraverso le quali, criminali più o meno organizzati, svolgono numerosi atti illeciti<sup>433</sup>.

Alla luce delle considerazioni sulle politiche pubbliche precedentemente esposte, le soluzioni di contrasto alle attività nelle Darknet non sono rappresentate dalla chiusura di TOR bensì da una presa di coscienza da parte delle istituzioni degli spazi illeciti della rete.

Questo vorrebbe dire definire giuridicamente sia il concetto di Darknet che di Mercato Nero Online o *Darkmarkets* rendendo, agli occhi dell'ordinamento giuridico, illegale l'accesso a questi spazi della rete.

Oggi agenti delle forze di polizia, sia in Italia che all'estero, per combattere i mercati neri della rete sono costretti a lunghe e costanti attività di monitoraggio cercando di entrare in prima persona a far parte delle "comunità invisibili" aperte nelle Darknet. Fin dalla chiusura del primo Silk Road, gli organi di sicurezza si impegnano nella lotta ai *darkmarkets* attraverso infiltrazioni online, tentativi di intercettazione delle spedizioni e nella ricerca di nuove tecniche di intrusione nei siti *.onion*<sup>434</sup>.

Il problema è che anche una volta dentro o meglio intercettati gli utenti di queste reti<sup>435</sup>, finché non viene provata la compravendita illecita, il fatto di navigarvi non costituisce reato.

---

<sup>432</sup> Si veda il link: <https://www.torproject.org/docs/tor-onion-service.html.en>

<sup>433</sup> Si veda Capitolo III.

<sup>434</sup> Al Jawaheri, Husam, B, Masters, *Deanonymizing TOR Hidden Service Users Through Bitcoin Transaction Analysis*, giugno 2017.

<sup>435</sup> Si riesca in qualche modo a risalire all'IP degli utenti.

L'unico tipo d'accesso sanzionabile previsto dall'ordinamento italiano è quello al materiale pedo-pornografico. Infatti, una volta che un utente scarichi determinato contenuto virtuale o entri all'interno di una piattaforma che offra contenuti di pornografia minorile, l'atto rientrerebbe nel disposto dell'art. 600 quarter 1. "Pornografia virtuale" del codice penale.

I visitatori di blog riguardanti modi attraverso i quali fabbricare diversi tipi di droga o contraffare mezzi di pagamento non sono sanzionati in alcun modo.

Ragion per cui è importante sia a livello nazionale che a livello internazionale che si criminalizzi l'accesso a determinati servizi nascosti in modo che le forze dell'ordine possano avvalersene in fase processuale.

Questa iniziativa, oltre a far prendere consapevolezza alle istituzioni della fiorente economia sotterranea del crimine, scoraggia gli utenti della rete nel navigare in determinati spazi online, ben prima che possano impegnarsi in una transazione.

Mettere in pratica tale intento già soltanto da un punto di vista europeo, potrebbe ridurre notevolmente la clientela dei *darkmarkets* riducendo enormemente gli introiti dei diversi gruppi di criminalità organizzata agenti in rete.

#### 4.3.4.2 Limiti all'operatività del crimine organizzato nelle reti (dal 416 al 416bis c.p.)

Rilegendosi alle osservazioni portate avanti nel secondo capitolo di questo lavoro, si può constatare la forte presenza di diverse forme di criminalità organizzata in rete<sup>436</sup>.

Anche in questo caso esistono però delle difficoltà ad inquadrare in un'ottica penalistica le attività di tali organizzazioni consumate online.

Esistono due sfide principali a livello italiano e comunitario:

- 1) Stabilire il contributo virtuale nell'associazione a delinquere (art. 416 c.p.)
  - 2) Agire a livello europeo perché si assimili nei diversi stati membri l'aggravante mafiosa (art. 416 bis c.p.); in modo da riconoscere la differenza nelle reti di un semplice gruppo organizzato da un'organizzazione tradizionale come quella mafiosa operante in diversi Stati e a più livelli.
- 
- 1) Il concorso necessario di tipo associativo, base fondante su cui si forma la fattispecie di associazione a delinquere nell'ordinamento italiano, è il risultato della cooperazione volontaria di più persone nel reato<sup>437</sup>.

---

<sup>436</sup> In riferimento al crimine organizzato in rete, si vedano gli studi: McGuire, M., *Organized Crime in the Digital Age*. London: John Greive Center for Policing and Aecurity, 2012, & IOCTA 2014/2018.

<sup>437</sup> Pellissero, Grosso, *Manuale di Diritto Penale*, parte generale, seconda edizione, Giuffrè Editore, 2017.

Spunti di riflessione vengono offerti dall'imputazione di associazione a delinquere laddove la stessa fosse desunta esclusivamente da rapporti nel contesto virtuale ovvero rispetto a soggetti che hanno contatti tra loro esclusivamente in rete. Tali soggetti compiono condotte soltanto attraverso piattaforme telematiche create per delinquere, come possono essere i Darkmarkets ed altri servizi *.onion*.

Essendo l'art. 416 c.p. scritto in un'epoca in cui non esistevano le comunicazioni digitali, appaiono oggi incerti i criteri da utilizzare per verificarne l'applicazione nel contesto virtuale.

Un primo problema si riscontra nel momento in cui forze dell'ordine o altri organi di scurezza si impegnano nell'individuazione degli associati, che nel rispetto della norma devono essere almeno tre. Essendo di per sé già complessa l'identificazione dei colpevoli grazie alle tecniche di anonimato sfruttate, anche nel caso si riuscisse a risalire al sistema operativo di partenza si dovrebbe comunque cercare di capire chi ci fosse dietro al momento della commissione del crimine.

Un secondo problema è quello di dimostrare, in ambito virtuale, la volontà di far parte in modo permanente dell'associazione con la consapevolezza di perseguire comuni obbiettivi criminosi. Nel più dei casi amministratori e suddetti delle piattaforme commerciali presenti nel dark web non hanno alcun legame di conoscenza tra loro e dimostrare la compartecipazione può rivelarsi impresa ardua. Riuscire in questi scopi è frutto di una complessa ed articolata attività investigativa, spesso transnazionale, non sempre accompagnata da un giusto contesto giuridico e tecnico che consentirebbe di cristallizzare tutte le prove in maniera adeguata e completa.

È necessario così integrare le disposizioni previste dall'articolo 416 c.p. per far sì che possano applicarsi anche al contesto virtuale. Se i nostri sistemi operativi diventano "domicili"<sup>438</sup> è giusto responsabilizzare i proprietari nel controllarli.

I nuovi mezzi digitali che forniscono l'accesso alla rete sono potenziali armi attraverso le quali gruppi organizzati possono commettere frodi telematiche, accessi abusivi o pubblicare materiale pedo-pornografico, ed è giusto che siano ricollegabili al legittimo proprietario responsabile.

La Sentenza più celebre in quest'ambito, ed anche una delle prime che ha scatenato il dibattito sull'integrazione dell'associazione a delinquere in senso "virtuale", è stata la n.

---

<sup>438</sup> In riferimento al reato di accesso abusivo, punibile con la reclusione fino a tre anni. La Cassazione esprime a riguardo che la violazione di un sistema informatico è pari alla violazione di domicilio ( Cass.Sent. 36338/2015, in riferimento ad art. 615 ter Codice penale, Accesso abusivo ad un sistema informatico o telematico)

1872 del 21 settembre 2005<sup>439</sup> del Tribunale di Roma che si è pronunciata su un caso riguardante un gruppo coinvolto nella pubblicazione di materiale pedo-pornografico:

“Il Tribunale ha ritenuto che tale reato è, in astratto, configurabile anche nell’ambito di una comunità virtuale quale quella dell’Internet quando si abbia a che fare con un’organizzazione stabilmente dedita alla commercializzazione e distribuzione di immagini oscene e ricorra la volontà degli aderenti al *consortium sceleris* di partecipare all’attività in questione. Nel caso di specie pur essendo emerso un collegamento stabile tra alcuni imputati, non risulta sufficientemente provata la compartecipazione a un continuativo programma delittuoso.”<sup>440</sup>

Gruppi ben organizzati con una forte struttura gerarchica, come gli “hub” di McGuire<sup>441</sup>, ancora oggi sfuggono all’imputazione del reato di associazione a delinquere, proprio per l’assenza di regole definite in materia.

- 2) In Europa il contrasto delle associazioni a delinquere a stampo mafioso resta ancora un tema dibattuto ed in via d’evoluzione<sup>442</sup>.

Sin dall’entrata in vigore del Trattato di Lisbona gli organi istituzionali europei pensano ad una risposta comune da dare al problema del rafforzamento della criminalità organizzata operante su scala transfrontaliera<sup>443</sup>.

Il punto di partenza di un eventuale risposta ha origine dai disposti forniti dall’ordinamento italiano in materia penale, in particolare dall’art.416 bis c.p. che istituisce l’associazione a delinquere a stampo mafioso<sup>444</sup>.

Come si è ricordato nel secondo capitolo, le diverse legislazioni europee mancano di un corpus normativo riguardante questo particolare genere di criminalità organizzata; una mancanza che rappresenta un ostacolo alle indagini su le forme di associazione mafiosa sia a livello italiano che a livello internazionale<sup>445</sup>.

---

<sup>439</sup> Il tribunale Penale di Roma, Sezione 9°, 21/09/2005, si veda il link: <http://www.penale.it/page.asp?mode=1&IDPag=97>

<sup>440</sup> Ibid.

<sup>441</sup> Si veda Capitolo II.

<sup>442</sup> Si veda il link: <https://www.ilfattoquotidiano.it/2016/10/26/mafie-in-europa-ok-del-parlamento-ue-alla-risoluzione-ferrara-m5s-piu-vicino-il-reato-comune-di-associazione-mafiosa/3121385/>

<sup>443</sup> Si veda Capitolo II.

<sup>444</sup> Parlamento Europeo, *Relazione sulla lotta contro la corruzione e il seguito dato alla risoluzione della commissione CRIM*, 2016.

<sup>445</sup> In riferimento al contrasto di Europol/Interpol ad associazioni come Cosa Nostra o la ‘Ndrangheta .

Calandosi nel contesto del digitale, come si è analizzato in questo lavoro<sup>446</sup>, le organizzazioni criminali tradizionali operano nella rete con il fine di alimentare i propri guadagni allargando la portata dei mercati illeciti nel mondo virtuale.

Vista la “Valutazione della minaccia della criminalità organizzata su Internet” (IOCTA), elaborate da Europol<sup>447</sup> e le conseguenti valutazioni sulle gravi forme di criminalità organizzata presenti in Europa<sup>448</sup> è necessario che le legislazioni interne adattino piani normativi conformi nel distinguere associazioni a delinquere operanti in rete (come possono essere gli *hub*<sup>449</sup>) da organizzazioni criminali operanti nella rete per migliorare le attività illecite offline (come quelle mafiose). Seguendo l’esempio proposto dal professor Micheal McGuire nel 2012<sup>450</sup>, si dovrebbe creare da un punto di vista legislativo la divisione in dei tre gruppi di criminalità organizzata agenti in rete: quelli operanti esclusivamente online (come gli hub), gli ibridi e le forme di criminalità organizzata tradizionale.

Il 25 ottobre del 2016 il Parlamento Europeo ha proposto il tema di creare un quadro legislativo più forte in tema di criminalità organizzata, invitando la Commissione a redigere un disegno legislativo che migliori la cooperazione giudiziaria transfrontaliera in materia<sup>451</sup>.

L’obiettivo è quello di legiferare in ambito di norme minime comuni, specie dove non esiste già il reato di associazione a delinquere, per perseguire le stesse condotte sul territorio<sup>452</sup>.

Si attende che la Commissione rediga un testo da presentare in seduta plenaria che, se approvato, può essere presentato in forma di direttiva alle diverse legislazioni degli Stati membri.

Rafforzare le norme in tema di crimine organizzato vorrebbe dire agire in maniera anche più propria nei confronti delle forme di criminalità presenti in rete.

Solo attraverso un corpo legislativo uniforme che coinvolga gli Stati dell’eurozona, forze dell’ordine ed altri organi di sicurezza possono operare nel combattere l’economia del crimine organizzato online che, attraverso l’uso delle comunicazioni telematiche, si espande oltre i confini nazionali e a livello globale.

---

<sup>446</sup> Si veda Capitolo III.

<sup>447</sup> Si veda il link: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015>

<sup>448</sup> In riferimento al SOCTA, si veda il link: <https://www.europol.europa.eu/activities-services/main-reports/serious-and-organised-crime-threat-assessment>

<sup>449</sup> In riferimento al gruppo di McGuire, si veda Capitolo II.

<sup>450</sup> Ibid. McGuire, 2012, si veda Capitolo II.

<sup>451</sup> Risoluzione del Parlamento europeo del 25 ottobre 2016 sulla lotta contro la corruzione e il seguito dato alla risoluzione della commissione CRIM (2015/2110(INI)), si veda il link: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0403+0+DOC+XML+V0//IT>

<sup>452</sup> Ibid.

#### 4.5 L'ambito del Cybericiclaggio

Come abbiamo descritto nel terzo capitolo, la vera rivoluzione offerta da Internet nel campo dei sistemi di pagamento è rappresentata dall'introduzione del "denaro elettronico" e della "moneta virtuale"<sup>453</sup>.

Ben prima dello sviluppo delle cripto-valute il riciclaggio di denaro, evoluto nell'era digitale, si era configurato come un fenomeno transnazionale<sup>454</sup> facendo sì che le azioni di contrasto assumessero un carattere sistematico e globale<sup>455</sup>.

Nel seguente paragrafo si affronterà l'approccio internazionale del GAFI nella lotta al cybericiclaggio, per poi passare a descrivere lo scenario normativo europeo e nazionale. Si inquadreranno i punti salienti dell'evoluzione del diritto nell'ambito del riciclaggio di denaro relazionato all'uso della moneta elettronica prima e delle cripto-valute dopo.

Il semi-anonimato delle monete virtuali ha facilitato nuove vie al riciclaggio rendendo il fenomeno soggetto ad ulteriori regolamentazioni a più livelli. Oggi, grazie alle nuove direttive antiriciclaggio e ai progressi apportati a livello nazionale, si ha modo di limitare lo sviluppo dell'uso di cripto-valute nel processo di riciclaggio di denaro, le cui tecniche sono continuamente in evoluzione.

##### 4.5.1 L'azione Internazionale: il GAFI

Il Gruppo di Azione Finanziaria Internazionale (GAFI), è ampiamente riconosciuto per rappresentare il fulcro globale delle politiche antiriciclaggio<sup>456</sup>. Le Quaranta raccomandazioni<sup>457</sup> sviluppate nel 1990 insieme alle ulteriori 9 raccomandazioni<sup>458</sup> promulgate all'indomani degli attacchi dell'11 settembre del 2001, sono considerate come le principali norme a livello internazionale che promuovono un approccio comune alle politiche di antiriciclaggio. Nelle presenti raccomandazioni si evince l'esigenza di creare un sistema nazionale antiriciclaggio efficace incentrato sul coordinamento tra gli istituti finanziari e le autorità giudiziarie, sollecitando gli stati

---

<sup>453</sup> G. Lemme, *Pag 12, Moneta scritturale e moneta elettronica*, Giappichelli editore, 2003.

<sup>454</sup> A.M. Stile, *Riciclaggio e reimpiego di proventi illeciti*, 2009, si veda il link: [http://www.treccani.it/enciclopedia/riciclaggio-e-reimpiego-di-proventi-illeciti\\_%28XXI-Secolo%29/](http://www.treccani.it/enciclopedia/riciclaggio-e-reimpiego-di-proventi-illeciti_%28XXI-Secolo%29/)

<sup>455</sup> Ibid.

<sup>456</sup> Jacobi, A.P. "The FATF as the central promoter of the anti-money laundering regime", In *Securitization, Accountability and Risk Management. Transforming the Public Security Domain*, London: Routledge, 2012.

<sup>457</sup> GAFI, 40 raccomandazioni, 1990, Si veda il link: <http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf>

<sup>458</sup> GAFI, 9 raccomandazioni Si veda il link: <http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IIX%20Special%20Recommendations%20and%20IN%20orc.pdf>

membri<sup>459</sup> a riconoscere il reato di riciclaggio al fine di attuare le norme cautelari o confische di patrimoni sospetti<sup>460</sup>.

Tale approccio decentralizzato, basato su raccomandazioni, forum e pareri è stato applicato anche alle cripto-valute<sup>461</sup>. In una serie di rapporti tra il 2013 e il 2014 il GAFI ha segnalato la pericolosità rappresentata dalle cripto-valute nell'ambito del riciclaggio di denaro, identificando una mancanza di chiarezza nella *governance* del fenomeno<sup>462</sup>. Nel 2015 è stata pubblicata un'ulteriore versione aggiornata delle raccomandazioni<sup>463</sup> contenente il duplice scopo di aiutare diversi istituti<sup>464</sup> a identificare e agire nei confronti delle minacce di riciclaggio di denaro poste dalle cripto-valute. L'intento parallelo è quello di aiutare le autorità nazionali nello sviluppare quadri normativi standard per sostenere gli sforzi delle politiche globali antiriciclaggio<sup>465</sup>. Nella raccomandazione il GAFI suggerisce che le autorità nazionali istituiscano "meccanismi di coordinamento"<sup>466</sup> per condividere in modo proattivo informazioni in maniera che possano promuovere una più profonda comprensione dei rischi dell'ecosistema del riciclaggio di denaro relazionato all'uso delle cripto-valute<sup>467</sup>. In secondo luogo, si suggerisce alle autorità dei diversi paesi di mirare più che ai singoli utenti e ai fornitori di cripto-valute, al regolamentare istituti e intermediari finanziari i quali rappresentano un alto rischio di coinvolgimento nel riciclaggio di denaro poiché hanno la possibilità di "inviare, ricevere e archiviare" cripto-valuta<sup>468</sup>.

L'efficacia del GAFI e le sue raccomandazioni non obbligatorie sono state a lungo oggetto di dibattito accademico<sup>469</sup>, essendo ritenute da molti studiosi come deboli strumenti di contrapposizione<sup>470</sup> ad un problema così ingente come quello della relazione tra il riciclaggio di denaro e le tecnologie computerizzate. Da diversi paesi si sono pensate soluzioni come la creazione di sistemi di cripto-valuta nazionale gestiti ed erogati da enti governativi<sup>471</sup>. Eppure, la

---

<sup>459</sup> I membri del GAFI sono 38 (si veda il link: <http://www.fatf-gafi.org/about/membersandobservers/>) e come osservatori rilevanti organismi finanziari internazionali e del settore (tra i quali Nazioni unite, Fondo monetario internazionale, Banca mondiale, Banca centrale europea ed Europol,).

<sup>460</sup> 40 raccomandazioni, 1990, Ibid.

<sup>461</sup> Malcolm Campbell-Verduyn, Bitcoin, crypto-coins, and global anti-money laundering governance, gennaio 2018.

<sup>462</sup> GAFI. Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, 2013 e GAFI, Virtual Currencies: Key Definitions and Potential AML/CFT Risks: FATF Report, 2014.

<sup>463</sup> GAFI. Guidance for a Risk-Based Approach: Virtual Currencies, giugno 2015, si veda il link: <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

<sup>464</sup> Banche e altri istituti finanziari

<sup>465</sup> Ibid.

<sup>466</sup> Ibid.

<sup>467</sup> P.8 Ibid.

<sup>468</sup> Ibid.

<sup>469</sup> Zoppi, V. *Money Laundering: A New Perspective in Assessing the Effectiveness of the AML Regime. The European Review of Organised Crime* 2015.

<sup>470</sup> Ibid.

<sup>471</sup> Spaven, E. *UK Government Should Create Own Digital Currency. CoinDesk*, Maggio 2015.

competizione di mercato degli Altcoin si dimostra molto alta, tanto che per alcuni l'iniziativa della moneta di stato è inefficace<sup>472</sup>, in quanto i riciclatori userebbero le monete virtuali alternative.

L'approccio regolatorio del GAFI ha fatto sì che istituzioni finanziarie, organi istituzionali e altri intermediari fossero scoraggiati nell'uso delle cripto-valute.

Conseguentemente molte delle critiche provengono dagli organi finanziari in appoggio delle cripto-valute, sostenendo che una regolamentazione di queste ne accompagnerebbe l'uso verso realtà finanziarie "sotterranee" ed illegali, le quali rimangono immuni dall'intervento dei regolatori<sup>473</sup>. Realtà industriali come la Digital Finance Institute<sup>474</sup> si sono unite alle critiche affermando che l'approccio del GAFI condurrebbe le istituzioni del mondo finanziario ad evitare l'impegno con gli operatori di servizi di cripto-valute<sup>475</sup>.

Nonostante i suoi limiti, l'iniziativa del 2015 del GAFI si è concentrata sulle istituzioni centralizzate che scambiano cripto-valuta in moneta statale, cercando di sensibilizzare le istituzioni dei diversi paesi ad applicare norme tese alla regolamentazione. Anche un approccio non basato su un apporto di norme coercitive in materia, come quello internazionale proposto dal GAFI, può essere vincente nel momento in cui si va ad occupare di un ambito così decentralizzato come le cripto-valute, incentivando Stati e organizzazioni regionali ad agire in maniera propria nei singoli ordinamenti.

#### 4.5.2 Le Direttive Europee

Un primo tipo di attività disciplinare posto a limitare l'espansione del fenomeno del riciclaggio attraverso l'uso della rete e dei sistemi computerizzati è la Direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno dell'UE, che stabilisce norme per i servizi di pagamento quali bonifici, addebiti diretti e pagamenti con carta<sup>476</sup>. La direttiva aveva il duplice scopo di rendere uniforme i servizi di pagamento e introdurre una nuova figura di intermediario finanziario specializzato nell'offerta di servizi di pagamento: l'istituto di pagamento (IP). La delicata funzione di questo nuovo tipo di istituto è tracciare i flussi finanziari intermediari e quindi conoscere e ricostruire la loro provenienza e destinazione. In Italia gli IP sono pertanto tenuti a eseguire l'adeguata verifica della clientela con la quale operano, a effettuare le registrazioni nell'Archivio

---

<sup>472</sup> Cohen, B. The IPE of money revisited. *Review of International Political Economy*, p. 24, 2016.

<sup>473</sup> Ibid. Campbell-Verduyn 2018.

<sup>474</sup> Si veda il link: [http://www.digitalfinanceinstitute.org/?page\\_id=892](http://www.digitalfinanceinstitute.org/?page_id=892)

<sup>475</sup> Ibid. Campbell-Verduyn 2018.

<sup>476</sup> Si veda il link: <https://eur-lex.europa.eu/legalcontent/IT/TXT/HTML/?uri=LEGISSUM:l33226&from=EN>

Unico Informatico<sup>477</sup> e a segnalare le operazioni sospette all'Unità di Informazione Finanziaria. Anche detta UIF l'Unità è stata istituita già dal 2007, dal decreto legislativo, n. 231 presso la Banca d'Italia in posizione di indipendenza e autonomia funzionale, ha iniziato a operare il 1° gennaio 2008, subentrando all'Ufficio italiano dei cambi (UIC) nel ruolo di autorità centrale antiriciclaggio<sup>478</sup>.

“Gli agenti degli IP sono destinatari diretti degli obblighi antiriciclaggio; essi sono tenuti a effettuare l'adeguata verifica della clientela anche in relazione a operazioni di importo inferiore a € 15.000. Gli obblighi di registrazione vengono assolti attraverso la trasmissione dei dati necessari all'IP per il quale operano, che a sua volta li registra nell'Archivio. Gli agenti comunicano le operazioni sospette al proprio IP, che poi provvede ad effettuare la segnalazione<sup>479</sup>”. Ai sensi della direttiva con l'avvento delle cripto-valute, non essendoci di norma un ente centrale che ne ha la proprietà e il controllo, queste non possono neanche essere definite come istituto di pagamento, che comunque traccia le transazioni di monete elettroniche.

Da un riesame del quadro europeo emerse nell'arco degli anni il crescente problema del riciclaggio a livello internazionale venne così pubblicata un'ulteriore Direttiva la 2015/849<sup>480</sup>, datata al 20 maggio, anche detta quarta direttiva antiriciclaggio. Questa afferma ufficialmente l'importanza di applicare misure altamente restrittive e di controllo per sistemi sviluppati tramite l'utilizzo di internet. La Direttiva introduce diverse innovazioni tra cui disposizioni più stringenti nei trasferimenti elettronici di fondi eseguiti al di fuori del sistema dell'Unione Europea<sup>481</sup>. Inoltre, sono presenti l'applicazione delle norme sull'adeguata verifica nell'ambito della prestazione di servizi di pagamento e di emissione e distribuzione di moneta elettronica anche per operazioni di importo inferiore a 15.000 euro<sup>482</sup>. Nello stesso anno la Corte di Giustizia dell'Unione Europea, con la sentenza 22 ottobre 2015, causa C-264/14 in relazione alle operazioni di cambio tra bitcoins e valuta a corso legale o di utilizzo dei bitcoins quale mezzo di pagamento, ne ha stabilito la natura di servizi ricadenti sotto l'esenzione IVA<sup>483</sup>.

---

<sup>477</sup> L'Archivio Unico Informatico (AUI), è l'organo teso alla registrazione ed il tracciamento di operazioni monetarie con importo pari o superiore ai 15.000 euro, siano esse singole o frazionate. Previsto dall'art. 37 del Decreto legislativo 231/2007, costituisce lo strumento principale nell'azione prescritta dalle Autorità di Vigilanza per il rispetto degli obblighi di adeguata verifica della clientela degli intermediari finanziari.

<sup>478</sup> Si veda il link: <http://uif.bancaditalia.it/sistema-antiriciclaggio/uif-italia/>

<sup>479</sup> Commissione VI della Camera dei Deputati (Finanze), cit. da: “Gli Istituti di pagamento in Italia” Audizione del Direttore Centrale per la Vigilanza Bancaria e Finanziaria della Banca d'Italia Stefano Mieli, ottobre 2011, disponibile al link: [https://www.bancaditalia.it/pubblicazioni/interventi-vari/int-var-2011/Istituti\\_pagamento\\_Italia..pdf](https://www.bancaditalia.it/pubblicazioni/interventi-vari/int-var-2011/Istituti_pagamento_Italia..pdf)

<sup>480</sup> Si veda il link: <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32015L0849>

<sup>481</sup> Ibid.

<sup>482</sup> Ibid.

<sup>483</sup> Corte di Giustizia UE, Quinta Sezione, sentenza 22 ottobre 2015, *causa C-264/14* (\*), si veda il link: [http://www.dirittoegiustizia.it/allegati/17/0000071427/Corte\\_di\\_Giustizia\\_UE\\_Quinta\\_Sezione\\_sentenza\\_22\\_ottobre\\_2015\\_causa\\_C\\_264\\_14.html](http://www.dirittoegiustizia.it/allegati/17/0000071427/Corte_di_Giustizia_UE_Quinta_Sezione_sentenza_22_ottobre_2015_causa_C_264_14.html)

Nonostante l'EBA (European Banking Authority), aveva precisato di non considerare la valuta virtuale un'autentica forma di moneta<sup>484</sup>, la sentenza considera il bitcoin quale "mezzo di pagamento contrattuale"<sup>485</sup>.

Al passo con i nuovi cambiamenti apportati dai nuovi metodi di pagamento, il 30 maggio del 2018 il Parlamento ed il Consiglio Europeo, hanno adottato un'ulteriore direttiva, la n. 843<sup>486</sup>. Ben consapevoli del miglioramento già avvenuto nel corso degli ultimi anni, a livello di Stati membri, sul fronte dell'adozione e dell'applicazione delle norme del gruppo di azione finanziaria internazionale (GAFI)<sup>487</sup>, Parlamento e Consiglio esprimono attraverso la nuova direttiva la volontà di rafforzare le norme dell'Unione Europea in tema di antiriciclaggio, modificando la quarta del 2015 ed aggiungendo le cripto-valute al sistema di regolamentazione. Rispetto al passato la direttiva aumenta lo spettro dei soggetti obbligati includendovi i prestatori di servizi di cambio tra valute virtuali e valute aventi corso legale<sup>488</sup> (ossia gli *exchange provider* ed *exchange platform* nella più ampia accezione) ed aggiungendo particolari obblighi antiriciclaggio ai prestatori di servizi di portafoglio digitale, che non sono soggetti all'obbligo della UE di individuare le attività sospette<sup>489</sup>. Si va in questo modo ad allargare le disposizioni poste dalla n.849 del 2015, coinvolgendo nell'obbligo le cripto-valute, ben distinte da altri tipi di trasferimento elettronico<sup>490</sup>, il cui anonimato, come si è discusso in questo lavoro, ne consente usi per scopi criminali. In questo modo le autorità competenti avranno la possibilità di monitorare, attraverso i soggetti obbligati, anche l'uso delle valute virtuali<sup>491</sup>. Nelle categorie di obbligati della direttiva sono ascrivibili ciò che il legislatore comunitario individuerà come soggetti che forniscono "servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali<sup>492</sup>". All'atto pratico tali soggetti, meglio conosciuti come *wallet provider*, dovranno incaricarsi di effettuare l'adeguata verifica in fase (almeno) di registrazione dell'utente. La direttiva definisce chiaramente il "prestatore di servizi di portafoglio digitale" quale soggetto che fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali<sup>493</sup>.

---

<sup>484</sup> EBA Opinion on 'virtual currencies', 4 luglio 2014, si veda link: <https://eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>

<sup>485</sup> Punto 42, sentenza 22 ottobre 2015 Ibid.

<sup>486</sup> Ibid.

<sup>487</sup> Direttiva 2018/843, Si veda il link: <http://www.giurisprudenzapenale.com/wp-content/uploads/2018/08/V-Direttiva-Europea-Antiriciclaggio-.pdf>

<sup>488</sup> per esempio, monete e banconote considerate a corso legale e la moneta elettronica di un paese, accettate quale mezzo di scambio nel paese emittente.

<sup>489</sup> Ibid. Direttiva 2018/843.

<sup>490</sup> Modifica dell'art. 3 (d), punto 16 e 18, Direttiva 2018/843.

<sup>491</sup> Ibid. Direttiva 2018/843.

<sup>492</sup> Ibid.

<sup>493</sup> Ibid.

Come riportato nella Direttiva<sup>494</sup>, l'inclusione dei prestatori di servizi di cambio in cripto-valuta e di portafoglio digitale non risolve completamente il problema dell'anonimato poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, lasciando anonimo gran parte dell'ambiente delle valute virtuali<sup>495</sup>. “Per contrastare i rischi legati all'anonimato, le Unità Nazionali di Informazione Finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate<sup>496</sup>”.

La direttiva, nonostante sia rilevante ai fini dello Spazio Economico Europeo<sup>497</sup>, rappresenta un enorme passo avanti nell'ambito dei limiti posti dal cybericiclaggio, andando a regolamentare degli istituti, che prima di quest'intervento, erano parte fondamentale nel percorso di “ripulitura” dei proventi attraverso cripto-valute<sup>498</sup>.

#### 4.5.3 L'Ordinamento Nazionale

La differenza da sottolineare nell'ordinamento penale italiano in materia è quella tra il reato di riciclaggio, art.648 bis c.p., e autoriciclaggio art. 648 1.ter c.p.

La differenza tra le due fattispecie consiste sostanzialmente nella presenza necessaria di un terzo soggetto che assume su di sé l'azione di sostituzione o di impiego di denaro proveniente da attività illecite. In altre parole, l'art. 648-bis c.p. è finalizzato a sanzionare il soggetto estraneo che autonomamente contribuisce al consolidamento del patrimonio illecitamente acquisito<sup>499</sup>. Tale soggetto in quanto estraneo non deve aver preso parte al reato presupposto, ovvero al fatto criminoso che ha generato quei proventi, mentre il reato di autoriciclaggio, introdotto dal primo gennaio del 2015<sup>500</sup>, punisce colui che compie l'attività tipica del riciclaggio sui beni tratti da delitti da lui stesso commessi.

In Italia la normativa antiriciclaggio ha una storia trentennale<sup>501</sup>, con numerosi organi di garanzia dediti al controllo del fenomeno, le così chiamate autorità di vigilanza, stabilite d.lgs. n. 231/2007,

---

<sup>494</sup> Punto (9) della Direttiva 2018/843.

<sup>495</sup> Ibid.

<sup>496</sup> Ibid.

<sup>497</sup> Istituito nel 1994, lo Spazio economico europeo estende le disposizioni applicate dall'Unione europea al proprio mercato interno ai paesi dell'Associazione europea di libero scambio (EFTA). Attualmente lo SEE comprende i Paesi dell'UE, l'Islanda, il Liechtenstein e la Norvegia (la Svizzera fa parte dell'EFTA ma non del SEE).

<sup>498</sup> Si veda capitolo III.

<sup>499</sup> G. Nanulla, *pag. 319, cit* La lotta alla mafia, 1992.

<sup>500</sup> L.n.186, 15 dicembre 2014.

<sup>501</sup> Il recepimento della prima direttiva comunitaria in Italia avvenne attraverso la normativa contenuta nel D.L. 3 maggio 1991, n. 143, convertito, con modifiche, nella L. 5 luglio 1991, n. 197, recante provvedimenti urgenti per

tra cui: il MEF, il Ministero dell'economia e delle finanze (art.5) la già citata UIF disciplinata dal regolamento della Banca d'Italia (art. 6), le Autorità di vigilanza di settore (art. 7) come Banca d'Italia, Consob<sup>502</sup>, IVASS<sup>503</sup>, il Ministero di Giustizia, forze di polizia (in particolare Guardia di Finanza e la Direzione Nazionale Antimafia) e Ordini professionali (art.8 e 9)<sup>504</sup>.

La Direttiva 2007/64/CE è stata recepita nell'ordinamento attraverso l'introduzione del d.lgs. 11 del 2010 e integrazioni al Testo Unico Bancario (TUB)<sup>505</sup>, stabilendo gli istituti di pagamento descritti nel paragrafo precedente.

Nel rapporto annuale UIF<sup>506</sup> del 2014 si sottolinea come dalle ricerche svolte a livello internazionale emergerebbe che la maggior parte delle unità di cripto-valuta sarebbe detenuta per fini speculativi; l'anonimato che caratterizza le transazioni, facilitando la possibile elusione di vincoli normativi al trasferimento di fondi, renderebbe inoltre questa valuta virtuale utilizzabile per finalità illecite<sup>507</sup>.

Nel momento così, in cui si è arrivati a parlare di cybericiclaggio, per la giurisprudenza nostrana, assimilare le cripto-valute al denaro corrente, sarebbe considerato, in assenza di una definizione propria nel diritto, un'illecita estensione della punibilità, in violazione del divieto di analogia in materia penale<sup>508</sup>. Con il progressivo ampliamento dei reati di presupposto, della condotta incriminabile e dell'oggetto del reato, il legislatore, utilizzando la locuzione "altre utilità", ha inteso colpire con il delitto di riciclaggio "ogni vantaggio derivante dal compimento del reato presupposto"<sup>509</sup>. Proprio in questo tipo di qualificazione giuridica rientrano le cripto-valute che, essendo considerate "utilità", si conformano perfettamente ai reati di riciclaggio e autoriciclaggio.

---

limitare l'uso del denaro contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio.

<sup>502</sup> La Commissione nazionale per le società e la Borsa, la cui attività è rivolta alla tutela degli investitori, all'efficienza, alla trasparenza e allo sviluppo del mercato mobiliare italiano.

<sup>503</sup> L'Istituto per la vigilanza sulle assicurazioni è un'autorità amministrativa indipendente che esercita la vigilanza sul mercato assicurativo italiano, per garantirne la stabilità e tutelare il consumatore.

<sup>504</sup> Il primo comma dell'articolo 8 dispone, infatti, che gli ordini promuovono e controllano l'osservanza da parte dei professionisti degli obblighi stabiliti dal decreto legislativo. il comma 6 dell'art. 9 prevede che gli ordini professionali devono informare la Uif delle ipotesi di omissione delle segnalazioni di operazioni sospette e di ogni fatto che potrebbe essere correlato a riciclaggio o finanziamento del terrorismo, rilevato nei confronti dei propri iscritti.

<sup>505</sup> Senato della Repubblica e della Camera dei deputati, dossier XVII legislatura, Servizi di Pagamento nel mercato Interno, ottobre 2017, disponibile al link: <https://www.senato.it/service/PDF/PDFServer/BGT/01045451.pdf>

<sup>506</sup> UIF, Relazione annuale del 9 luglio 2014 si veda il link: <http://uif.bancaditalia.it/pubblicazioni/rapporto-annuale/2015/index.html>

<sup>507</sup> Ibid.

<sup>508</sup> L'art. 14 disp.att. esclude il procedimento analogico in caso di leggi penali, tale esclusione si ricava anche dagli artt. 1 c.p. (nessuno può essere punito per un fatto che non sia espressamente preveduto dalla legge come reato) e 199 c.p. (nessuno può essere sottoposto a misure di sicurezza fuori dai casi dalla legge preveduti).

<sup>509</sup> Fabio Di Vizio, *Lo statuto giuridico delle valute virtuali: le discipline e i controlli, Tra oro digitale ed ircocervo indomito*, 2018.

Il decreto legislativo del 25 maggio 2017, n. 90 recependo la direttiva UE 2015/849 (IV direttiva antiriciclaggio), introduce diverse innovazioni anticipando in ambito delle monete virtuali la n. 843/2018.

Il decreto fa due passi importanti nella lotta all'espansione delle cripto-valute nel mondo del riciclaggio di denaro: in primo luogo, offre una definizione di cripto-valuta:

la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente<sup>510</sup>.

In secondo luogo, inserisce tra i soggetti tenuti al rispetto delle regole antiriciclaggio i “prestatori di servizi relativi all'utilizzo di valuta virtuale: (ovvero) ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale<sup>511</sup>”. Disponendo previsioni aggiuntive<sup>512</sup> e i requisiti per l'esercizio dell'attività di cambiavalute applicabili anche ai soggetti prestatori di servizi relativi all'utilizzo di valuta virtuale, li sottopone all'iscrizione in una sezione speciale del registro tenuto dall'Organismo degli Agenti e dei Mediatori<sup>513</sup>, dove vengono raccolti tutti i soggetti non finanziari e autorizzati ad esercitare l'attività di cambiavalute.

A seguito di questo decreto, le imprese dotate di personalità giuridica, tutte le persone giuridiche private e i trust<sup>514</sup> saranno tenuti a comunicare alle autorità i dati relativi alla proprietà e al controllo degli assetti aziendali posseduti, anche se indirettamente, che saranno poi inseriti in apposite sezioni del Registro delle imprese<sup>515</sup>.

---

<sup>510</sup> D.lgs, 25 maggio 2017, n. 90, <http://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg>

<sup>511</sup> Ibid.

<sup>512</sup> “Ai sensi del comma 8 bis, art. 17bis, Dlgs 141/2010, “i prestatori di servizi relativi all'utilizzo di valute virtuali sono tenuti all'iscrizione in una sezione speciale del registro dei cambiavalute”, con conseguenti obblighi antiriciclaggio ai sensi del comma 2, art. 1, lett. ff) e qq), Dlgs 231/2007. Ciò implica, indirettamente, che le E-Coin, pur assimilabili, non sono definite dal Legislatore civilistico mere “valute”, talché non vi sarebbe stata – in quel caso – necessità alcuna di introdurre una sezione speciale se rientrassero tout court nell'alveo dell'oggetto dell'attività dei cambiavalute stessi.” In questo caso si inseriscono i prestatori di servizi di cambio di cripto-valute.

<sup>513</sup> Attività finanziaria che promuove e conclude contratti relativi alla concessione di finanziamenti sotto qualsiasi forma o alla prestazione di servizi di pagamento, su mandato diretto di intermediari finanziari, istituti di pagamento, istituti di moneta elettronica, banche o Poste Italiane. Si veda il link: <https://www.organismo-am.it/>

<sup>514</sup> I trust sono istituti giuridici che consentono di creare un fondo con patrimonio autonomo, amministrato da un fiduciario. Il fondo è creato per iniziativa di un donatore che immette nel fondo beni mobili e immobili dei quali trasferisce la proprietà a un amministratore fiduciario (trustee), tenuto ad agire secondo le istruzioni del primo per il raggiungimento di uno scopo o nell'interesse di un beneficiario.

<sup>515</sup> Ibid. Decreto Legislativo 2017.

Con il decreto, l'Italia diventa così il primo paese europeo a limitare la realtà degli *exchanger*, figura in progressiva espansione nel panorama della rete e di fondamentale importanza per il cybericiclaggio.

#### 4.5.4 Nuove prospettive nello scenario italiano

Alla luce del d.lgs. n. 90/2017 e della successiva direttiva europea, si dovrà sempre più cercare di andare a regolamentare i servizi di cambio di cripto-valuta, che rappresentano l'inizio del percorso d'immissione del denaro sporco nel sistema finanziario.

Intercettare la fase di collocamento<sup>516</sup>, per le forze dell'ordine e le autorità di vigilanza rappresenta la vera opportunità di bloccare l'intento criminale di ripulire i proventi illeciti che, una volta entrati in circolazione nel sistema finanziario, specialmente con l'aiuto delle cripto-valute, diventa impossibile rintracciare.

Nell'ambito della regolamentazione il seguente lavoro cerca di addurre un'osservazione che può rappresentare un ulteriore ostacolo nella lotta al cybericiclaggio, ovvero l'avvento delle nuove valute ad anonimizzazione totale (come Z-cash e Monero).

Attraverso i nuovi mezzi introdotti tesi a limitare i prestatori di servizi di cambio tra cripto-valute e moneta corrente, compresi quelli di portafogli digitali, in riferimento a quelle valute che non utilizzino nuove tecniche di occultamento, la previsione di tracciabilità realizzata dalle autorità di vigilanza appare idonea a garantire un adeguato livello di contenimento del rischio di sfruttamento delle monete virtuali nell'alimentare economie illegali<sup>517</sup>.

Il problema si presenta nel momento in cui le cripto-valute sfruttino metodi aggiuntivi che permettono un anonimato assoluto come Z-Cash che utilizza tecniche avanzate di crittografia chiamata "zero-knowledge proofs"<sup>518</sup>, per garantire la validità della transazione senza però rivelarne informazioni aggiuntive.

Per questo motivo nell'ottobre del 2016, un gruppo di parlamentari ha proposto il disegno di legge n. 4119, intitolato: "Divieto di utilizzo delle cripto-valute che impiegano tecniche di anonimizzazione totale nelle transazioni economiche"<sup>519</sup>. Il presente progetto, andatosi ad arenare nell'arco degli anni seguenti, rappresentava un tentativo di limitare l'esordio delle nuove cripto-valute totalmente anonime che mettono davanti agli organi di controllo un ulteriore scoglio per

---

<sup>516</sup> Si veda capitolo III.

<sup>517</sup> Proposta di Legge, *Divieto di utilizzo delle cripto-valute che impiegano tecniche di anonimizzazione totale nelle transazioni economiche*, Presentata il 26 ottobre 2016. Si veda il link: <http://www.camera.it/dati/leg17/lavori/stampati/pdf/17PDL0060630.pdf>

<sup>518</sup> Si veda Capitolo I.

<sup>519</sup> Ibid. proposta di legge, 2016.

rintracciare le transazioni. Il semi-anonimato dei Bitcoin lascia una traccia che offre una possibilità agli operatori antiriciclaggio di rintracciare i percorsi della moneta, (considerando che molti degli utenti di cripto-valute usano i sistemi di anonimato come TOR, oscurando l'IP e rendendo più difficili i processi di de-anonimizzazione) mentre le nuove cripto-valute attraverso mescolanze di indirizzi, suddivisioni dell'importo reale ed altre tecniche d'anonimato, rendono impossibile la tracciabilità.

Tra le prospettive future in tema di cripto-valute in Italia esistono ancora conflitti giurisprudenziali riguardanti la qualifica giuridica che queste devono avere nel contesto normativo. Nel 2016 l'Agenzia delle Entrate, con la risoluzione 2 settembre 2016, n. 72/E, sulla scia di quanto affermato dalla Corte di Giustizia<sup>520</sup>, ha sostenuto che le transazioni tra euro e cripto-valute per i soggetti residenti in Italia devono essere trattate alla stregua di transazioni in valuta straniera, con tanto di imposta sulle plusvalenze<sup>521</sup>. L'Agenzia precisa che la detenzione di valute virtuali va monitorata nel quadro della dichiarazione dei redditi, sul presupposto che le stesse siano assimilabili sotto il profilo fiscale a valute estere<sup>522</sup>. La risoluzione in questo modo tratta Bitcoin e simili come moneta corrente, imponendo alle imprese che dovessero operare con cripto-valute di applicarne le stesse regole fiscali.

Considerando che le monete virtuali sono state create come strumento di pagamento svincolato da qualsiasi tipo di istituto tradizionale centralizzato, vi è una certa difficoltà a concepirle come monete. In accordo con questa linea di pensiero infatti si sono allineate le direttive antiriciclaggio europee, e la presente legge n.90/2017, creando così un contrasto tra la definizione fornita in ambito tributario e quella in riferimento al riciclaggio di denaro.

Alla luce di questa divergenza l'interpello 956-39/2018 della Direzione Regionale della Lombardia<sup>523</sup> ribadisce, stavolta esplicitamente, la piena equiparazione secondo tale amministrazione delle valute virtuali alle valute estere e il *wallet* a un conto corrente, in piena contraddizione con quanto statuito dalla giurisprudenza interna ed europea.

Come recentemente ribadito dalla sentenza 6185/2017 della V sezione della Cassazione<sup>524</sup> le circolari e le risoluzioni dell'Agenzia delle Entrate non vincolano il giudice, in quanto riconoscere

---

<sup>520</sup> Corte di Giustizia UE, Quinta Sezione, sentenza 22 ottobre 2015, Ibid.

<sup>521</sup> Agenzia delle Entrate, risoluzione 2 settembre 2016, n. 72/E, si veda il link: <https://www.agenziaentrate.gov.it/wps/file/nsilib/nsi/normativa+e+prassi/risoluzioni/archivio+risoluzioni/risoluzioni+2016/settembre+2016+risoluzioni/risoluzione+n.+72+del+02+settembre+2016/RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf>

<sup>522</sup> Ibid.

<sup>523</sup> Agenzia delle Entrate, Direzione Lombardia, si veda il link: <https://lombardia.agenziaentrate.it/>

<sup>524</sup> Si veda il link: [http://www.rivistadirittotributario.it/wpcontent/uploads/2017/03/GF\\_Cass\\_2017\\_6185.pdf](http://www.rivistadirittotributario.it/wpcontent/uploads/2017/03/GF_Cass_2017_6185.pdf)

in capo all'ente il potere normativo sarebbe in contrasto con il principio di riserva di legge dell'art. 23 della Costituzione<sup>525</sup>, non costituendo fonte di diritto.

Nonostante ciò, sia nella giurisprudenza nostrana che in quella europea<sup>526</sup> uno dei dibattiti ancora aperti è proprio quello della comparazione della moneta virtuale con la moneta corrente, con il fine di garantire un'equa tassazione e una sicurezza maggiore nel mondo delle cripto-valute.

---

<sup>525</sup> Giovanni Di Ciollo, cit. da *Criptovalute: profili giuridici*, 2018 si veda il link: [https://www.jei.it/approfondimenti-giuridici/497-criptovalute-profil-giuridici#\\_ftn56](https://www.jei.it/approfondimenti-giuridici/497-criptovalute-profil-giuridici#_ftn56)

<sup>526</sup> In riferimento alla decisione presa dalla Corte di giustizia Europea a riguardo.

## Conclusioni

Lo sviluppo tecnologico e la globalizzazione hanno trasformato le odierne realtà criminali. Azioni che un tempo erano limitate ad una determinata regione o area, oggi si sono estese oltre i confini nazionali, consentendo a molti reati di crescere e prosperare.

Le organizzazioni criminali sfruttano Internet, quale vasto spazio non regolamentato, per trasferire le proprie attività in rete, utilizzando tecniche di anonimato in modo da garantirsi l'immunità.

Il presente lavoro si è posto l'obiettivo di indagare il tema dell'uso improprio di tali tecniche, ovvero l'*onion routing* e le cripto-valute, da parte di vecchie e nuove forme di crimine organizzato, intente nel compiere reati transnazionali di diverso genere. Le reti criminali, con l'arrivo delle nuove tecnologie di rete, hanno trovato ulteriori modi e spazi attraverso i quali delinquere, specialmente nei mercati occulti online ed attraverso nuovi mezzi di riciclaggio dei proventi illeciti.

I diversi rapporti presentati dagli uffici di Europol illustrano come il commercio online di beni e servizi illegali e il fenomeno del cybericiclaggio siano diventanti, negli ultimi dieci anni, meccanismi di propulsione della criminalità organizzata in Europa<sup>527</sup>. Nel gennaio 2016, è stato stimato che i cripto-mercati abbiano generato guadagni che si attestano tra 14,2 e i 25 milioni di dollari americani al mese<sup>528</sup>, con un progressivo aumento negli ultimi tre anni<sup>529</sup>. Solo in Europa nel maggio del 2017 si è stimata una crescita del contrabbando nelle piattaforme del web oscuro che va dai 3 ai 5 miliardi di euro annui<sup>530</sup>.

Le organizzazioni criminali, impegnate in queste attività commerciali, hanno allargato la propria sfera di vendita ad una sempre più vasta clientela internazionale, aumentando così le proprie prospettive di guadagno. Inoltre, sfruttando i nuovi mezzi di pagamento come le cripto-valute per riciclare denaro, riescono a eludere molti dei controlli imposti agli istituti finanziari dalle leggi antiriciclaggio<sup>531</sup>.

Questa economia sotterranea, non percepita dai "comuni" utenti della rete, influenza enormemente la realtà in cui viviamo. L'apertura di nuovi mercati illegali alimenta la circolazione di droga e armi per le strade, contribuendo ad aumentare il fatturato del crimine organizzato di miliardi di euro<sup>532</sup>. Somme di denaro così ingenti, frutto delle compravendite illecite, vengono reinvestiti in appalti

---

<sup>527</sup> Europol, IOCTA 2018, SOCTA 2017.

<sup>528</sup> Kruithof Kristy, *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*, Rand Corporation, 2016.

<sup>529</sup> EMCDDA, 2018.

<sup>530</sup> Vitrais Benjamin, Europol: *The Dark Web Is The Heaven For Organized Criminals In The EU*, del 9 maggio 2017, si veda il link: [www.deepdotweb.com/2017/05/09/europol-dark-web-heaven-organized-criminals-eu](http://www.deepdotweb.com/2017/05/09/europol-dark-web-heaven-organized-criminals-eu)

<sup>531</sup> In riferimento al caso UIF e alle dichiarazioni della DIA.

<sup>532</sup> UNODC, *Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crime*, Ottobre 2011, si veda il link: [https://www.unodc.org/documents/data-and-analysis/Studies/Illicit\\_financial\\_flows\\_2011\\_web.pdf](https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf)

edilizi, bar, ristoranti, negozi e centri scommessa, i quali oltre ad avere la funzione di ripulire il denaro sporco, aumentano i capitali delle organizzazioni criminali che, se diffuse e radicate nel territorio, riescono ad influenzare le varie sfere della politica e i processi decisionali di un intero paese.

Dal punto di vista metodologico, per fornire una visione chiara e più possibilmente completa del quadro di cui si sta parlando, il presente lavoro ha affrontato diverse aree disciplinari coinvolte da tali tematiche, ambiti che vanno da aspetti più tecnico informatici a quelli di tipo storico-sociologico fino ad arrivare quelli più prettamente giuridici.

La tesi, oltre a ricostruire il quadro della situazione vigente, si pone l'obiettivo di individuare contributi utili, nell'ambito della giustizia criminale, finalizzati a limitare l'espansione di tali fenomeni.

Si è iniziato descrivendo tecnicamente il funzionamento dell'*onion routing* (partendo dai sistemi crittografici a cipolla fino a comprendere cosa sia il dark web) e delle cripto-valute, quali nuovi asset-class della rete (partendo dal bitcoin fino alle monete che vanno a rafforzare le transazioni anonime). Successivamente si è descritto come la criminalità organizzata si sia evoluta nell'arco degli anni ed abbia migliorato metodi e tecniche per delinquere. Tra i molteplici gruppi criminali presenti online, questo lavoro si è concentrato su due tipologie diverse, responsabili di reati transnazionali commessi attraverso la rete: le vecchie organizzazioni criminali, tese nel processo di digitalizzazione, e i nuovi cyber-gruppi criminali. Sistemi informatici e tecniche di anonimato non sono più in mano esclusiva di hacker e programmatori, ma sono diventate d'uso comune per il crimine tradizionale che si unisce ai nuovi gruppi della rete per spacciare droga, investire in nuove forme di riciclaggio di denaro o perpetrare vecchie condotte con l'aiuto di nuove tecnologie. Si è voluto così distinguere tre ruoli attraverso i quali le forme di crimine organizzato operanti online sfruttano l'*onion routing* e le cripto-valute: in primo luogo muovendosi come fornitori di prodotti e servizi (sfruttando i portali delle Darknet per alimentare il contrabbando di prodotti illeciti), poi come investitori (impegnandosi non solo nelle transazioni dei prodotti illeciti nei mercati oscuri, ma nel riciclaggio di denaro sporco online) ed infine come mano guida (di operazioni gestite esclusivamente nel cyberspazio). Una volta descritti protagonisti e ruoli, si è passati a descrivere il panorama delle azioni condotte attraverso l'uso improprio di queste tecnologie. Si è analizzata, in principio, la natura dei cripto-mercati, descrivendone le tipologie, i prodotti venduti e le attività illecite perpetrate. Successivamente si è mostrato come le organizzazioni criminali hanno evoluto le loro tecniche di riciclaggio attraverso i sistemi computerizzati arrivando alle cripto-valute, quali nuovi mezzi per "ripulire" i proventi illeciti. La digitalizzazione del crimine organizzato e la

convergenza di diversi tipi di tecniche informatiche nell'ambito delle transazioni in rete, rende estremamente complesso il percorso di regolamentazione e controllo.

Per cercare di comprendere quali siano le risposte finalizzate al combattere questi nuovi fenomeni criminali, il quarto capitolo ha inizialmente delineato un quadro normativo e delle istituzioni di contrasto alle attività illecite nelle Darknet, per poi passare ad un'analisi speculare riguardante il cybericiclaggio. Una delle principali problematiche esistenti nel momento in cui si cerca di approcciarsi agli aspetti tesi a disciplinare le azioni nel Darkweb ed in particolare nei *Darkmarktes*, consiste nel fatto che non esistano leggi o regolamenti propri per questo determinato settore della criminalità. Nella prassi governi e forze dell'ordine si affidano a provvedimenti già esistenti (come quelli sul divieto relativo alla compravendita di droga o armi) oppure a leggi riguardanti il crimine informatico che possano trovare spazi di applicabilità in tale contesto. L'auspicio delle Nazioni Unite nel sensibilizzare gli Stati a prendere decisioni in questo senso ha avuto scarsi risultati. La Convenzione di Budapest sulla criminalità informatica (2001) insieme alla Convenzione di Palermo (2000), sulla criminalità organizzata transnazionale, possono essere due strumenti normativi utili per contrastare tali fenomeni criminali in rete, ma insufficienti. Questo lavoro si conclude interrogandosi su quali possano essere le eventuali strade da percorrere, partendo dal presupposto che chiudere TOR, in quanto sistema d'implementazione dell'anonimato in rete, potrebbe non essere una soluzione efficace. Tale considerazione viene desunta da una serie di riflessioni esposte nel testo relative non solo all'impossibilità tecnica di agire in tal modo, ma al fatto che TOR possa svolgere un ruolo importante nella protezione dei dati personali, specialmente nel periodo in cui stiamo vivendo (la tendenza delle democrazie liberali nel proteggere dati e riservatezza del cittadino in rete). Le istituzioni europee, attraverso numerosi strumenti normativi a disposizione (art. 82 e 83 TFEU), possono rappresentare un punto di partenza per una regolamentazione riguardante l'economia "sotterranea" del crimine organizzato che, solo nei confini dell'Unione, fattura miliardi di euro annui. In questo lavoro vengono pertanto proposte due strategie di intervento finalizzate a limitare l'operabilità della criminalità organizzata negli spazi oscuri della rete.

La parte finale del lavoro ha affrontato il tema relativo alle azioni di regolamentazione e controllo nell'ambito del Cybericiclaggio che, come ampiamente descritto nel lavoro, ha avuto un importante sviluppo specialmente attraverso l'uso delle cripto-valute. Si è quindi analizzato in primo luogo la funzione del GAFI (Gruppo di Azione Finanziaria Internazionale) attore principale a livello internazionale che attraverso le sue raccomandazioni invita gli Stati nel cercare di aggiornare le proprie giurisdizioni in materia di riciclaggio di denaro. Si è mostrata l'efficacia della normativa antiriciclaggio a livello europeo che attraverso l'uso delle Direttive ha inciso fortemente nel processo di armonizzazione legislativa tra i diversi Stati membri. In conclusione vengono mostrati i

progressi della normativa italiana in materia di riciclaggio per mezzo di cripto-valute, evidenziando quali sono ancora le sfide poste dall'uso improprio delle nuove monete virtuali.

Nonostante i passi avanti svolti nel cercare di tenere sotto controllo gli scambi in cripto-valuta, esiste ancora una poca uniformità sia tra le istituzioni nazionali che europee in materia, mentre nell'ambito del dark web è ancora assente una regolamentazione adeguata. L'art.82 ed 83 del TFUE conferiscono agli organi decisionali dell'Unione poteri in ambito penale, tuttavia tali poteri oggi rimangono totalmente inesercitati. Una delle principali cause resta la volontà dimostrata dagli Stati di mantenere una piena sovranità nell'ambito della giustizia criminale, specialmente nell'attuale momento di crisi delle istituzioni europee.

Tuttavia, la crescita dei nuovi fenomeni criminali impone alle diverse nazioni di intervenire in senso unitario. Sin dal 1992 Giovanni Falcone con l'intento di istituire una procura europea, aveva auspicato l'unità legislativa degli Stati nel trovare misure adeguate a contrastare il processo di internazionalizzazione della mafia. A quasi trent'anni dalla sua morte tale processo è parte integrante dello sviluppo delle economie criminali, oggi fortificate dall'avvento delle tecnologie digitali. È essenziale così che i singoli Stati membri mettano da parte le incertezze, sfruttando l'Unione Europea quale fulcro nella lotta alla criminalità organizzata transnazionale.

## Bibliografia

### *Opere Monografiche*

Arduini Giorgio, Yakuza, un'altra mafia. Luni editrice 2017.

Douglas R. Stinson, Cryptography Theory and Practice, Third Edition, 2005.

Durante Massimo - Pagallo Ugo, Manuale di Informatica giuridica e diritto delle nuove tecnologie, Capi I Tecnologie dell'informazione e della comunicazione. 2017.

Conforti Benedetto, Diritto Internazionale, XI edizione 2018.

Narayanan Arvind, Joseph Bonneau, Edward Felten, Andrew Miller Steven Goldfeder, Bitcoin and Cryptocurrency Technologies, 19-07-2016.

Pellisero, Grosso, Manuale di Diritto Penale, parte generale, seconda edizione, Giuffrè Editore, 2017.

### *Articoli e saggi*

Al Jawaheri, Husam, B, Masters, Deanonimizing TOR Hidden Service Users Through Bitcoin Transaction Analysis, giugno 2017.

Alhighbani Abdulmajeed, Going Dark: Scratching the Surface of Government Surveillance, 23 Commlaw Conspectus 2015.

Aldridge & Décary-Héту Not an 'Ebay for Drugs': *The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation*, 2014.

Bakken, Silje; Møller, Kim & Sandberg, Sveinung. Coordination problems in dark net drug markets: Changes in cooperation, competition and valuation. *European Journal of Criminology*. 2017.

Brenner, Susan W., and Leo L. Clarke. Distributed Security: Preventing Cybercrime. *John Marshall Journal of Computer & Information Law*, 2005.

Broadhurst R. - Grabosky P. - Alazab M. - Chon S., Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 2014.

Broadhurst R., Malware Trends on 'Darknet' Crypto-markets: Research Review 2018.

Broadhurst R. and P. Grabosky, eds. *Cyber-Crime: The Challenge in Asia*, University of Hong Press, 2005.

Broadhurst R. (Ed.) *Bridging the GAP: A Global alliance on Transnational Organised Crime*, Hong Kong Police: Printing Department HKSAR, 2003.

Broadhurst R. - Grabosky P. - Alazab M. - Chon S., Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*. 01, 06, 2014.

Butler Eamonn, Cryptocurrencies: Threats and Investigative Opportunities for Law Enforcement, Charles University 31-07-2018.

Buxton Julia e Bingham Tim, The Rise and Challenge of Dark Net Drug Markets, 2015.

Campbell-Verduyn, Malcolm. "Bitcoin, Crypto- Coins, and Global Anti-Money Laundering Governance". *Crime, Law and Social Change* 01-2018.

Cipolla Alessandro, Antimafia: "Così la Camorra guadagna con la Borsa e i Bitcoin" L'allarme lanciato da Giuseppe Borrelli dell'Antimafia: "La Camorra investe in Borsa e Bitcoin perché meno accessibili alle indagini", 2 febbraio 2018.

Chaikin, David. *Network investigations of cyber-attacks: The limits of digital evidence*. *Crime, Law and Social Change* 2006.

Choi Sinyong, *Illegal Gambling and Its Operation via the Darknet and Bitcoin: An Application of Routine Activity Theory* 2018.

Christopher, C.M. *Wack-a-mole: Why prosecuting digital currency exchanges won't stop online money laundering*. *Lewis and Clarke Review*, 2014.

Cohen, B. *The IPE of money revisited*. *Review of International Political Economy*, 2016.

Clark Nicholas. *The Impact of Recent Money Laundering Legislation On Financial Intermediaries*, 1996.

Dalla Chiesa Nando, *Manifesto dell'Antimafia*, Einaudi 2014.

Dalla Chiesa Nando, *gli Scenari Internazionali della criminalità organizzata. Lineamenti teorici e di ricerca*, Mafia Globale, Laruna Editore, 2017.

Di Vizio Fabio, *Lo statuto giuridico delle valute virtuali: le discipline e i controlli, Tra oro digitale ed ircocervo indomito*, 2018.

Durrant Sarah, *Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations*, City University of New York CUNY Academic Works, 2018.

Falcone Giovanni, *Cose di Cosa Nostra*, ediz. Rizzoli, 1991.

Feola Raffaella, *Il reato di "money muling" Analisi del fenomeno legato al crimine informatico*, 21-09-2017.

Fiedler Ingo, *Online Gambling as a Game Changer to Money Laundering?* 2013.

Fornari L., *Criminalità del profitto e tecniche sanzionatorie* 1997.

Frunza, Marius-Cristian. "Solving Modern Crime in Financial Markets: Analytics and Case Studies". *Academic Press*, 9-12-2015.

Hardy, Augustus Robert Julia R. Norgaard, *Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web*, 2015.

Klip A., *European Criminal Law, 3rd Ed.*, Intersentia 2016.

Krebs Brian, "Tax Fraud Advice, Straight from the Scammers," *Krebs on Security*, 24-03-2015.

Kruithof Kristy, *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*, *Rand Corporation*, 2016.

Liu, Yi; Li, Ruilin; Liu, Xingtong; Wang, Jian; Zhang, Lei; Tang, Chaojing; Kang, Hongyan "An efficient method to enhance Bitcoin wallet security". *11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, 29-10-2017.

Lennon Y.C. Chang, *Cybercrime and Cyber Security in ASEAN*, luglio 2017.

Leong Angela Veng Mei, Chasing dirty money: domestic and international measures against money laundering, *Journal of Money Laundering Control*, 2007.

Lunde Paul, *Organized Crime: An Inside Guide to the World's Most Successful Industry*, 2004.

Matonis Jon, ECB: “Roots of Bitcoin Can Be Found in the Austrian School of Economics,” *FORBES BLOG* 3-11- 2012.

McGuire, M., *Organised Crime in the Digital Age*. London: John Grieve Centre for Policing and Security, 2012.

McQuade III, Samuel C. *Understanding and Managing Cybercrime*. 2006.

Merces, Fernando. *The Brazilian Underground Market*.2014.

Milad George, Irwin S.M. Angela: The use of crypto-currencies in funding violent jihad, *Journal of Money Laundering Control*, Ottobre 2016.

O'Neill Patrick Howell - Tor's ex-director: 'The criminal use of Tor has become overwhelming, 2017.

Paoli Giacomo Persi, Judith Aldridge, Nathan Ryan, Richard Warnes, *Behind the Curtain, the illicit trade of firearms, explosives and ammunitions on the dark web*, © Copyright, RAND Corporation. 2017.

Rapetto Umberto, *Cyberlaundering – Il riciclaggio del terzo millennio, "Cyberlaundering 2000"*, Università di Trento 1999.

Razzante Ranieri, *Bitcoin e Criptovalute, profili fiscali, giuridici e finanziari*, 2018.

Razzante Ranieri, *Bitcoin e monete digitali Problematiche giuridiche*, *Rivista Italiana d'Intelligence*, GNOIS, 2014.

Reynold Perri & Irwin Angela S.M. “Tracking digital footprints: anonymity within the bitcoin system” *Research Paper*, Emerald Publishing Limited, 2017.

Rhyme Upadhyaya, Aruna Jain, *Cyber ethics and cybercrime: A deep dwelled study into legality, ransomware, underground web and bitcoin wallet*, 2016.

Richet Jean-Loup, *Laundering Money Online: a review of cybercriminals' methods*, 2013

Romiti Maria Luisa, *Riciclaggio e gioco d'azzardo on line Il dark web sfrutta i “casinò” in rete*, 2014.

Rubinfeld, S. *FATF Pushes Risk-Based Approach Toward Virtual Currencies, Services*. *Wall Street Journal*, 2-07-2015.

Shams Heba, *Legal Globalization: Money Laundering Law and Other Cases*, *International Financial Law Series*, 2004.

Spaven, E. *UK Government Should Create Own Digital Currency*.*CoinDesk*, Maggio 2015.

Stokes, R. *Anti-Money Laundering Regulation and Emerging Payment Technologies*. *Banking & Financial Services Policy Report* 2013.

Stile A.M., *Riciclaggio e reimpiego di proventi illeciti*, 2009.

Tafazzoli Tala, *Cyber Crime Legislation*, *ICT Research Institute*, maggio 2018.

Tzanetakis Meropi , Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time, 2018.

Van Houta Marie Claire, Tim Bingham, ‘Silk Road’, the virtual drug marketplace: A single case study of user experiences, pubblicato su International Journal of Drug Policy, 2013.

Vitrais Benjamin, Europol: The Dark Web Is the Heaven For Organized Criminals In The EU, del 9 maggio 2017.

Weaver, S.: Modern day money laundering: does the solution exist in an expansive system of monitoring and record keeping regulations? Annu. Rev. Bank. Law Financ. Law, 2005.

Welling Sarah N., Andy G. Rickman, Cyberlaundering: The Risks, the Responses, 1998.

Yermack, David, Is Bitcoin a Real Currency? An economic appraisal, NBER Working Paper No. 19747 Dicembre 2014.

J.P. & G.T., Bits and Bob, “The Economist”: Babbage 13-06-2011,

Zaklina Spalevic, Milos Ilic, The Use of Dark Web for the purpose of illegal activity spending 2017.

Zoppei, V. Money Laundering: A New Perspective in Assessing the Effectiveness of the AML Regime. The European Review of Organised Crime 2015.

#### *Altri Contributi*

Commissione VI della Camera dei Deputati (Finanze): “Gli Istituti di pagamento in Italia” Audizione del Direttore Centrale per la Vigilanza Bancaria e Finanziaria della Banca d’Italia Stefano Mieli, ottobre 2011.

Consiglio D’Europa, 2005. Organised Crime in Europe: The Threat of Cybercrime., Situation Report 2004.

Consiglio D’Europa, Organised Crime in Europe: The Threat of Cybercrime., Situation Report 2004.

Directorate General Human Rights and Rule of Law Strasbourg, France – Report on Activity 6.1, Criminal money flows on the Internet Intra-regional workshop Kyiv, Ukraine, February 2012.

Eurasian Group on Combating Money Laundering and Financing of Terrorism, Cybercrime and Money Laundering 2014.

European Bank Authority, Opinion on ‘virtual currencies’, 4 luglio 2014.

European Central Bank, Virtual currency schemes –a further analysis 2015.

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) ed Europol, Drugs and the darknet: Perspectives for enforcement, research and policy, 2017.

Europol, “Drugs and the darknet Perspectives for enforcement, research and policy”, The Hague, the Netherlands, 2017.

Europol, Internet Organised Crime Threat Assessment (IOCTA) 2018.

Europol, Serious and Organized Crime Threat Assessment (SOCTA) 2013.

Europol, Serious and Organized Crime Threat Assessment, (SOCTA) 2017.

Europol ed EMCDDA Darknet markets ecosystem – Lifetimes and reasons for closure of over 100 global darknet markets offering drugs, sorted by date, Lisbon, April 2018.

GAFI, Report on Money Laundering Typologies 2000–2001.

GAFI, Money Laundering Using New Payment Methods, Report ottobre 2010.

GAFI, Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, 2013

GAFI, Virtual Currencies: Key Definitions and Potential AML/CFT Risks: FATF Report, 2014.

GAFI. Guidance for a Risk-Based Approach: Virtual Currencies, giugno 2015.

Internet Watch Foundation, Annual Report 2017.

Ministero dell’Interno, Primo rapporto nazionale sulla mafia – Progetto PON Sicurezza, Transcrimine, 2007 – 2013.

Polizia Postale e delle Comunicazioni, Documento Ufficiale 2016.

Parlamento Europeo, Commissione speciale sulla criminalità organizzata, la corruzione e il riciclaggio di denaro, Documento di lavoro sulla Criminalità Organizzata, 1-10-2012.

Parlamento Europeo, Directorate General for Internal Policy Policies Department for Citizens Rights and Constitutional Affairs, Counter-Terrorism, Virtual currencies and terrorist financing: assessing the risks and evaluating responses 2018.

Parlamento Europeo, Relazione sulla lotta contro la corruzione e il seguito dato alla risoluzione della commissione CRIM, 2016.

Parlamento Europeo, Virtual currencies and terrorist financing: assessing the risks and evaluating responses, Maggio 2018.

Senato della Repubblica e della Camera dei deputati, dossier XVII legislatura, Servizi di Pagamento nel mercato Interno, ottobre 2017.

UIF (Unità d’Informazione Finanziaria) Quaderni dell’antiriciclaggio, Casistiche di riciclaggio e di finanziamento del terrorismo, 2018.

UNICRI, Cybercrime and Organized Crime, 2015.

UNODC, Handbook on Identity-related Crime, 2011.

UNODC, Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime, 2013.

UNODC, “Strengthening international cooperation to combat cybercrime”, 2010.

UNODC, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, 2015.

UNODC, World Drug Report, United Nations Office On Drugs And Crime, Vienna, 2016.

UNODC, The Studies and Threat Analysis Section, Policy Analysis and Research Branch, Division for Policy Analysis and Public Affairs, UNODC”, “The Globalization of Crime – The threat of Transnational Organized Crime” 2010.

UNODC, The Global Programme against Money Laundering, Proceeds of Crime and the Financing of Terrorism 2011-2017.

UNODC, The Protocol against the Illicit Manufacturing and Trafficking in Firearms, 2001.

UNODC, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, 2015.

### *Fonti Normative*

#### ○ Livello Internazionale

40 Raccomandazioni “Standard internazionali per il contrasto del riciclaggio di denaro e del finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa” GAFI, 1990.

“VIII Congresso delle Nazioni Unite sulla Prevenzione del crimine e il trattamento dei detenuti” Nazioni Unite, Havana, Cuba, dal 27 agosto al 7-09- 1990.

IX Raccomandazioni, GAFI, 10-2001.

AG/RES. 2004 (XXXIV-O/04), Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: a Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, OAS, 08-06-2004.

“Convenzione del Consiglio d'Europa sulla lotta contro la tratta degli esseri umani”, Trattato n. 197, Varsavia, 16-05-2005, Consiglio d'Europa.

“Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale” Palermo, 12 - 15 dicembre 2000. Assemblea Generale delle Nazioni Unite.

“Convenzione sul Crimine Informatico”, Consiglio d'Europa, Budapest, 2001.

“Dichiarazione di Salvador on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World”, 19-04-2010. XII Congresso delle Nazioni Unite sulla Prevenzione del Crimine e la Giustizia Criminale.

“Dichiarazione di Vienna su Criminalità e Giustizia” adottata nel corso del X Congresso delle Nazioni Unite sulla Prevenzione del crimine e il trattamento dei detenuti, 10-17 aprile 2000.

“Effective measures to prevent and control computer-related crime”, Consiglio economico e sociale delle Nazioni Unite, 2002.

Pub.L. 109–347, Congresso degli Stati Uniti, Title VIII to the SAFE Port Act, Unlawful Internet Gambling Enforcement Act, UIGEA 2006.

Pub.L 87-216 To amend chapter 50 of title 18, United States Code, with respect to the transmission of bets, wagers, and related information.

Risoluzione, n. 55/25: “United Nations Convention against Transnational Organized Crime”, 10-11-2000, Assemblea Generale delle Nazioni Unite.

Risoluzione, n. 55/63: “Combating the criminal misuse of information technologies”, 22-01- 2001, Assemblea Generale delle Nazioni Unite.

Risoluzione, n. 58/199: “Creation of a global culture of cybersecurity and the protection of critical information infrastructures” 301-01-2004, Assemblea Generale delle Nazioni Unite.

Risoluzione, n. 65/230: “Twelfth United Nations Congress on Crime Prevention and Criminal Justice”, 1-04-2011, Assemblea Generale delle Nazioni Unite.

- Livello Europeo

Decisione 2009/968/GAI del Consiglio, 30-11-2009, che adotta le norme sulla protezione del segreto delle informazioni di Europol.

Direttiva 2013/40/UE, del 12 agosto 2013, Parlamento europeo e Consiglio dell'Unione Europea, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio.

Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR).

Risoluzione (UE) 25-10-2016, del Parlamento europeo, sulla lotta contro la corruzione e il seguito dato alla risoluzione della commissione CRIM (2015/2110(INI)),

Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI.

Trattato sul Funzionamento dell'Unione europea, (TFEU), ultima modifica dall'articolo 2 del Trattato di Lisbona 13 dicembre 2007.

- Livello Italiano

Codice Penale e leggi complementari, Editor Minor 2017.

D.lgs. 3 maggio 1991, n. 143 “Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio”.

D.lgs. 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali”.

D.lgs. 21 novembre 2007, n. 231 “Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché' della direttiva 2006/70/CE che ne reca misure di esecuzione”.

D.lgs. 13 agosto 2010, n. 141 “Attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori, nonché' modifiche del titolo VI del testo unico bancario (decreto legislativo n. 385 del 1993) in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi”.

D.lgs. 25 maggio 2017, n. 90 “Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006”.

Decreto del Ministero dell'Interno, 9-01-2008, “Individuazione delle infrastrutture critiche informatizzate di interesse nazionale”, “Istituzione C.N.A.I.P. I.C.”.

L. 5 luglio 1991, n. 197. “Conversione in legge, con modificazioni, del decreto-legge 3 maggio 1991, n. 143, recante provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio”.

L. 18-03- 2008, n. 48, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" pubblicata nella Gazzetta Ufficiale n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79.

L. 15 dicembre 2014, n. 186, Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio”.

L. 7 luglio 2016, n. 137 Ratifica ed esecuzione della Convenzione tra il Governo della Repubblica italiana e la Santa Sede in materia fiscale, fatta nella Città del Vaticano il 1° aprile 2015, con relativo Scambio di Note verbali del 20 luglio 2007.

Proposta di Legge, “Divieto di utilizzo delle cripto-valute che impiegano tecniche di anonimizzazione totale nelle transazioni economiche”, Presentata il 26-10- 2016.

Risoluzione, n. 72/E, Agenzia delle Entrate: “Interpello ai sensi dell’art. 11, legge 27 luglio 2000, n. 212. Trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali”.2-09-2016.

### *Fonti Giurisprudenziali*

Cassazione penale, sez. I, sentenza 08-09-2015 n° 36338, “Accesso abusivo a sistema telematico: il luogo di consumazione è quello in cui si trova l'operatore”.

“Case 1:17-at-00557” – USA v. Alexandre Cases19-17-2017, Corte del Distretto Orientale della California, Stati Uniti d’America.

“Case 14-cr-68 (KBF)” – USA v. Ross Ulbricht, 10-10-2014, Corte Sud del Distretto di New York, Stati Uniti d’America.

Corte di Giustizia UE, Quinta Sezione, sentenza 22 ottobre 2015: “Rinvio pregiudiziale – Sistema comune d’imposta sul valore aggiunto (IVA) – Direttiva 2006/112/CE – Articolo 2, paragrafo 1, lettera c), e articolo 135, paragrafo 1, lettere da d) a f) – Servizi a titolo oneroso – Operazioni di cambio della valuta virtuale “bitcoin” contro valuta tradizionale – Esenzione”.

EBA/Op/2014/08, EBA Opinion on ‘virtual currencies’, 4 - 07 - 2014.

UIF, Quaderni dell’antiriciclaggio, Casistiche di riciclaggio e di finanziamento del terrorismo, 2018, caso n. 6, p. 33 e 34.

