Quaderni di C.R.S.T.

Centro di Ricerca sulla Sicurezza ed il Terrorismo

Centro Ricerca Sicurezza e Terrorismo

Direttore Ranieri Razzante

Mariagrazia Mazzaraco

L'Intelligence economica nel dark web

Pacini Giuridica

Quaderni di

C.R.S.T.

Centro di Ricerca sulla Sicurezza ed il Terrorismo

1. Dante Gatta, *Africa occidentale e Sahel: problematiche locali dalla valenza globale*
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*
8. Giuseppe Lana, *Si Vis Pacem Para Ludum. Ping Pong Diplomacy: When Sport Breaks Walls*
9. Costanza Pestarino, *Permanent Structured Cooperation (PESCO). Opportunities and Risks for the italian military Sector*
10. Fabio Giannini, *Terrorismo internazionale. Aspetti criminologici e normativi*
11. Alessandro Anselmi, *Polizia e popolo. Dall'assolutismo allo stato di diritto tra il XVIII e il XIX secolo*
12. Antonio Rosato, *Profili penali delle criptovalute*
13. Giuliana Milone, *Recupero e valorizzazione dei beni confiscati alla criminalità organizzata*
14. Alessia Pietrantuono, *Sanzioni internazionali individuali e compliance come strumento di lotta al terrorismo*
15. Elena Canopoli, *Il coraggio di opporsi. Tutela e protezione nei confronti di chi denuncia la criminalità organizzata*
16. Sara Nazzaro, *Il valore educativo dei beni confiscati alla mafia*
17. Ken Terranova, *L'infiltrazione mafiosa nelle crisi: il caso dell'emergenza Coronavirus*
18. Bruno Mattia Balletti, *L'antiriciclaggio ai tempi dell'emergenza da Covid-19*
19. Sofia Mazzei, *The financing of Terrorism*
20. Mariagrazia Mazzaraco, *L'Intelligence economica nel dark web*

Realizzazione editoriale

Pacini Editore

Via A. Gherardesca
56121 Pisa

Responsabile di redazione
Gloria Giacomelli

Indice

“L’attacco migliore è quello che non fa capire dove difendersi. La difesa migliore è quella che non fa capire dove attaccare” Sun Tzu

Abbreviazioni

AISE - Agenzia informazioni e sicurezza esterna

AISI - Agenzia informazioni e sicurezza interna

ARPANET - Advanced Research Projects Agency NETwork

APT - Advanced Persistent Threat

BCH - Bitcoin Cash

BTC –Bbitcoin

CaaS - Crime-as-a-Service

CERN - Organizzazione Europea per la Ricerca Nucleare

CESIS - Comitato esecutivo per i servizi di informazione e di sicurezza

CTI - Cyber Threat Intelligence

DARPA - Defense Advanced Research Projects Agency

DIS - Dipartimento delle Informazioni per la Sicurezza

GPG - Gnu Privacy Guard

HUMINT - Human Intelligence

IMINT - Imaging Intelligence

IOC - Indicatore di Compromissione

IOT - Internet of Things

IP - Internet Protocol

IVAFE - Imposta sul Valore di prodotti Finanziari, conti correnti e libretti di risparmio detenuti all'estero da persone Fisiche residenti in Italia

MASINT - Measurement Intelligence

NIS - Direttiva UE in materia di sicurezza di Network and Information System

NIT - Network Investigative Technique

OSINT - Open Source Intelligence

P2P - Peer-to-Peer

TCP - Transmission Control Protocol

TUIR - Testo Unico delle Imposte sui Redditi

TUF – Testo Unico della Finanza

SISMI - Servizio per le informazioni e la sicurezza militare

SISDE - Servizio per le informazioni e la sicurezza democratica

SOCMINT - Social Media Intelligence

SNA - Social Network Analysis

TCP - Transmission Control Protocol

Tor - The Onion Router

VPN - Virtual Private Protocol

WWW - World Wide Web

Introduzione

Questo saggio vuole far riflettere il lettore sul fatto che il proliferare dei mezzi di comunicazione tecnologici, la globalizzazione, la libera circolazione di beni, servizi, capitali ed individui sui territori nazionali ed internazionali hanno mutato l'assetto socioeconomico tradizionale che, purtroppo, il progressivo processo di governance non è riuscito a controllare.

In questo marasma il cybercrime sta assumendo la connotazione internazionale di una vera e propria economia sommersa che con le sue sfaccettature di attività illegali aventi per oggetto la compravendita spesso fraudolenta di beni e servizi non propriamente leciti, transazioni monetarie produttrici di redditi non dichiarati, incidono prepotentemente sulla sicurezza e l'economia degli Stati.

Stati chiamati a contrastare un fenomeno di così grandi dimensioni e volume d'affari con una legislazione carente limitante dei poteri di operatività conferiti agli organi di controllo.

Il crimine organizzato si sta sempre più digitalizzando fino al punto da utilizzare le strumentazioni informatiche impropriamente: opera comunicando in anonimato (utilizzano il broser Tor - onion routing) nello spazio oscuro della rete (deep web e dark web), crea piattaforme e-commerce in cui armi, droga, corrispondenze epistolari, documentazione falsa e/o riservata, dati sensibili vengono venduti e/o scambiati con i nuovi mezzi di pagamento elettronici: le criptovalute definite dagli analisti dell'intelligence i nuovi asset class.

I black markets, i mercati neri virtuali presenti nel dark web diventano il volano dei crimini finanziari e del cybericiclaggio, di quell'attività di riciclaggio del denaro sporco della criminalità organizzata che risente, nella regolamentazione, del vuoto normativo.

In Italia il D.lgs. n. 90/2017, attuativo della Direttiva Europea 2015/849 inerente la prevenzione dell'uso del sistema finanziario a scopo di riciclaggio deiproventi di attività criminose e di finanziamento del terrorismo e recantemodifica 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, abrogativa del regolamento (CE) n. 1781/2006. (17G00104) vede un importante intervento del legislatore per rendere maggiormente trasparenti quelle transazioni anonime virtuali cherappresentano un grave pericolo per l'economia.

L'economia sommersa che va ad intaccare gli aspetti socio-culturali-economici della quotidianità, necessita di un incisivo intervento legislativo nei campi del diritto internazionale, europeo, penale, bancario e tributario per definire, giuridicamente, condotte criminose singole e/o associate nonché di una mirata e sempre più avanzata attività info-investigativa da parte degli analisti dell'intelligence.

L'ardua sfida che li vede impiegati consiste nella raccolta delle informazioni attraverso l'interrogazione e l'analisi delle open source – OSINT -, nel riprodurre off-line dei market, nel creare web profiling con cui infiltrarsi nella

rete, nell’affinare le metodologie d’indagine anche nell’ottica di una cooperazione internazionale vista la portata mondiale del fenomeno.

Innovativa è la piattaforma Cyber Assessment di Namirial che, senza l’installazione di alcun software, è in grado di identificare e valutare potenziali attacchi hacker rispetto all’efficacia dei controlli di sicurezza.

Il lavoro sinergico di una politica legislativa attenta ed adeguata ai cambiamenti tecnologici e di un’intelligence sempre più professionale rappresenteranno la chiave di volta per proteggere il sistema Paese e l’economia, interna ed internazionale, dai crimini della rete.

Capitolo 1 - L’intelligence economica

1.1 L’intelligence economica: concetto in continua evoluzione

Non si dispone di una definizione univoca di intelligence economica ma si ritiene che quella più appropriata sia fornita da Carlo Jean e Paolo Savona per i quali l’intelligence economica è quella disciplina che studia il ciclo dell’informazione di cui le imprese e lo Stato necessitano per adottare scelte operative, di sviluppo tali da garantirne la competitività nei contesti internazionali.

Quando si parla di intelligence economica si fa riferimento ad una misura collettiva, offensiva, formata da un insieme di azioni coordinate di ricerca, trattamento, diffusione e protezione di informazioni assunte legalmente – interrogazione delle “fonti aperte” Osint o attraverso sistemi “legalizzati” da attività statali Humint.

L’accesso all’informazione potrebbe anche avvenire con modalità segreta che diverrebbe lecita allorquando lo stesso accesso diverrebbe legalizzato. Naturalmente è necessario disporre, all’interno di un’organizzazione di reti e strumenti, all’esterno di influenza ed incisività al fine di preservare ed accrescere la governance geoeconomica di uno Stato; l’intelligence economica è, dunque, una strategia collettiva atta a ricercare una sinergia equa a gestire le sfide del mondo globalizzato.

La capacità dell’intelligence economica, nella contingente realtà globalizzata e tecnologicamente innovata è quella di saper gestire fenomeni eterogenei in

continua evoluzione (investimenti, ricchezza, equilibri economico-finanziari, proprietà intellettuale, scientifica, artistico-industriale) appartenenti tanto al settore pubblico quanto a quello privato.

La raccolta delle informazioni, la sorveglianza dei concorrenti, la protezione delle informazioni strategiche, la capitalizzazione delle conoscenze, diventa fonte di potere economico capace di condizionare le scelte della geopolitica economica, aumentare la crescita ed il benessere della nazione, stabilizzare il potere.

Business intelligence e competitive intelligence per esempio, specie nel settore privato, devono coordinarsi, attraverso una perfetta osmosi oseremmo dire, con l'analisi dei big data, gli esiti del controspionaggio piuttosto che dello spionaggio industriale, con una politica legislativo-governativa favorevole allo sviluppo del Paese.

Per il decisore politico l'intelligence economica deve divenire bene pubblico, bene della collettività, attraverso cui proteggere l'economia nazionale sostenendo lo sviluppo del tessuto economico per il tramite dell'acquisizione di nuove tecnologie piuttosto che di nuovi segmenti del mercato mondiale conquistato… il rafforzamento economico-sociale del paese è la sua più alta espressione di potere internazionale.

1.2 L'intelligence economica: come è cambiata negli anni

Una serie di mutamenti sono intervenuti negli scenari politici ed economici succedutisi nel tempo: l'avvento del capitalismo sempre più competitivo e conflittuale, la contrapposizione ideologica e militare Est-Ovest, i modi di interpretare gli aspetti della vita nella sua evoluzione quotidiana, l'uso dell'informazione per trasformare l'ordine politico-economico in un nuovo ordine mondiale. Dal punto di vista dell'intelligence, l'allora periodo della guerra fredda era il mondo in cui l'informazione era assente; nell'era odierna in cui la tecnologia informatica è predominante, i decisori finiranno per essere sempre più vincolati e dipendenti dagli apparati per la raccolta, l'interpretazione,l'analisi delle informazioni.[1]

La fine della guerra fredda ha spostato la "potenza di fuoco" dal campo militare a quello economico evidenziando quella stretta correlazione tra economia e sicurezza che rende il controllo dell'informazione decisivo per la competizione globale, la programmazione strategica, lo sviluppo del tessuto imprenditoriale nazionale ed internazionale.

Politica ed economia in questa nuova era di minacce, sono paragonabili a due guerre che si affrontano con l'uso delle informazioni. Una minaccia che si definisce asimmetrica in quanto si conduce in rete, sul web, immediata che non

[1] Treverton, G., *Reshaping National Intelligence for an Age of Information*. In: RAND Studies in Policy Analysis, 2001, 93-104;

mira a colpire obiettivi militari o politici ma interessi industriali, economici, commerciali, scientifici e tecnologici.

1.3 L'intelligence economica e lo stato strategico

Nell'era della competizione economico-internazionale, l'informazione rappresenta lo strumento di potere di cui lo Stato dispone, il bene più importante. Lo Stato modifica le proprie specifiche funzioni istituzionali fino a divenire uno "stato strategico"[2]: servendosi dell'intelligence economica affina le abilità cognitive e decisionali con lo scopo di favorire il proprio tessuto economico nello scacchiere globale implementando le dovute politiche a sostegno della produzione nazionale.

Lo *"stato strategico"*, per dirla con Gyula Csurgai[3] deve servirsi di apparati d'intelligence economica per gestire strategicamente l'informazione tanto da consentire allo Stato di anticipare, controllare, gestire il balance of power, le scelte politiche tanto offensive (minacce esterne) quanto difensive, perseverare o aumentare la propria posizione privilegiata nel mondo attraverso la creazione di un quadro geo-economico favorevole.

Nella realtà operativa l'effettiva funzione dell'intelligence economica è "sapere per anticipare". L'intelligence è intellegere, ossia saper analizzare le situazioni civili, economiche nazionali ed internazionali che riguardano un Paese, gli

[2] *Economic Intelligence and World Governance. Reinventing States for a New World Order*, ed. Il Cerchio, RSM 2016;
[3] G. CSURGAI, *Geopolitical and Geo-Economic Analysis of the S.W.F.*, LAP, Saarbruchen 2011;

scenari geo-economici dei Paesi esteri, valutare i rischi delle nazioni derivanti dal possibile stato di insolvenza o dagli investimenti nazionali.

L'informazione, come già previsto da Hayek e Mises[4] è il bene strategico più ricercato.[5] Tra gli attori dell'intelligence economica oltre agli Stati, vi sono le imprese, la società civile e l'infosfera in cui qualsiasi informazione divulgata ha un potere così energico da scatenare reazioni politiche mediatiche o danni reputazionali.

L'intelligence economica presenta due chiavi di lettura: per un verso getta le basi delle relazioni internazionali contemporanee, per l'altro consente di riflettere sulle metodologie e possibilità di rinnovamento di uno Stato in relazione alle funzioni di regolamentazione e redistribuzione delle risorse sue proprie non solo nell'ottica della competitività ma delle alleanze tra Stati ed imprese. Per quanto sopra esposto è lapalissiano che in un mondo sempre più cangiante, aperto a continue minacce, una sola definizione di intelligence *strictu sensu* non è più sufficiente; parimenti dicansi per il concetto di "sicurezza economica".

Un salto di qualità nel campo dell'intelligence economica è richiesto perché, almeno in Italia non esiste una cultura dell'intelligence economica: basti pensare alla concorrenza, all'elaborazione dei dati ed al successivo

[4] L. MISES, *Human Action*, Yale University Press, New Haven 1949;

[5] F.A. HAYEK, *The Use of Knowledge in Society*, in «American Economic Review», XXXV, 4, 1945, pp. 519-30;

monitoraggio dei sistemi tecnologici, dei brevetti che, *ex adverso*, in altri Paesi sarebbero operazioni di intelligence economica pura.

Seppure la legge n. 124/2007 rubricata "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto" che ha novellato la legge 24 ottobre 1977, n. 801 rappresenti con le strutture preposte al coordinamento (DIS – informazioni e sicurezza[6] sostitutivo del CESIS[7]) ed all'operatività (AISI ed AISE già rispettivamente SISMI[8] e SISDE[9] – agenzie informazioni e sicurezza esterna ed interna) il fiore all'occhiello della professionalità e della capacità d'indagine, favorita, altresì, dall'Unione Europea che con la direttiva NIS e la direttiva delle infrastrutture critiche ha avviato un percorso di atti e strumenti che vanno dalla golden power al perimetro di sicurezza nazionale cibernetica. La legge n. 124 ha introdotto oltre ad una nuova disciplina del Segreto di Stato un'idonea regolamentazione in materia di garanzie funzionali.

La normativa in questione a livello internazionale guarda ai c.d. attori di prioritario interesse informativo, ai principali rischi di attacchi invisibili a cui il nostro sistema Paese potrebbe andare incontro, a rafforzare la difesa delle infrastrutture critiche materiali ed immateriali nei settori informatici e della

[6] Legge 3 agosto 2007, n. 124. "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", pubblicata nella *Gazzetta Ufficiale* n. 187 del 13 agosto 2007. Articolo 3, commi 1 e 2;
[7] Comitato esecutivo per i servizi di informazione e sicurezza;
[8] Servizio per le informazioni e la sicurezza democratica;
[9] Servizio per le informazioni e la sicurezza militare;

cybersecurity[10] a cui rimanda la Legge 133/2012. La sicurezza cibernetica implica la capacità di affrontare prontamente la penetrazione economica ostile di attori stranieri, controllare i flussi finanziari internazionali che sovvenzionano attività terroristiche e di pirateria informatica[11], l'esportazione illegale di capitali all'estero.

Anche l'Italia si sta adoperando per sviluppare un servizio di intelligence sempre più orientato verso il contrasto dello spionaggio economico attraverso il "Piano nazionale per la protezione cibernetica e la sicurezza informatica"[12]. Già introdotto nel 2017 con Decreto n. 13 del Presidente del Consiglio dei Ministri, il piano contempla diverse iniziative volte ad analizzare i livelli di sicurezza dei sistemi e delle reti italiane[13]. Tra gli 11 indirizzi operativi presenti nel piano, merita attenzione l'indirizzo numero uno in materia di *"misure di potenziamento delle capacità di Intelligence, di polizia e di difesa civile e militare"*[14] atteso che la *"protezione cibernetica e la sicurezza informatica nazionali, presuppongono un'approfondita conoscenza delle vulnerabilità e delle minacce cibernetiche che le sfruttano".*

Concludendo si può quindi affermare che le nuove attività di intelligence devono rivolgersi all'analisi delle minacce e della vulnerabilità, allo sviluppo di

[10] Santarelli, "L'intelligence: cosa fanno i nostri servizi segreti, i reparti, le funzioni", *Network Digital 360,* 2020;
[11] Sistema di informazione per la sicurezza della Repubblica a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia, "Le nuove sfide";
[12] Cerra, "Perché la Cybersecurity è al centro dello scontro politico", 2021*;*
[13] "Piano nazionale per la protezione cibernetica e la sicurezza informatica", Presidenza del Consiglio dei Ministri, 2017;
[14] Ibidem;

strumenti a contrasto delle minacce cibernetiche, all'incremento di attività di raccolta, elaborazione, disseminazione, archiviazione delle informazioni digitalizzate e della relativa gestione per i progetti strategici infrastrutturali[15], a garantire la difesa negli ambienti cibernetici[16], l'integrità, l'autenticità, la riservatezza dei dati assunti[17].

1.4 L'intelligence economica in Italia

"Se vogliamo che l'Italia continui a mantenere un ruolo di primo piano a livello internazionale, dobbiamo rapidamente aggiornare gli strumenti essenziali per la nostra competitività" riflette Enrico Borghi, membro Copasir e responsabile politiche della sicurezza del Pd.

"Siamo in piena metamorfosi: esistenziale, politica, economica, istituzionale. All'Italia serve una "strategia di sicurezza nazionale" che non sia la somma di provvedimenti settoriali, spesso tra loro incoerenti (pensiamo ad esempio al proposto tema della liberalizzazione e della frammentazione di competenze sulle concessioni idroelettriche mentre mezza Europa le ha blindaterendendole di fatto quasi perpetue e paesi come la Francia le hanno addirittura nazionalizzate!).

[15] Cerra, "Perché la Cybersecurity è al centro dello scontro politico", 2021;
[16] Piano nazionale per la protezione cibernetica e la sicurezza informatica", Presidenza del Consiglio dei Ministri, 2017;
[17] Ibidem;

E tutto ciò, inevitabilmente, ci rimanda ad una esigenza di implementazione, di rafforzamento e di ulteriore qualificazione della nostra intelligence economica. Anzi, di una sua profilazione specifica.

Il processo di IE - a parer mio - potrebbe essere suddiviso in nove steps e per ciascuno di essi è possibile declinare gli attori coinvolti, le attività operative eseguite, le metodologie e gli strumenti di supporto di cui avvalersi.

Ovviamente ogni Stato è responsabile della scelta della strategia di intelligence e del conseguente processo di realizzazione scelto, tenendo conto del fatto che molti fattori possono influenzare la potenziale scelta:

- *l'organizzazione socio-politica;*
- *la cultura della sicurezza;*
- *la base giuridica;*
- *i valori economici di ogni singolo Paese.*

I nove steps del processo di Intelligence Economica, potrebbero essere:

***1**: identificazione del problema da risolvere, in termini di minaccia, rischio e/o pericolo;*

***2**: definizione degli obiettivi;*

***3**: identificazione delle fonti di informazione pertinenti;*

***4**: validazione delle fonti di informazione;*

***5**: raccolta delle informazioni;*

***6**: elaborazione delle informazioni raccolte per il calcolo di indicatori;*

7: *interpretazione degli indicatori;*

8: *definizione del processo decisionale per la risoluzione del problema;*

9*: tutela del patrimonio informativo durante l'intero processo.*

Gli attori del processo svolgono, nella adeguata riservatezza, attività di ricerca, selezione e di studio dei fenomeni di minaccia che interessano la sicurezza nazionale (terrorismo, eversione, proliferazione, criminalità, immigrazione clandestina, ecc.).

In particolare:

- ✓ *analizzano le informazioni ed elaborano report con riferimento alle insidie e ai dettagli insiti nelle singole minacce;*
- ✓ *formulano analisi previsionali sui potenziali profili evolutivi dei fattori di rischio connessi alle minacce;*
- ✓ *forniscono supporto informativo ai settori operativi, effettuando "scambi informativi" con strutture esterne facendo riferimento al processo iterativo articolato che presenta i vari step collegati tra loro in maniera lineare e ciclica.*

La gestione ottimale delle attività di processo prevede la combinazione di know how specifico e l'utilizzo di strumenti informativi connessi ed alimentati anche dalle precedenti esperienze di ricerca e analisi. Inoltre la gestione dell'IE dovrebbe tendere ad incrementare un approccio di comunicazione tra i diversi attori del processo, al fine di trasformare la conoscenza sommersa o implicita, in esplicita e intellegibile stabilendo di volta

in volta le operazioni di fine tuning da eseguire in ogni momento dell'intero processo di raccolta dati, analisi e diffusione.

Molti dati economici finanziari e di informazioni aziendali sono disponibili mediante ricerche specifiche sul Web, piuttosto che attraverso l'utilizzo di banche dati in grado di valutare le attività di M&A delle società, di delineare il profilo di un determinato Paese (es. indicatori macroeconomici e demografici) e di monitorare i settori di mercato. Grazie a sistemi automatici anche di text e data mining, tali dati possono essere organizzati, confrontati e valutati con massicce tipologie di informazioni non strutturate, plurinazionali, pluritematiche, al fine di identificare e anticipare un evento o un cambiamento.

Il trasferimento e la tutela della conoscenza tacita o implicita rappresentano gli aspetti critici legati ad ogni processo di apprendimento e di conseguenza necessitano di particolare attenzione e - secondo alcuni esperti[18] di Knowledge Management - questo può avvenire seguendo un iter suddiviso in quattro fasi:

***1**: socializzazione: in un contesto informale gli esperti di IE e gli analisti condividono le esperienze e gli approcci utilizzati su progetti inerenti tematiche affini a quelle trattate;*

***2**: esternalizzazione: in questa fase si creano dei progetti/casi di studio che consentono di attingere alla conoscenza tacita degli individui, favorendone l'esplicitazione, la comunicazione e la condivisione selettiva all'interno del gruppo;*

[18] Nonaka I, Takeuchi H. The Knowledge Creating Company, University Press, Oxford, 1995;

***3**: combinazione: consente di combinare le conoscenze esternalizzate degli individui tramite il passaggio di informazioni, al fine di maturare le metodologie e gli approcci corretti;*

***4**: internalizzazione che consente di interiorizzare le conoscenze apprese mettendole in pratica tramite sessioni di learning by doing, per entrare a far parte del bagaglio professionale di ciascuno.*

L'approccio proposto, crea questo ciclo di condivisione, sviluppo e tutela delle informazioni, permettendo di diffondere e trasferire in maniera selettiva il know-how implicito ed esplicito tra i partecipanti del gruppo di lavoro, favorendo il coinvolgimento e la partecipazione attiva di tutte le risorse, anche quelle di livello più operativo.

Il contributo dell'IE consiste sostanzialmente nel comprendere e anticipare le cause, le logiche delle azioni e delle operazioni potenzialmente nocive al sistema-Paese, fornendo l'informazione giusta alla persona giusta, nelmomento giusto, al fine di prendere la giusta decisione.

Uno degli aspetti più significanti è, quindi, quello di sviluppare una cultura della sicurezza, che permetta agli addetti ai lavori di creare un sistema e un network informativo valido sia per i semplici cittadini che per i decisori.Le attività di Intelligence Economica sono divenute imprescindibili per la sicurezza nazionale, soprattutto in relazione ai settori strategici considerati irrinunciabili per la crescita economica dell'intero sistema-Paese.

Lo Stato, inteso come sistema autopoietico[19] , ha il compito di sapere come essere in grado di rendere le comunità e le economie immuni agli attacchi caratterizzanti di questo periodo storico dominato dall'ipercompetizione, dalla finanziarizzazione e dall'informatizzazione, utilizzando tutti gli strumentiadeguati ed efficaci: dal "lobbismo" alla disinformazione, alle più sofisticate operazioni di politica economica.

Pertanto, per incrementare la base informativa, può essere utile ottenere la collaborazione di tutte le istituzioni, delle Università, dei centri di ricerca pubblici e privati e acquisire il consenso diffuso sull'attività di Intelligence Economica. Sono passi importanti verso il riconoscimento di un rinnovato ruolo dell'intelligence, propedeutico allo sviluppo della cultura dell'intelligence che consideri le imprese non solo beneficiarie, ma anche collettori di informazione per condividere notizie e consolidare posizioni economiche incrementando la percezione della sicurezza percepita/fornita.

Il concetto stesso di cultura della sicurezza non può prescindere dalla assimilazione della indispensabilità dell'intelligence nel settore economico finanziario, oggi come non mai, motore della solidità di un Paese.

[19] Termine utilizzato per l'impresa privata. Essa possiede due proprietà apparentemente contrastanti: è "aperta", poiché scambia risorse con l'ambiente in cui è parte; è "chiusa", poiché è in grado di mantenere relativamente stabile la propria organizzazione rendendola impermeabile alle spinte provenienti dall'esterno. Fontana F., Caroli M., Economia e Gestione delle imprese, McGraw-Hill, 2008 - Università LUISS Guido Carli;

Capitolo 2 - Navigare in Internet: Surface Web, Deep Web e Dark Web

2.1 Internet e World Wide Web: cenni storici

Si fa risalire al 1969 la nascita della rete Internet. In quell'anno l'agenzia governativa del Dipartimento della Difesa degli Stati Uniti, DARPA – *Defense Advanced Research Projects Agency* -, incaricata dello sviluppo di nuove tecnologie per uso militare, elaborava una rete di nodi denominata ARPANET - *Advanced Research Projects Agency NETwork* -, strutturata su un'architettura *client/server* destinata ad esclusivo uso militare. *Ab origine*, ARPANET era stata pensata appunto, ad esclusivo uso militare atteso il periodo di guerra fredda che si stava vivendo: intorno agli anni '80 trasforma la sua naturale connotazione e diviene uno strumento da impiegare nell'ambito universitario per scambio relazionale e di conoscenze scientifiche.

Differentemente, del web – www - World Wide Web, ossia l'architettura attraverso la quale è possibile usufruire della maggior parte dei contenuti disponibili sulla rete Internet, se ne comincia a parlare il 12 marzo del 1989 ad opera del suo inventore, il britannico Timothy John Berners-Lee. Lee in una memoria che presentò al Cern[20], a Ginevra ai suoi capi, descrisse il MESH prima, divenuto Word Wide Web poi, come un sistema che consentiva la gestione di una miriade di informazioni derivanti dagli esperimenti scientifici

[20] Il CERN (Organizzazione Europea per la Ricerca Nucleare) è il più grande laboratorio al CERN. Fu proprio nell'agosto di quell'anno che Berners-Lee annunciò pubblicamente la straordinaria invenzione del web;

che si svolgevano proprio all'interno del CERN. I dati che di volta in volta si assumevano venivano resi disponibili per lo studio di circa 17.000 scienziati. La svolta Tim Berners-Lee la raggiunse nel 1990 allorquando, unitamente ai suoi collaboratori, pubblicò la prima pagina web che, nel descrivere il progetto, esemplificava e conteneva alcuni collegamenti - link -, ipertestuali per il raggiungimento di alcune pagine. Il primo server si appoggiava sul computer di Lee, nel marzo del 1991 i software per usare il Word Wide Web furono localizzati presso il mondo di fisica delle particelle, al confine tra Svizzera e Francia, nel comune di Mevrin, alla periferia ovest della città di Ginevra e resi fruibili al pubblico.

Alla luce di questo breve *excursus* storico per meglio comprendere cosa sia Internet è necessario approcciarsi alla definizione tanto da un punto di vista tecnologico quanto da una prospettiva sociologica. Tecnologicamenteparlando ed usando la definizione già fornita da Kurose**,** *Internet è il network di computer che interconnette dispositivi computazionali chiamati host o end systems cioè nodo ospite*: trattasi di dispositivi connessi tra loro per il tramite di una struttura di communication links e packet switchers che collegano vari apparati trasportando e smistando pacchetti di dati.

I nodi ospiti scambiano dati senza elaborarne il contenuto ma rendendone visibile il percorso.

Ogni componente di questo sistema segue delle regole denominate protocolli - TCP (*Transmission Control Protoco*l) e l'IP (*Internet Protocol*), di formato ed ordine per comunicare i dati fra due o più sorgenti.

Ross definiva Internet, sempre secondo l'aspetto tecnologico, come quell'infrastruttura capace di fornire servizi alle applicazioni: per citarne alcune mail, web, peer-to-peer, voip, instant messaging, ecc…

Le applicazioni di cui si parla sono distribuite sui vari dispositivi e permettono lo scambio di dati fra i vari endsystems che le ospitano.

L'infrastruttura dunque fornisce servizi alle applicazioni distribuite sui dispositivi. A conclusione si può affermare che la rete Internet è l'infrastruttura tecnologica sulla quale viaggiano i dati[21].

Uno dei servizi di Internet è il web che permette il trasferimento e la visualizzazione dei dati, sotto forma di ipertesto; il medesimo processo vale anche per altri servizi quali la posta elettronica, i newsgroups, i trasferimenti FTP.

[21] Metaforicamente potrebbe paragonarsi ad una ferrovia digitale, composta di binari (canali), stazioni (server) e regole (protocolli);

2.2 Surface Web, Deep Web e Dark Web: differenze

La struttura su cui si appoggiano il surface web, il deep web ed il dark web è Intenet.

Per capirne il funzionamento il lettore deve immaginare il web come una piramide, un'iceberg, dove in superficie c'è il Surface web, al centro il Deep web ed in fondo il Dark web.

Nel primo strato visibile - Surface web o clear web -, si rinviene tutto quanto accessibile pubblicamente[22], siti scansionati ed indicizzati cioè ricercabili, attraverso un semplice motore di ricerca tipo Google, Bing, Yahoo o altri normali browser. Sia i siti che le aziende presenti nel *web* si servono di strumenti di ricerca e di proliferazione (i cookie per esempio) al fine di raccogliere quante più informazioni possibili relativamente alle abitudini, ai gusti, alle scelte dei cibernauti per poi elaborare offerte aziendali personalizzate. Quando si accede ad un sito *web* non sempre è possibile disattivare i descritti strumenti di proliferazione tanto che alcuni rimarranno attivi all'insaputa dell'utente e a discapito della privacy e della sicurezza dei dati: ci sarà sempre l'occhio del grande fratello che ne spierà la navigazione.

Nel Deep web, web profondo o web sommerso, nell'acqua di quella famosa piramide a forma di iceberg, si reperiscono, invece, tutti quei dati **non** raggiungibili attraverso un comune motore di ricerca tipo Google in quanto non

[22] il 4% dei contenuti che complessivamente girano sul *web;*

indicizzati[23]. Si tratta di dati non accessibili pubblicamente tanto che il fruitore deve dotarsi di credenziali, cioè username e password, per accedervi anche a garanzia della tutela dei medesimi. L'esempio di scuola è l'accesso al proprio conto corrente o al proprio indirizzo di posta elettronica: in entrambi i casi sono necessarie specifiche credenziali.

Il Dark web, punta inferiore della parte sommersa dell'iceberg, è l'insieme dei siti web, che offrono i loro contenuti, volutamente tenuti segreti, accessibili pubblicamente ma non indicizzati e quindi invisibili, per navigare in totale anonimato e sottrarsi ad ogni forma di controllo, attraverso un indirizzo IP[24] nascosto (che non permette di individuare facilmente il proprietario del sito) e che sono raggiungibili soltanto attraverso la rete Onion.

Non esiste quindi un'univoca definizione di Dark Web che è il *luogo digitale dove si incontrano le communities dell'underground*, sostanzialmente dedite ad attività illecite di qualsiasi genere. Alcune communities potrebbero essere isiti onion accessibili tramite Tor, altre potrebbe avere solo un indirizzo IP, ma nessuna ha mai un nome. Infatti i computer per comunicare tra loro necessitano di un indirizzo IP che permetta di rendere conoscibile il mittente e il destinatario di un pacchetto dati.

[23] secondo alcune stime, ammonterebbe al 96% circa del totale delle informazioni nell'intera rete;

[24] Un indirizzo IP è un'etichetta numerica che identifica univocamente un dispositivo detto *host* collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete;

2.3 Il Dark web e l'economia sommersa: il lato oscuro della rete

Il dark è il più fiorente mercato dell'economia sommersa e delle attività illegali.I cyber criminali offrono servizi, si rendono disponibili a completare lavori specifici richiesti quali la violazione di sistemi informatici, a compravendere database clienti, a pianificare potenziali attacchi hacker a siti web (blocco temporaneo di un sito), a sottrarre risorse sensibili di sistemi informatici aziendali.

Con il termine di dark web, di web oscuro o rete oscura si definiscono quei contenuti del *web* presenti nelle darknet, ovvero quelle reti virtuali, oscure appunto, private a cui è possibile accedere solo tramite specifici software o particolari configurazioni di rete.

Se il core business del dark web è il black market cioè il mercato nero, illegale in cui è possibile acquistare ogni tipo di bene, dai medicinali alle sostanze stupefacenti, ai documenti di identificazione falsi, alle armi, alle carte di credito clonate, ai dati malware e a quelli rubati alle aziende quali, indirizzi di posta elettronica riservati, indagini di mercato, database, cosa spinge l'utente fruitore ed utilizzatore ad accedere con sempre maggiore frequenza alle reti oscure? Acquistare e vendere prodotti illegali, diffondere notizie di carattere riservato, aggirare la censura di Internet e dei sistemi di filtraggio dei contenuti, superare i firewall*,* condividere file illegali, contraffatti, piratati, compiere crimini informatici quali frodi o hacking, attacchi informatici nelle modalità del keylogger, del botnet, del phishing e del ransomware*.*

2.4 Dark web e modalità di accesso: il browser Tor

Secondo il professore Nicolas Christin, docente alla Carnegie Mellon University**,** il dark web *segnala semplicemente tutte quelle pagine che non possono essere trovate dai motori di ricerca.* Una delle caratteristiche del dark web è la navigazione in anonimato attraverso darknet, browser speciali, tipo I2P, Freenet, Tor – The Onion Router.

La navigazione nel dark in linea di massima non ha niente di malevolo o di illegale: occorre però precisare che le condotte illecite non si configurano per la pura navigazione in anonimato attraverso il browser *Tor* ma scaturiscono dall'interazione con i mercati illegali, i black market.

Nei regimi totalitari la navigazione in riservatezza, ancora oggi, viene usata da coloro che non hanno libero accesso ad Internet. A tal proposito si ricordi che, per tale finalità, la BCC ha creato un'apposita pagina per consentirne l'accesso a chiunque in qualsiasi luogo si trovasse.

Nel 1995 la Marina Militare degli Stati Uniti ha elaborato il progetto TOR, ora gestito dalla *The Tor Project* per sottrarre le conversazioni governative (ordini e disposizioni di impiego), riservate, alle potenziali intercettazioni dei servizi di intelligence stranieri e delle entità nemiche.

Gli attori sociali, autori del progetto, hanno tenuto a precisare che "*Tor è più di un semplice software: è il lavoro d'amore prodotto da una comunità internazionale di persone devote ai diritti umani*" – e che "*… tutte le persone che sono state coinvolte in Tor sono unite da un credo comune*… [vale a dire

che] … *gli utenti di Internet dovrebbero avere un accesso privato ad un web senza censura…*". Ricordano, infine, di "*combattere ogni giorno perché tutti possano ottenere un accesso privato ad un Internet senza censure*"[25].

Come si è anticipato in qualche riga sopra uno dei *browser* da installare per navigare in anonimato e riservatezza nel dark web al fine di fare file sharing ovvero scambiare pacchetti di dati tra il cibernauta ed il fornitore di servizi e non solo http, è TOR – *The Onion Router*, software gratuito (scaricabile da chiunque) e open source che dirige il traffico Internet attraverso una rete di overlay volontaria gratuita.

Approfondendo il funzionamento della rete Tor da un punto di vista squisitamente informatico, il network di server ospitati, presenta una stratificazione a cipolla tra i punti di partenza e quello di arrivo della comunicazione rendendo quasi del tutto impossibile risalire all'utente. Chi interroga la rete Tor è garantito nel non vedere comparire il proprio indirizzo IP, la collocazione geografica (*torproject.org*) ed i dati acquisiti, prima digiungere a destinazione, viaggiano sui nodi della rete Tor.

[25] Sul sito viene inoltre riportato, all'apertura della Homepage, lo *slogan*: "*Naviga in Privato. Esplora liberamente. Difenditi contro tracciamento e sorveglianza. Evita la censura".* Vengono, inoltre, esplicitate le finalità di Tor, che consistono, in particolare, nel garantire l'anti-tracciamento ("*… isola ogni sito che visiti, così i tracciatori e gli ad di terze parti non possono seguirti. Qualunque cookie verrà automaticamente cancellato quando hai finito di navigare. Così come la cronologia*") e nella difesa contro la sorveglianza ("… *impedisce ad un estraneo di controllare la tua connessione per conoscere quali siti visiti...*");

La non identificabilità è assicurata perché l'*Hidden Service Protocol* permette di ospitare su un server un hidden service*,* ossia un servizio nascosto che ne garantisce l'anonimato.

Se volessimo adattare la teoria dei macrosistemi sociotecnici di cui parlava Hughes vedremmo che i darknet presentano artefatti simbolici, sociali, fisici. Questi ultimi sono i nodi di uscita della rete di onion routers su cui si fonda tutto il funzionamento del sistema e le infrastrutture prestate da Internet.

Essendo una rete di overlay volontaria e gratuita, composta da oltre settemila relè[26], per nascondere la posizione e l'utilizzo di un utente a chiunque esegua la sorveglianza della rete o l'analisi del traffico, Tor necessita di un underlay network su cui appoggiarsi anche se dispone di dispositivi con funzioni sue proprie.

Il software (distribuito dall'attore sociale *The Tor Project,* organizzazione senza scopo di lucro[27]) di cui si serve è molto importante perché rappresenta

[26] 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;

[27] L'organizzazione, diretta da Bruce Schneier, crittografo e tecnologo della sicurezza di fama mondiale il cui blog "Schneier on Security" è tra i più noti e letti sui temi della Cybersecurity, gode delle esenzioni fiscali che si applicano agli enti dedicati esclusivamente a fini religiosi, di beneficenza, scientifici, letterari o educativi. È inoltre finanziata da una pluralità di organizzazioni, tra le quali figurano anche istituzioni del

l'artefatto tecnologico che detiene il protocollo vale a dire le chiavi dell'artefatto simbolico globale della rete.

Il browser occulta l'attività e l'identità dell'utente on line dalla sorveglianza e dall'analisi del traffico separando il routing e l'identificazione, in che modo? Si tratta di un'implementazione del routing onion che crittografa end-to-end, non soggetta ad intercettazioni, quindi rimbalza le comunicazioni, in modo del tutto casuale, avvalendosi di una rete di relè di volontari sparsi in tutto il globo. L'anonimato in una posizione di rete e quindi la segretezza di inoltro dei relè di ingresso (relè ponte) si estendono all'hosting dei contenuti resistenti alla censura di Internet e sono garantiti perché i router onion usano la crittografia multistrato - da qui la metafora della cipolla.

Nel dettaglio i dati della navigazione non transitano direttamente dal client al server, ma per il tramite di relays, in gergo informatico nodi, che in qualità di router[28] realizzano un circuito virtuale crittografato a strati: questo il motivo per cui gli URL[29] della rete Tor hanno il TLD (punto) *.onion* piuttosto che (punto) .it o (punto) .com.

Governo USA, quali "*DARPA*" ("*Defense Advanced Research Projects Agency*") e il "*Bureau of Democracy, Human Rights and Labor Affairs*" del Dipartimento di Stato degli Stati Uniti, che – peraltro – è uno dei maggiori sostenitori del progetto;

[28] 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;

[29] "Uniform Resource Locator" (in acronimo URL) è la sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa su una rete di computer;

Avviata la navigazione il browser estrae dalla directory server una lista di nodi da cui in modo del tutto casuale ne individua almeno 3 (guard, middle, exit relays) per formare una catena di navigazione[30].

Ogni passaggio - nodo[31] - è crittografato e ricordando la conformazione della cipolla, a strati, ogni nodo della rete può conoscere solo quello precedente e successivo ma non gli altri ossia il *client* di partenza.

Il guard relay o entry o primo nodo, trasmette il traffico dati al middle relay (secondo nodo) che a sua volta lo trasmette all'exit relay (terzo nodo). La tipicità dei relays intermedi è l'essere maggiormente sicuri anche perché l'essere visibili solo all'interno della rete Tor non fa identificare il proprietario del guard relay.

L'exit relay, nodo di uscita, è l'ultimo nodo che il traffico Tor attraversa prima di giungere a destinazione: ciò significa che i clienti Tor, dei servizi a cui si connettono (provider di posta elettronica, siti web) visualizzano solo l'indirizzo IP del nodo di uscita e non del real client che, erroneamente, verrà identificato quale fonte del traffico.

A differenza dell'exit relay che, se non criptato può leggere il traffico in uscita ma non chi lo ha trasmesso, cioè il middle relay, il guard relay conosce sì il Tor

[30] Nella pagina del browser si può vedere – in tempo reale – il percorso che viene fatto ed anche cambiarlo con il pulsante che si trova alla sinistra della barra dell'URL. Non è però possibile scegliere personalmente i relays, ma solo fare in modo che Tor ne individui altri tre differenti;

[31] Un nodo (o come si è accennato in precedenza un *host*) è un punto di ridistribuzione della comunicazione. Ovvero un qualsiasi dispositivo hardware del sistema in grado di comunicare con gli altri dispositivi che fanno parte della rete;

client (indirizzo IP sorgente dell'informazione da trasmettere) ma non la portata delle comunicazioni.

2.4.1 Dark web e modalità di accesso: Tor e i livelli di sicurezza

Si è già detto che sia l'indirizzo IP del mittente che quello del destinatario non sono in chiaro durante la navigazione, pertanto, chi volesse intercettare qualsiasi punto lungo il canale della comunicazione non potrà identificarli in quanto al destinatario il nodo di uscita di Tor apparirà come l'autore della comunicazione piuttosto che il mittente.

Atteso che la navigazione in anonimato, sempreché condotta per finalità lecite, dovrebbe assicurare la privacy dei dati personali - *"qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"* si legge all'art. 4 Definizione, lettera b del D.Lgs.196/03 del Codice sulla Privacy - dell'utente e la riservatezza delle informazioni che veicola, il browser Tor nel caso di specie, oltre a crittografare i dati e a modificare costantemente l'indirizzo IP attraverso un circuito virtuale di relè selezionati casualmente, presenta tre livelli di sicurezza: standard, più sicuro, più sicuro.

Nel primo livello predefinito, dove il livello di sicurezza è il più basso, le funzionalità del *browser* sono tutte abilitate, nel secondo più sicuro, Java risulta disabilitato sui siti non HTTPS, nei siti in cui è abilitato le ottimizzazioni delle prestazioni sono disabilitate tanto che alcuni script potrebbero funzionare in

modo più lento, audio e video nei linguaggi HTML5 e WebGL sono click-to-play, alcuni meccanismi che permettono la visualizzazione di equazioni matematiche sono disabilitati.

Il terzo livello di sicurezza, anch'esso denominato più sicuro, presenta delle aggiunte alle funzionalità del secondo livello nel senso che Java è disabilitato di default su tutti i siti, anche in questo livello audio e video nei linguaggi HTML5 e WebGL sono click-to-play alcune icone, immagini, simboli matematici sono disabilitati.

2.4.2 Dark web e modalità di accesso: I2P, VPN, FREENET

Oltre al browser Tor ampiamente descritto nel paragrafo precedente, altre modalità di accesso al dark web sono possibili grazie all'utilizzo di altrettante reti oscure: I2P, VPN, FREENET.

I2P, anno di nascita 2003, è una rete anonima certamente molto più sicura della rete Tor ma molto meno usata causa la difficile configurazione.

Le comunicazioni P2P - Peer-to-Peer – sfruttano una struttura informatica in cui i nodi non sono ordinati esclusivamente nella forma di client (clienti) o server fissi (serventi) ma anche nella forma di nodi equivalenti o paritari (*peer*): svolgono contemporaneamente ed in modalità interscambiabile tanto la funzione di client quanto quella di server nei confronti degli host della rete (nodi terminali). Le comunicazioni viaggiano attraverso i tunnel (inbound: tunnel in entrata e outbound; tunnel in uscita) cioè una connessione virtuale crittografata ed unidirezionale che si serve fino a 4 peer (il primo è noto come gateway

tunnel l'ultimo come endpoint tunnel). Si noti che il router I2P che genera l'outbound è il gateway tunnel - primo peer, il router che genera l'inbound è l'endpoint - ultimo peer.

Le informazioni crittografate vengono trasmesse da un peer, passano attraverso il proprio outbound tunnel e giungono all'inbound tunnel del destinatario: è importante per questo funzionamento che ogni peer mantenga un tunnel in entrata ed uno in uscita.

La quantità e la lunghezza dei contenuti non sono predefiniti (più un contenuto è lungo e più è sicuro) ma criptati attraverso 3 strati di crittografia: la garlic per verificare che il messaggio sia stato consegnato al destinatario; la crittografia tunnel che accerta che tutti i messaggi transitino attraverso un *tunnel* e la crittografia del livello di trasporto tra i router.

Al pari della rete Tor anche la rete I2P è scaricabile dal sito del progetto, è gratuita e gli hidden services presentano quale suffisso (punto) .i2p**.**

La VPN - Virtual Private Protocol è una rete privata[32] (gratuita e/o a pagamento) che collega il computer ad un server tramite tunnel sicuri, in modalità da remoto, di cui l'utente si serve per navigare in sicurezza.

[32] È nata per uso aziendale, per consentire al personale esterno di connettersi alla rete aziendale in sicurezza. Il suo uso è poi stato esteso anche ai privati. Le VPN hanno caratteristiche che possono variare da fornitore a fornitore: solitamente sono a pagamento, ma esistono anche VPN gratuite. Tuttavia, come spesso accade, sono i prodotti a pagamento ad offrire le prestazioni migliori. Inoltre, possono essere istallate su qualsiasi sistema operativo ed anche da su smartphone;

I dati trasmessi sono criptati e protetti da un firewall che si interpone a mo' di scudo tra la macchina ed il server per bloccare eventuali software malevoli (malware) o potenziali tentativi di intercettazione.

Di VPN esiste la rete trusted con cui si è garantiti che nessun altro soggetto non autorizzato acceda al circuito del cliente. Per questo l'utente deve essere particolarmente accorto a preservare il proprio indirizzo IP.

La secure VPN trasmette dati su *i*nternet usando la cifratura e quindi di difficile intercettazione. Per finire si ha l'hybrid VPN che è una singolare rete privata: una secure VPN viene utilizzata come parte di una trusted VPN.

Diversamente dalle altre la rete oscura Freenet si basa sull'immagazzinamento a pezzi, di informazioni.

I file confluiscono in un data base distribuito, spezzettati, allocati in più computer (nodi) della rete, salvati in diverse copie.

I file immagazzinati sono recuperabili attraverso una chiave di cifratura consegnata allorquando si inseriscono nel data base. Anche per questa rete risalente agli anni 2000, l'accesso è pubblico ma la navigazione riservatissima. Diventa alquanto dispendioso se non impossibile controllare il contenuto dei file immessi così come la rimozione degli stessi che per tale motivo diverranno incensurabili.

2.5 Dark web e Black Market

E’ da non sottovalutare, però, la parte più insidiosa del dark in cui alloggiano i black market, portali e-commerce, criptati, non propriamente legali in cui è possibile acquistare e vendere, in totale anonimato, ogni genere di merce: dai più comuni - sostanze stupefacenti, armi, documenti falsi, carte di credito clonate, dati personali, informazioni aziendali, ai più impensabili - esseri umani, minori, organi, servizi di sicari. Gli utenti che accedono a queste piattaforme virtuali devono comunque accreditarsi in quanto i siti sono suddivisi in sezioni specifiche a seconda della tipologia del prodotto che si vuole compravendere. La monetizzazione non avviene tramite regolare mezzo di pagamento tracciato (bonifico bancario) ma tramite moneta virtuale, criptovalute, Tecnicamente il black market è un “hidden space” una piattaforma virtuale per attività di hosting illecite. Accanto ad Amazon, Ebay, un famoso black market è Skill Road (via della seta), nato nel 2011 che seppur adottando una piattaforma simile a quella in uso ad Amazon, è stato più volte chiuso dalle autorità. Attualmente il sito è nuovamente on line con la dicitura Skill Road 3.1.

Per accedere al sito è necessario registrarsi, fornire un nome utente (nickname), una password ed un codice identificativo per le transazioni, rispondere ad un CAPTCHA per accedere alla home page e beneficiare di tutti i servizi.

Gli scambi avvengono secondo il metodo del deposito di garanzia: per spiegarci, l’acquirente non versa il *quantum* dovuto direttamente al venditore

ma lo deposito presso l'operatore del mercato dimodochè possa rintracciare e monitorare in qualsiasi momento la transazione. Non sono ammessi dunque pagamenti diretti. All'atto del deposito dell'importo, il venditore invierà la merce, l'acquirente registrerà un feeedback, il venditore riceverà il dovuto. Tutta questa corrispondenza avverrà nella forma criptata per garantire l'anonimato servendosi della tecnica di criptazione a doppia chiave, una segreta ed una pubblica. La crittografia asimmetrica o a chiave pubblica – GPG – Gnu Privacy Guard -, è un sistema crittografico che utilizza coppie di chiavi pubbliche che, come dice la parola stessa sono pubblicamente accessibili e private in quanto conosciute solo dal proprietario. Predisposto nel 1981 dall'informatico statunitense David Lee Chaum, il sistema crittografato può essere spiegato con un esempio: se il soggetto A volesse inviare un messaggio solo al soggettoB, il primo dovrà disporre della chiave pubblica di B a cui invierà la comunicazione criptata. B, a sua volta deve avere una sua chiave privata per decodificarne il contenuto e leggere il messaggio che sarà segreto per tutti compreso il mittente che, non possedendo la chiave privata, non accederà al testo da lui stesso redatto.

L'utente durante la navigazione per inviare i propri messaggi al venditore, nasconde la chiave segreta e diffonde solo quella pubblica anche se li firma con la propria chiave privata per assicurare l'identità parimenti fa il venditore.

2.5.1. Dark web: l'operazione Berlusconi market

Tutta italiana è l'operazione denominata "Darknet.Drug" condotta dal Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza conclusasi nel novembre del 2019. L'attività tecnica captativa e under cover, nonché rilevamenti mediante sistemi di videosorveglianza e dispositivi GPS, come si legge nella sentenza n. 2233 del 17 novembre 2020 pronunciata dal Tribunale Ordinario di Brescia, consentivano ai militari della Guardia di Finanza di smantellare la piattaforma nota in rete con il nome di "Berlusconi Market" e di trarre in arresto gli ideatori ed i gestori. Nella comunicazione della notizia di reato redatta in data 3 luglio 2019 e recante il protocollo n. 83181 aff. PM 000997 i militari della Guardia di Finanza descrivevano nel dettaglio i black market ossia i mercati virtuali operanti nel dark web ponendo particolare attenzione alla piattaforma già citata Berlusconi Market, realizzata nel luglio del 2017 dove i venditori pubblicizzano e propongono in vendita sostanze stupefacenti, software dannosi, carte di credito clonate, documenti di identità e merci contraffatte, armi ed esplosivi, si legge nell'informativa. *"Il portale è gestito da due utenze: una avente lo pseudonimo Vladimir Putin con il ruolo di amministratore; l'altra operante come Emmanuel Macron con il ruolo di moderatore. dagli atti emerge che nel 2019 Berlusconi Marjet rappresentava, sia per la quantità dei beni posti in vendita sia per il valore della transazioni, il più importante mercato della dark net, composto da oltre 103.000 annunci di prodotti illegali; esso funziona come un normale sito di e-commerce; la*

creazione di un account è agevolmente effettuabile tramite l'impostazione di uno username e una password; una volta creato l'account, gli utenti sono in grado di navigare nel market e visionare i prodotti in vendita, suddivisi in categorie e sottocategorie; nella categoria stupefacenti e sostanze chimiche erano presenti, al 2-7-2019, n. 33.278 annunci, suddivisi in psicofarmaci, cannabis e hashish, allucinogeni, ecstasy, oppioidi; medicinali soggetti a prescrizione medica; steroidi; stimolanti, prodotti del tabacco; sostanze psicadeliche, ecc…; nella sezione guide e tutorial alla data del 28-6-2019 erano presenti n. 4.686 annunci, relativi alla vendita di manuali digitali per spedizione e ricezione di sostanze stupefacenti, metodi per compiere truffe on line, hackeraggio, sicurezza e tecniche per rendersi anonimi online; nella sezione oggetti contraffatti, al 24-6-2019, erano presenti n. 40.290 annunci, tra cui capi di abbigliamento, gioielleria, banconote, documenti d'identità, prodotti digitali tra cui ebook recanti metodologie per compiere frodi; virus e software per compiere truffe online; nella sezione gioielli e oro, al 28-6-2019, vi erano n. 670 annunci aventi ad oggetto la vendita di ori, argenti altri prodotti di gioielleria, verosimilmente di provenienza illecita o con marchi di fabbrica contraffatti; nella sezione armi erano presenti n. 5.327 annunci al 24-6-2019, aventi ad oggetto la vendita di armi, esplosivi e munizioni di vario tipo; nella sezione frodi sono proposti prodotti di vario genere, suddivisi in cinque sottosezioni, tra cui account finanziari violati o intestati a soggetti terzi; servizi di bank drop, ove il venditore si offre di effettuare una transazione su un conto

corrente indicato dal cliente, previo pagamento di una commissione, al fine di celare la provenienza di una certa disponibilità finanziaria; carte di credito clonate; documenti d'identità, nazionali ed esteri, materiali e digitali; nel caso di documenti d'identità digitali, sono in vendita i cosiddetti template, ossia dei file editabili sui quali inserire i dati anagrafici e fotografie, per poi stampare un numero illimitato di documenti.

In conformità al meccanismo descritto, anche tale piattaforma consente i pagamenti fornendo in automatico un indirizzo bitcoin agli utenti che effettuano acquisti e, a seguito di tali pagamenti, trattiene i relativi importi finchè i venditori non procedono al prelevamento o (per i venditori che non abbiano ancora ricevuto un sufficiente numero di recensioni positive) finchè l'acquirente non dimostri di aver ricevuto la merce (c.d. acquisti "in escrow"); il controllo su tali fondi presuppone la titolarità delle funzioni proprie dell'amministratore del market, in specie operante, come detto, con lo pseudonimo di Vladimir Putin.

Tanto premesso, le indagini condotte dal Nucleo Speciale della Guardia di Finanza hanno consentito di ricondurre alle persone degli odierni imputati non solo il venditore operante con lo pseudonimo gOOdOO (come si dirà, molto attivo sui black market), ma, altresì, la gestione dello stesso mercato virtuale denominato Berlusconi Market.

Tale, di seguito, l'articolato percorso investigativo che ha consentito di approdare agli esiti poi recepiti dall'organo di accusa e declinati nell'imputazione in addebito.

L'originario oggetto di indagine è stato il market on line accessibile nel dark web denominato Italian Darknet Community; esso è nato come forum in lingua italiana, raggiungibile esclusivamente sulla rete TOR, dove diversi utenti, individuati da uno pseudonimo, potevano mettersi in contatto tra loro per concordare compravendite di beni illegali (stupefacenti, banconote false, documenti falsi, dati di carte di credito clonate, ecc...); sul forum era inoltre possibile scambiare informazioni e richiedere consigli al fine di condotte illecite; nel febbraio 2017 il portale ha cambiato veste graficae si è diviso in due siti distinti; uno analogo alla versione precedente, e un altro che si presentava come un comune portale di e-commerce; il forum era prevalentemente utilizzato per recensire i prodotti venduti sul market, scambiare informazioni e per conoscere altri utenti; il market era finalizzato alla presentazione dei prodotti e alle compravendite; i pagamenti venivano effettuati in bitcoin.

Tra i venditori più attivi operanti su tale portale vi era quello avente nickname gOOdOO, già operante nel forum Italian Deep Web, nei market Dream Market e Berlusconi Market; esso offriva in vendita considerevoli quantitativi di stupefacente, in particolare marijuana, hashish, cocaina; mediante l'impiego di appositi software, sono stati ricondotti vari indirizzi di contatto del venditore in questione relativi ad un unico wallet (per 2145 indirizzi), con operatività, nel periodo 18-2-2016 – 15-6-2018, pari a 732.2452137 bitcoin, per un controvalore di 935.146,00 dollari, calcolato in base alle

quotazione corrispondente al momento delle transazioni.

Al fine di identificare i soggetti riconducibili al venditore gOOdOO veniva autorizzata un'operazione speciale con l'impiego di un agente sotto copertura, il quale, dopo aver creato un account sulla piattaforma BerlusconiMarket, effettuava quattro diversi acquisti simulati di stupefacente (cfr. annotazioni prot. n. 159325 e n. 1177 del 4-12-2018).

In particolare, in data 23-4-2018 era inoltrato un primo ordine di cocaina, a seguito del quale l'agente sotto copertura ritirava un plico spedito con busta affrancata (priva di indicazione del mittente) recante tagliandino postale del tipo "Posta 1 " e contenente una confezione di pellicole protettive per lo schermo dei cellulari, dentro la quale era occultata una bustina sottovuoto che racchiudeva, a sua volta, lo stupefacente, risultato all'analisi cocaina pura al 76%, tagliata con lidocaina (cfr. relazione tecnica 225C/2018 -48923 del 10/7/2018, ff. 514 ss. nonché verbale di sequestro trasmesso dalla Procura di Roma, aff. PM 512 ss.).

In data 16-7-2018 era inoltrato un secondo ordine; al fine di individuare il centro di meccanizzazione postale (CMP) di partenza della missiva contenente lo stupefacente, i militari presenziavano alle operazioni di smistamento postale notturno presso il C:MP di arrivo (Fiumicino) e individuavano, quale punto di smistamento della busta, il CMP di Bari, dove transita la corrispondenza proveniente dalla Puglia e dalla Basilicata; anche in questo caso la missiva pervenuta, sequestrata il 25/712018 (cfr. fascicolo trasmesso dalla Procura

di Roma, aff. 529 ss.), risultava contenere cocaina pura al 77% (cfr. relazione tecnica 225/C/2018 – 85426 del 16/11/2018, aff. 538 ss.). In data 16-11-2018 era effettuato un terzo ordine, all'esito del quale era ricevuto, con modalità analoghe, stupefacente della medesima tipologia.

Il successivo 7-12-2018 era effettuato un ulteriore ordine, a seguito del quale i militari si recavano presso il CMP di Bari per controllare tutta la corrispondenza in entrata, così accertando che la busta indirizzata all 'agente sotto copertura proveniva dalle cassette postali presenti nel comune di Barletta.

Era quindi predisposto un servizio di p.g. in collaborazione con Poste Italiane S.p.A., affinché il contenuto di ogni cassetta postale di Barletta fosse immesso in separati sacchi trasparenti riportanti l 'indirizzo della cassetta di riferimento, che venivano poi inviati al CMP di Bari; ivi gli operanti individuavano alcuni tagliandi Posta l all'interno dei sacchi provenienti da due cassette di invio site in Barletta, in via Dante Alighieri, n. 20 ed in via Giacomo Leopardi, n. 31; emergeva inoltre, come comunicato dal responsabile della distribuzione logistica di Poste Italiane S.p.A. per la regione Puglia, un considerevole flusso di vendita di tagliandi Posta1 presso una tabaccheria ubicata a Barletta, nei pressi della menzionata cassetta di via Giacomo Leopardi.

Erano, quindi, installate telecamere di sorveglianza a controllo remoto in prossimità delle due cassette postali di via Giacomo Leopardi e di via Dante Alighieri.

In data 17-3-2019, alle ore 18:30, era osservato un soggetto di sesso maschile imbucare numerose buste gialle, prima nella cassetta sita in via Dante Alighieri e poi nella cassetta sita m via Giacomo Leopardi; il soggetto risultava utilizzare un'autovettura Fiat Grande Punto di colore grigio, della quale non si distingueva chiaramente la targa, ma che recava un'evidente ammaccatura sul portellone del bagagliaio. L'analisi delle registrazioni delle telecamere fisse e dei varchi cittadini di Barletta consentiva di accertare, grazie all'intervallo di tempo rispetto alla spedizione e al segno particolare dell'ammaccatura, che l'autovettura recava la targa DS107YE; anche in data 26-9-2019, alle ore 17:50 circa, nei pressi della cassetta di via Giacomo Leopardi, veniva osservato lo stesso soggetto che, una volta sceso dall'auto in questione, imbucava una rilevante quantità di buste gialle.

Dal numero di targa si risaliva all'intestatario del veicolo, tale Ruscino Michele, nato a Barletta il 22-9-1964 ed ivi residente in via Canosa 240, tuttavia non identificabile nel soggetto immortalato dalle immagini delle telecamere di sorveglianza, in quanto evidentemente più giovane; quest'ultimo veniva identificato in uno dei due figli del Ruscino, tale Giannicola, nato il 4-5-1994, risultato dipendente (come da profilo Linkedln) della società MasterCoin, operante (come da sito internet) nel settore della

compravendita di criptovalute…sulla base di tali evidenze deve affermarsi una gestione comune della piattaforma Berlusconi Market da parte dei tre imputati…egualmente coinvolti nella gestione dei profili tecnici, organizzativi e finanziari del portale Berlusconi Market, anche, si è visto, in qualità di amministratori del sistema.

Prende così corpo e credito la prospettazione di accusa che vuole I tre imputati organizzatori di un'associazione a delinquere finalizzata alla commissione di un indefinito numero di reati riconducibili alle transazioni illecite concluse, anche da soggetti terzi (oltre che dal vendor g00d00), mediante l'utilizzo della piattaforma informatica gestita dai tre consociate[….]

Il portale Berlusconi Market costituisce strumento e veicolo che consente la conclusione – da parte del vendor g00d00 e dei restanti (e numerosissimi) venditori e acquirenti – di transazioni illecite, ciascuna delle quali costituisce singola ed autonoma ipotesi delittuosa, dalla materia degli stupefacenti a quella delle armi, solo per citare gli ambiti "merceologici" più eclatanti e di maggiore impatto".

Gli accertamenti condotti a seguito dell'arresto hanno riscontrato l'accumulo di proventi illeciti per 41 Bitcoin, circa 400.000,00 euro a dispetto di un volume complessivo di transazioni annue pari a 2 milioni di euro circa.

2.6 Dark web: i rischi per la sicurezza

Habitat naturale degli hacker piuttosto che dei criminali informatici, come più volte ribadito, è il dark web, ambiente in cui i pericoli maggiori sono originati dal cyber risk. *L'Institute of Risk Management*, ne parla come un *rischio dal quale deriva una perdita finanziaria, un'interruzione o un danno al sistema informatico addebitabile tanto ad eventi accidentali (spegnimento del server) quanto dolosi (furto di identità o dei dati sensibili).*

Una crew di pirati del *web* che rubano documenti, sottraggono denari dai conti correnti bancari, copiano le credenziali di accesso ai servizi internet. Ma quale la finalità ultima? Quella di monetizzare le informazioni: trasferire il denaro su un conto corrente, ritrasferirlo su un altro magari estero cosicchè si possa facilmente e rapidamente riciclare.

Stiamo parlando di operazioni di spionaggio industriale. I dati assunti illegalmente vengono trasferiti, previa corresponsione di ingenti somme di denaro (tecnica della double extortion - doppia estorsione) ad altrettanti cyber criminali.

Quando ci si accorge che le credenziali, i dati sono stati sottratti *fraudolentemente,* è ormai troppo tardi. Pertanto, Ted Ross, CEO & Founder, SpyCloud, consiglia di investire nella prevenzione: modello zerotrust.

"Per me, significa che se ho un dispositivo in mano, posso fidarmi solo delle cose che sto trasmettendo da quel dispositivo. Questo significa che non mi fido

della rete a cui sono collegato. Anche se sono al lavoro, non mi fido di ciò che ricevo, e-mail, SMS, di mia moglie, del consiglio di amministrazione o dei collaboratori. Sembra che sia una posizione molto difficile in cui operare. Ma se ti sforzi per un modello a fiducia zero sarai più sicuro".

Erik *Guldentops ha elaborato il modello "cloud".*

"I dispositivi IoT sono molto probabilmente meglio controllati da qualche azienda che ha una presenza in cloud. Le aziende devono infatti fare i conti con la carenza di competenze, il turnover, il fatto che non si possono patchare tutti i server e molte altre criticità. Ma non appena si sposta tutto ciò nel cloud, diventa responsabilità del provider cloud".

Ai due luminari fa da contraltare Edwards il quale riconosce l'errore umano nel configurare le reti ed i dispositivi, quale passpartout del crimine informatico: *"Forse stiamo vincendo una battaglia e non la guerra, ma è importante alzare le barriere all'ingresso".*

Il Rapporto Clusit 2021 sulla sicurezza ICT in Italia e nel mondo, redatto dall'Associazione Italiana per la Sicurezza Informatica, ha registrato un incremento degli *attacchi cyber* a livello globale del 12% rispetto allo scorso anno, 2020.

2.7 Dark web: la Cyber Threat Intelligence ed i suoi investigatori

Nel dark web non ci sono solo criminali ma anche pirati informatici buoni che cercano di individuare e prevenire le minacce.

Gli analisti dell'intelligence si infiltrano digitalmente nel *dark web* per limitare i danni di eventuali data breach, recuperare codici informatici trafugati, vulnerabilità informatiche 0-day[33], carpire informazioni, non accessibili con i convenzionali strumenti di ricerca, utili a sventare possibili cyber attacchi (*malware, attacchi zero day indirizzati verso software o verso le APT – advanced persistent threat che, apparentemente potrebbero rimanere celati nei server per molto tempo ma, contemporaneamente esfiltrano una miriade di dati*) a cui potrebbero essere esposti potenziali *target,* fino a definire con precisione la magnitudo dell'attacco e l'indicatore di compromissione (IOC).

I militari in forza ai Nuclei di Polizia economico-finanziaria ed al NucleoSpeciale Tutela Privacy e Frodi Tecnologiche (quest'ultimo con competenza sull'intero territorio nazionale) della Guardia di Finanza sviluppano attività di polizia giudiziaria nel cybercrime, nel dark web per contrastare i reati nel settore economico-finanziario con particolare riguardo al fenomeno delle criptovalute che, favorito dall'elevato grado di anonimità è in crescita esponenziale, monitorano costantemente la rete per individuare ipotesi di riciclaggio piuttosto che di finanziamento al terrorismo internazionale.

[33] virus o malware per computer in precedenza sconosciuto per il quale la protezione degli antivirus non è ancora disponibile;

L’articolo 2 del Decreto Legislativo n. 68 del 2001 conferisce al Corpo della Guardia di Finanza poteri di polizia tributaria, economico-finanziaria da impiegarsi nella ricerca, nella prevenzione e nel contrasto degli illeciti doganali, delle frodi nel corretto impiego di fondi pubblici nazionali e comunitari, all’evasione fiscale, alle accise, agli illeciti commessi nei mercati finanziari, immobiliari e che interessano valori, mezzi di pagamento, titoli, alle condotte di contraffazione di brevetti, marchi, indicazioni di origine e qualità della merce, del diritto d’autore, perpetrati con l’apporto di mezzi informatici e tecnologici.

I moduli di azione si indirizzano verso il controllo economico del territorio virtuale per scovare ed annientare eventuali “sacche di illegalità” attraverso l’intercettazione di flussi “finanziari sospetti”, la verifica della posizione fiscale dei soggetti “osservati” per recuperare a tassazione proventi illeciti, filtrare informazioni rinvenute con sofistiche tecniche di reperimento per isolare possibili cibernauti dediti ad attività illegali.

Il black market è il supermercato delle informazioni, vi si trova di tutto: documenti riservati, copie di corrispondenza per posta elettronica, credenziali di accesso alla rete ed ai server dei web aziendali, password, progetti industriali, numeri di carte di credito, ricerche di mercato, propaganda politica terroristica, pornografia, pedofilia; penetrarvi, per un verso conferisce un vantaggio altamente competitivo per la sicurezza aziendale ed istituzionale, per l’altro significa “conoscere il nemico ed i suoi intenti, anticiparne le mosse, rafforzarne i settori maggiormente a rischio e lacunosi”. Il lato oscuro del *web*

diventa la più importante fonte per la Cyber Threat Intelligence (CTI) ovvero per quell'attività di raccolta attraverso l'interrogazione di varie fonti (social media, report pubblicati dai vendor di antivirus, portali dedicati, *log* dei sistemi informatici, fonti giornalistiche, blog sulla cybersecurity, forum frequentati da *hacker*), delle informazioni relative ad attacchi informatici provenienti prevalentemente dall'interno della rete che potrebbero diventare offensivi per la sicurezza.

Gli analisti d'intelligence nella loro attività di raccolta, elaborazione, analisi delle informazioni seguono un format bene definito.

La prima fase consiste nell'andare a ricercare una parola chiave che può essere il nome di un prodotto o di un servizio. La fase due vede da parte dell'investigatore, una richiesta ben precisa agli utenti del web circa l'azienda e/o l'istituzione per cui in quel momento lo stesso sta lavorando. La terza è la fase del monitoraggio in cui gli *hacker* tentano di monetizzare i dati trafugati mettendoli in vendita. Se vogliamo questa è la fase più delicata in cui l'analista deve essere particolarmente scaltro. Non sempre le informazioni vendute sono vere, spesso i criminali truffano il potenziale acquirente fornendo documenti e/o dati falsi, a volte addirittura inventati semplicemente per arricchirsi illecitamente. Il patrimonio conoscitivo che gli stakeholder acquisiscono con la loro attività di Threat Intelligence deve essere successivamente tradotto e pubblicato in report e insight per consentire ai decisori politici di definire gli obiettivi, pianificare la costituzione di un'unità di governance che si occupi di

individuare prima e classificare poi i fattori di rischio in rapporto alle conseguenze che potrebbero generarsi ed alla probabilità che possano verificarsi come incidenti; porre in essere procedure di sicurezza strategicamente proattive che si traducano in un'operatività concreta nel prevenire gli attacchi informatici.

Un buon analista d'intelligence che navigherà nel *web* non mancherà di attivare le notifiche dagli strumenti e dalle piattaforme di supporto alla Cyber Threat Intelligence. In questo modo sarà prontamente avvisato su nuove ed importanti informazioni emerse ed altrettanto prontamente avvierà quell'attività d'indagine cruciale per impedire il presumibile attacco cyber.

2.8 Dark web: ipotesi di reato associativo

Le Autorità Giudiziarie, Magistratura e Forze di Polizia, per i reati commessi nel web, analizzando le condotte dei singoli criminali, si sono interrogati sulla possibile configurazione di un reato associativo ovvero più identità virtuali, con ruoli differenti possono originare gruppi organizzati? Ripercorrendo le origini dei black market che hanno fatto la storia del dark web (AlphaBay e Silk Road) la loro fama deve ricondursi all'utilizzo di software elettronici sofisticati ed alla mente criminale di sofisticati inventori - per AlphaBay Alexander Cazes e per Silk Road Ross Ulbricht) che avevano architettato una "impresa virtuale individuale" per produrre profitto. A tal proposito lo "European monitoring centre for drugs and drug addiction", con il report datato 2017 si esprimeva dicendo che "*la maggior parte dei fornitori sui mercati darknet erano venditori*

individuali, che distribuivano quantità limitate di sostanze diverse in base alla loro disponibilità"; in riferimento allo specifico scambio on line di sostanze stupefacenti in continua crescita, faceva notare "*il coinvolgimento dei gruppi criminali organizzati, che sono in grado di procurarsi maggiori quantità di stupefacenti e distribuirli a singoli acquirenti*", precisando che "*indagini* [mostrano] *lo spostamento dei gruppi criminali organizzati coinvolti nella produzione su larga scala di cannabis a base di erbe nell'UE ai mercati darknet per la distribuzione della loro produzione*".

Fa eco in Italia la sentenza n. 50620/2013 in cui nell'ambito dell'operazione "Tango Down" condotta dalla Polizia di Stato, gli uomini con l'ermellino, assimilano l'Anonymous ad "*un'organizzazione non statica, operante in una dimensione di per sé aperta e non individuabile su una base meramente territoriale*". La Cassazione ha guardato all'associazione per delinquere con una prospettiva a più ampio raggio: al concetto di territorialità circoscritta ha sostituito quello della "dimensione aperta", del cyberspace in cui attualmente il sodalizio criminoso opera.

Con la sentenza n. 20921/2013, riconosce la configurabilità del reato di associazione per delinquere in un caso di pornografia minorile in cui i sodali di una comunità virtuale operante alla stessa maniera del noto social network "PedoBook" si riunivano per scambiare e diffondere materiale pedopornografico. Quale poteva essere l'elemento che giustificasse, secondo i giudici di legittimità, il carattere associativo? Il processo di iniziazione a cui i

membri si sarebbero sottoposti al fine di creare il fondamentale vincolo fiduciario con gli altri aderenti. Accettando il vincolo, conoscendo l'illecito perseguito dalla comunità, l'appartenente poteva a tutti gli effetti considerarsi un associato del sodalizio criminoso.

Anche se risalente al 2020 non meno importante è la sentenza n. 10485 pronunciata dalla terza sezione dove la Corte cita espressamente l'approntamento di un mercato oscuro: "*l'allestimento di un sito di black market e la sua gestione* [siano] *indicativi dell'esistenza di un programma criminoso finalizzato alla commissione di una serie indeterminata di reati e, di conseguenza, della sussistenza di un sodalizio ex art. 416 cod. pen.*".

La sentenza *de qua* è significativa in quanto rimanda alla vicenda in commento al paragrafo 2.5.1.

Nel 2019 il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza conduce l'operazione "Darknet.Drug" che si conclude con l'arresto di tre italiani gestori del blak market denominato Berlusconi Market.

A conferma della misura della custodia cautelare in carcere secondo la ricostruzione dei fatti da parte del Giudice delle Indagini Preliminari, della pronuncia del Tribunale del Riesame di Brescia adito a seguito dei ricorsi presentati dagli italiani, la Corte riprende l'articolo 416 del codice penale, rubricato "Associazione per delinquere", "… *con la partecipazione di altri soggetti non identificati, con i nickname di Vladimir Putin di Emmanuel Macron (in qualità, rispettivamente, di amministratore e moderatore), mediante:*

l'apertura della piattaforma denominata Berlusconi Market, attiva nel cd. Dark Web; la gestione di un market on-line attraverso la fornitura del servizio e-commerce per l'offerta in vendita… di sostanza stupefacente, dati finanziari abusivamente sottratti, documenti di identità contraffatti, prodotti industriali contraffatti, armi da sparo anche da guerra ed esplosivi; la cura nella programmazione dell'interfaccia grafica della Home e delle bacheche dei cd. vendor, la gestione delle iscrizioni dei vendor, la pubblicazione e cancellazione dal pannello dedicato agli annunci di vendita, la gestione e il controllo contabile del wallet Bitcoin e dei depositi a garanzia cd. escrow…, l'offerta di supporto tecnico sistematico ai vendor mediante la gestione delle richieste di apertura di tickets, la gestione delle dispute tra i vendor; si [erano associati] *fra loro allo scopo di consumare una serie indeterminata di delitti in concorso, quali il contrabbando di armi, lo spaccio di sostanza stupefacente, la vendita dimonete contraffatte, la ricettazione… tutti delitti aggravati dalla transnazionalità della condotta*…".

All'obiezione, oggetto di ricorso, secondo cui la misura applicata ossia la custodia cautelare in carcere fosse troppo afflittiva, il Tribunale cautelare pronuncia il dispositivo che "…*in considerazione della natura e delle modalità del reato come concretamente contestato, una misura meno affittiva non sarebbe* [stata] *idonea a preservare il pericolo di reiterazione di analoghe condotte criminose, tenuto conto…che… la piattaforma Berlusconi Market* [era] *ancora attiva e che i ricorrenti, dotati di specifiche competenze informatiche,*

non [avessero] *voluto rivelare agli inquirenti le credenziali di accesso a detta piattaforma, credenziali che, quindi,* [avrebbero potuto] *continuare ad utilizzare anche in regime di arresti domiciliari mediante computer o anche smartphone, strumenti facilmente reperibili anche in ambiente domestico*".

2.9 Dark web: il successo di un'attività investigativa complessa

Le attività d'indagine info-investigative condotte in rete dalle Forze di Polizia sono particolarmente complesse ed articolate tanto che oltre all'utilizzo di specifici strumenti informatici, competenze professionali da parte degli operatori, necessita fare ricorso ad altre tecniche quali l'attività di OSINT (interrogazione delle fonti aperte), di SOCMINT (interrogazione dei social media), il monitoraggio dei black market attivi nel dark web, le operazioni undercover, l'utilizzo di strumenti basati sui software - malware e NIT (Network Investigative Technique), i c.d. "attacchi informatici", efficaci forme di cooperazione internazionale visto che il fenomeno sta assumendo dimensioni mondiali.

Ma cosa significa fare intelligence in rete? Utilizzare metodologie e tecniche**,** in passato ad appannaggio esclusivo dei servizi segreti governativi e militari, per l'analisi delle minacce**.**

L'Open Source Intelligence o interrogazione delle fonti aperte (Web Surface, Deep Web e Dark Web*),* branca dell'intelligence meglio nota con l'acronimo OSINT, è uno strumento di investigazione che, se ben utilizzato, anche con l'ausilio di particolari *tools*, permette di indagare, incrociare, analizzare, una

serie infinita di informazioni e controinformazioni. Non esiste, giuridicamente parlando una definizione univoca di OSINT quale ciclo di raccolta, elaborazione, produzione, classificazione e diffusione di informazioni assunte da fonti disponibili, non segrete o coperte, dunque aperte, facilmente accessibili, consultabili dal pubblico sempre nel rispetto della legalità. Per esempio in ambiente militare la Nato parla di OSINT come "*processo di raccolta, selezione, distillazione e diffusione di informazioni non classificate ad una comunità ristretta di operatori ed in relazione a specifici argomenti*".

Considerando le c.d. "User generated content" (file multimediali postati sui social o sui *forum* quali Wikipedia, Youtube, post con *hasthtag*) fonti aperte, consente di procurare quelle notizie utili per l'attività d'indagine che non sarebbero facilmente acquisibili attraverso l'interrogazione delle banche dati istituzionali.

Due sono i principi fondamentali su cui l'OSINT si articola: l'informazione intesa come contenuto informativo e la fonte di cui l'analista si serve per entrare in relazione con l'informatore valutandone l'attendibilità atteso il crescente fenomeno delle fake news e la paternità al fine di sviluppare una corretta valutazione delle stesse.

L'analista nella sua attività di ricerca e raccolta delle fonti deve, altresì, considerare quanto le stesse siano aggiornate: le fonti di cui l'OSINT si serve sono i classici mezzi di comunicazione - giornali, emittenti televisive, radiofoniche, periodici -, le osservazioni dirette attraverso fotografie amatoriali

o geoferenziate satellitari, conversazioni ascoltate, professionisti e studiosi che hanno preso parte a conferenze, attività convegnistiche, autori di opere o pubblicazioni, dati pubblici assunti attraverso i piani finanziari, i rapporti informativi.

L'intelligence informatica si avvale di altrettante fonti di ricerca: la HUMINT che attenziona gli informatori, l'IMINT le immagini satellitari, la SIGINT le intercettazioni, il MASINT gli strumenti di indagine scientifica.

Il percorso di intelligence nel *web* si articola nelle 4 fasi di "planning and decision", "collection", "processing and exploitation", "analysis and production".

La prima fase consta nella pianificazione dell'obiettivo: identificazione, determinazione delle esigenze informative, decisione sulla tecnica di raccolta, analisi e successiva elaborazione. L'operatore indica le strumentazioni ed il personale da impiegare attribuendo a ciascuno di loro un ruolo specifico.

Nella fase di "collection" si ricercano specifiche pagine *web* e si raccolgono, attraverso tecnologie o risorse umane, i dati rilevanti, inerenti, significativi verificandone ed accertandone l'affidabilità.

Nella terza fase, "processing and exploitation" si selezionano e valutano gli indicatori; per meglio intenderci: i dati grezzi raccolti vengono interpretati, tradotti, convertiti per essere utilizzati come informazioni "organizzate", successivamente analizzate avvalendosi di metodologie quali la decrittografia,

la traduzione in lingua o l'organizzazione e l'indicizzazione dei dati per la standardizzazione in campi.

Attraverso la fase di "analysis and production" si procede all'estrapolazione e contestuale interpretazione delle informazioni in correlazione all'obiettivo che ci si è prefissati. Consta di 3 step:

l'analisi, in cui l'analista continua a studiare ed a valutare i fatti scorporandoli in segmenti per meglio studiarne le caratteristiche, correlandoli con le altre fonti delle informazioni raccolte; l'integrazione; si procede ad assemblare le informazioni raccolte per renderle fruibili in base agli obiettivi stimati; la disseminazione cioè la propagazione del risultato dell'attività info-investigativa condotta.

Nell'ambito dell'OSINT, la Social Media Intelligence - SOC.M.INT. -, è l'attività d'intelligence indirizzata ai social media comprensivi di blog, video, chat, forum, audio, siti social atti ad agevolare e sviluppare i rapporti interpersonali tra gli individui: solo per citarne alcuni facebook attraverso cui si esprimono emozioni e stati d'essere, twitter per comunicare brevi emozioni, instagram e foursquare per condividere rispettivamente foto e luoghi, linkedin per i professionisti, badoo e meetic per le relazioni affettive, youtube per i video.

L'interrogazione dei predetti *network* consente di conoscere le opinioni politiche, gli stati psicologici, le passioni, le condizioni di vita economico-sociali, i rapporti di lavoro di ogni singolo cibernauta: in una parola *"monitorare"* il soggetto. Si guarda quindi alle relazioni sociali tramite la teoria delle reti in cui

le relazioni sono rappresentabili da collegamenti – archi – tra individui – nodi – che possono illustrarsi attraverso grafi - SNA. E' con la navigazione internauta che il "soggetto attenzionato" lascia le proprie "impronte digitali".

L'investigatore professionista e professionale sa bene che ciò che contraddistingue i social media sono la proprietà (alto livello di pertinenza), l'immediatezza, l'usabilità (essendo intuitivi sono facilmente accessibili), la volatilità (i post eliminati sono difficilmente recuperabili), il dialogo e l'interazione (è possibile interagire e condividere elementi), immersività favorita dalla trasparenza, pertanto, deve circoscrivere l'obiettivo investigativo individuando le peculiarità mirate allo scopo attraverso l'aggiornamento degli strumenti utili per l'indagine (cultura, religione, interessi nazionali o del singolo ecc..).

Deve essere attento ad incrociare i dati ottenuti dal ciclo di intelligenceapplicato ai canali interni alla SOC.M.INT. con quelli più "raffinati" (per esempiola SNA – *Social Network Analysis* -, utile nell'individuare i "nodi" più importantiall'interno delle reti sociali) derivanti dalle ulteriori analisi condotte sfruttando altri strumenti.

Va da se' che l'attività investigativa di SOC.M.INT. per originare un'informazione utilizzabile non può limitarsi all'analisi di un unico *social network* e magari proprio quello alimentato dal soggetto monitorato che potrebbe introdurre notizie non veritiere ma deve esaminare ed incrociare più fonti.

Le recenti attività di OSINT condotte in riferimento ai *social network* vedono gli investigatori porre particolare attenzione verso la *"somiglianza culturale"* in rete tra identità solo apparentemente differenti.

Attraverso questo indicatore si scremano, tra le svariate informazioni di cui nel *web* si dispone, quelle che possano far convergere, su piattaforme differenti, comportamenti, atteggiamenti verso una stessa identità[34].

Affinchè un report sia funzionale all'attività di intelligence è opportuno che sia *celere* ovvero deve essere ultimato nel rispetto delle scadenze prestabilite (se tardivo non è più utile), comprensibile e fruibile a tutti non solo agli esperti del settore, quindi il linguaggio deve essere molto fluido, poco tecnico e le informazioni assunte confidenzialmente, suffragate da fonti di prova verificabili in qualsiasi momento e quindi producibili nelle sedi pertinenti.

Anche il format che si sceglie per redigere il report deve essere il più funzionale allo scopo. L'*optimum* sarebbe disporre di piattaforme di intelligence con capacità di crawling e gathering di dati, di link analysis ed eventualmente di analisi deduttiva per supportare gli analisti umani.

L'attività di analisi si avvale di diversi software che forniscono preziosi risultati tipo "Whois" - protocollo di rete che consente, mediante l'interrogazione di

[34] Si ricordi il caso Ross Ulbricht. Fondatore di Silk Road è stato possibile identificarlo grazie all'analisi dei suoi profili pubblici sui social network utilizzando proprio la "somiglianza culturale" che ha permesso una comparazione con i profili di tale Dread Pirate Roberts pseudonimo dello stesso Ulbricht. La somiglianza riguardava discorsi pubblici e post riconducibili alle teorie libertarie dell'economista austriaco Ludwing von Mises che, secondo Ulbricht potevano considerarsi *le basi filosofiche di Skill Road;*

appositi database server da parte di un client, di stabilire a quale provider Internet appartenga un determinato indirizzo IP per risalire non solo all'identità del titolare del dominio ma, altresì, al suo amministratore, a conoscere la data di creazione del sito, al suo ultimo aggiornamento; "Waybackmachine", una sorta di "libreria digitale", un patrimonio informativo comprensivo di oltre 330 miliardi di pagine web, raccolte già dal 1996 ad opera dell'organizzazione non-profit "Internet Archive"; "HTTrack", attraverso il *download* di un intero sito ne conserva una copia analizzabile off line, che potrà essere usata anche come fonte di prova; "Geosetter": grazie ad una comoda interfaccia dotata di una mappa interattiva consente di aggiungere a qualsiasi foto memorizzata nel PC le informazioni concernenti la posizione geografica, i c.d. "geotag", unitamente agli analizzatori rispettivamente di profili Facebook e Twitter, "Facebook Investigative Toll" e "TwitterForencis".

Condurre una attività d'indagine sui siti "proprietari" e su quelli "di intermediazione" significa acquisire la notizia di reato monitorando la rete, riscontrare le informazioni apprese, localizzare ed identificare gli utenti, i server o altri dispositivi collegati alla rete attraverso l'acquisizione di un indirizzo IP o la geolocalizzazione del "caller id".

Gli investigatori della rete per ricostruire virtualmente il percorso di compravendita di un bene o di un servizio illegale, creano un website profiling per infiltrarsi sul mercato oscuro e raccogliere il maggior numero di elementi informativi presenti in rete da materializzare.

Creare il profilo di un sito web è un'operazione laboriosa e particolarmente complessa che mira a comparare le notizie estratte dal web attraverso il monitoraggio di forum, blog, chat con gli elementi assunti nella classica attività investigativa per farli convergere verso l'identità sospettata.

2.10 Deep Web: altra pagina oscura della rete

Coniato da Michael Bergman, Il termine "deep web" indica "parts of the World Wide Web whose contents are not indexed by standard search engines for any reason", vale a dire *"le parti del World Wide Web i cui contenuti non sono indicizzati dai motori di ricerca standard, per qualunque ragione".*

Analizzando etimologicamente i termini della definizione, *"parts of the World Wide Web"* si riferisce ai servizi offerti da internet con il protocollo http;

"whose contents are not indexed" i cui contenuti non compaiono tra i risultati dei motori di ricerca in quanto non indicizzati; *"by standard search engines"* per cui i motori di ricerca globali e ad accesso non privilegiato che si utilizzeranno per navigare saranno i classici Googlem Bing; "for any reason": si è detto che i contenuti non sono indicizzati, il motivo non è dato sapere; errore di programmazione? Accesso riservato alla pagina? La definizione riportata potrebbe apparire poco esaustiva e fuorviante al punto da creare un parallelismo tra una pagina raggiungibile accedendo ad un motore di ricerca interno di un sito indicizzato su Google ed una pagina ad accesso privilegiato il cui indirizzo IP è conosciuto solo ad una ristretta cerchia di persone. Per fare chiarezza nel calderone del "deep web" ci si servirà di variabili capaci di

quantificare la profondità della pagina web. Il primo parametro da considerare è la presenza del collegamento[35] della pagina non indicizzata ad altrettante indicizzate, per esempio il backoffice di un blog che per raggiungerlo necessita del semplice collegamento “accedi” che diventa accesso privilegiato, il secondo parametro della nostra spiegazione. L’accesso si definisce privilegiatoperché può bloccare gli spider dei motori di ricerca o gli utenti e, a seconda seper concederlo l’amministratore del sito applica criteri selettivi o non ne consente la registrazione può o meno essere esclusivo: l’esempio è l’accessoa darknet privati ed alle pagine web contenute al suo interno. Il terzo ed ultimoparametro è l’indirizzabilità, cioè la composizione degli URL delle pagine web, che possono essere indirizzi semantici ed indirizzi non semantici. Il primo è composto da una sequenza alfanumerica nella parte del dominio esclusa l’estensione cui corrisponde un significato in una certa cultura o in una determinata realtà: per esempio, www.casa.it o www.repubblica.it.

Un indirizzo non semantico presenta ugualmente una stringa alfanumerica nella parte del dominio esclusa l’estensione ma non p significante in una specifica cultura o realtà (www.abcdefg.i2p, www.hilmno.onion).

La differenza tra indirizzi semantici e non semantici, porta a considerare un quarto parametro “la conoscenza di” un indirizzo di una pagina che attesta quanto la stessa sia profonda.

[35] Centerfor Internet Security, 2015;

Capitolo 3 - La legalità delle criptovalute ed i crimini finanziari

3.1 Le criptovalute: il protocollo Bitcoin

Da qualche anno la rete internet nella sua parte più oscura – black market "… *la nuova frontiera del crimine transnazionale, finanziario e informatico, su cui si concentra l'impegno delle forze di polizia di tutto il mondo*"[36] -, è diventata una piattaforma di e-commerce*,* di scambio merce di qualsiasi natura, molto allettante.

Nello spazio virtuale oscuro, il dark web, si genera un ingente volume d'affari stimato in circa 100 milioni di dollari annui che attraverso la compravendita di beni e servizi, per lo più illeciti, rende ricchi abili criminali che navigano in "anonimato" grazie ad appositi browser tipo il già menzionato TOR utilizzando quale mezzo di pagamento per le transazioni, moneta virtuale apparentemente non tracciabile: basti pensare ai protocolli Bitcoin - BTC[37] ma ce ne sono altrettanti che elenchiamo - *PPcoin* (PPC), *Litecoin* (LTC) – per citarne alcuni, che utilizzano algoritmi e formule differenti, ma che derivano, quanto alla loro

[36] Vds. "Relazione annuale 2019" della Direzione nazionale antimafia e antiterrorismo, nella quale viene richiamata – tra l'altro – l'azione denominata "OAP Carding Action 7.1", nell'ambito di un'importante azione EMPACT a leadeship italiana, che ha visto la partecipazione di investigatori di 9 Paesi europei ed esperti di Europol, coordinati dalla Polizia postale e delle comunicazioni. Tale azione ha condotto all'individuazione di numerosissimi account riconducibili a sodalizi criminali transnazionali attivi nel reperimento e nella commercializzazione illegale di dati personali e codici bancari;

[37] Con l'iniziale maiuscola si descrive il protocollo (o la rete) sul quale si regge la moneta virtuale. Con l'iniziale minuscola, ci si riferisce alla moneta stessa, vale a dire all'unità di conto;

struttura di fondo, proprio dai *bitcoins*[38], Ethereum (ETH): – piattaforma pubblica block chain, si badi - che permette la creazione di *"*Smart Contracts*"* - letteralmente contratto intelligente - cioè dei protocolli informatici che favoriscono, fanno rispettare e verificano la negoziazione o l'esecuzione di un contratto dal quale è esclusa totalmente o parzialmente alcuna clausola -, attraverso la criptovaluta Ether – token - che i partecipanti alla rete acquistano per utilizzare la potenza di calcolo; Bitcoin Cash (BCH), "hard fork" della criptovaluta Bitcoin è nata nel 2017.

La sua dimensione di blocco a 8 MB lo rende incompatibile con la blockchain del Bitcoin; Ripple (XRP), è una moneta protetta da misure di sicurezza tali da evitare la duplicazione e la falsificazione attraverso, ad esempio, funzioni di *hash crittografico* e meccanismi di convalida che, semplificando, tracciano la storia di ogni singolo conio digitale al fine di impedire frodi. Nata nel 2013 è una criptovaluta molto volatile in quanto garantisce la possibilità di scambiare e trasferire, rapidamente, moneta senza continuità di forma; IOTA, nata nel 2015, l'obiettivo era rendere più rapide le transazioni tra dispositivi connessi tramite l'IOT (Internet of things) dove le informazioni sulle transazioni sono organizzate in una struttura detta tangle anziché nella tradizionale blockchain; Waves (WAVES) è quella con la block chain decentralizzata più

[38] Per approfondimenti si veda *http://www.cryptocoincharts.info/coins/info*, *https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies*, *http://digitalcoin.altervista.org/le-migliori-alternativa-al-bitcoin/* e *https://coinmarketcap.com*;

veloce ed intuitiva: gli utenti utilizzatori possono creare token[39] monetari senza alcuna nozione in termini di programmazione informatica; Monero introdotta nel mercato sommerso nel 2014. Rispetto alle altre monete elettroniche Monero non basandosi su una block chain pubblica assicura agli utenti una maggiore privacy tanto che nelle transazioni in cui la stessa è impiegata non c'è tracciabilità: infatti non è possibile risalire né al mittente né all'importo ed utilizzando per la sua implementazione l'algoritmo CryptoNote, attualmente riscuote maggior successo dei bitcoins ed è maggiormente quotata.

La criptovaluta Zcash (ZEC) offre la privacy e la trasparenza selettiva delle transazioni tanto da divenire la valuta preferita dei riciclatori di denaro sporco. I pagamenti Zcash sono divulgati su una blockchain pubblica, ma il mittente, il ricevente ed il valore della transazione possono rimanere privati in quanto la tecnica di crittografia chiamata zk-Snark[40] usata, garantisce la riservatezza della transazione: ai terzi sono sconosciuti sia l'ordinante che il beneficiario.

---

[39] Insieme di informazioni digitali all'interno di una blockchain che conferiscono un diritto di proprietà a un determinato soggetto. L'Osservatorio Digital Innovation del Politecnico di Milano definisce un token come "*un'informazione digitale, registrata su un registro distribuito, univocamente associata a uno e un solo specifico utente del sistemae rappresentativa di una qualche forma di diritto: la proprietà di un asset, l'accesso a un servizio, la ricezione di un pagamento, e così via";*

[40] Si tratta di una nuova tecnologia di tipo "zero-knowledge proof" ("Dimostrazione a conoscenza zero") che richiede meno potenza computazionale di altre soluzioni simili. In informatica applicata per "zero-knowledge proof" si intende un sistema per cui un computer effettua una verifica su un'affermazione senza sapere altro che la dichiarazione di veridicità che gli viene trasmessa. È un concetto un po' complesso a livello teorico, ma più semplice se lo si applica. Un sistema del genere viene usato in diversi casi su Internet, ad esempio lo si può utilizzare per farsi autorizzare all'accesso in un sistema, inserendo una password ma senza dover necessariamente trasmetterla. Il protocollo ideato dai ricercatori di ZCash, nello specifico, permette agli utenti di provare che possiedono le monete che vogliono spendere senza rivelare però altre informazioni riguardo la

Il market in rete funziona esattamente come un negozio reale; vi è un amministratore che, previo compenso, assegna ad ogni singolo venditore uno spazio espositivo dove poter esporre, *virtualmente*, la propria mercanzia.

Le clausole giuridiche relative all'occupazione degli spazi, vengono definite **in** privato, (spesso si utilizzano le chat cifrate per mantenere l'anonimato che il sistema assicura), direttamente tra il venditore e l'acquirente che paga con moneta elettronica. Il fenomeno che ci si appresta a trattare presenta due caratteristiche, la globalità in quanto le piattaforme di vendita proprio perché virtuali possono appoggiarsi ad infiniti *server* sparsi in tutto il mondo e la mutabilità che si concretizza nella rapidità e facilità che si possono avere nell'aprire e chiudere un mercato on line.

Nei dark market come si è accennato, le transazioni commerciali più o meno anonime o pseudo anonime, si perfezionano con lo scambio di criptovalute, valute digitali che il legislatore nel d.lgs. 25 maggio 2017, n. 90, che ha novellato il d.lgs. 21 novembre 2007, n. 231 definisce "*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*[41]*".* Essendo moneta digitale non ha corso legale,

provenienza o la destinazione, cioè senza indicare da quale portafoglio sono arrivate né in quale finiranno;

[41] Si distingue dalla moneta elettronica, descritta dal TUB (Testo Unico Bancario) come: "*il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per*

ossia non vi è un ente erogatore legittimato e riconosciuto: qualunque privato può generarla attraverso un protocollo informatico definito dal mittente a cui gli interessati devono adeguarsi tanto che l'accettazione, quale mezzo di pagamento, è facoltativa. Infatti è proprio nel termine che si cela quell'anonimato che induce gli esperti di finanza a non classificare il *bitcoin* come moneta di scambio il cui valore, invece, si basa su domanda ed offerta[42]. Criptovaluta deriva dall'inglese *cryptocurrency*[43] che è l'unione di *cryptography* - *crittografia* (la privacy è garantita) – e di *currency* – *valuta*. La sua origine è ancora anonima: la storia narra di un documento apparso su *bitcoin.org* - dominio registrato in Finlandia -, a firma di tale Satoshi Nakamoto. Era la notte di Halloween del 2008 ed il suddetto documento riproduceva un *codice* (Bitcoin) e la prima versione di un software open source che sarebberodiventati il fondamento teorico della moneta virtuale[44]. Chi fosse SatoshiNakamoto non è dato sapere: un autore ignoto e misterioso, un documento reso pubblico la notte di Halloween facevano chiaramente pensare ad uno scherzo, ma così non fu…solo nel 2016 l'imprenditore australiano Craig Wright[45] se ne assume la paternità confutata dall'esibizione delle chiavi di

effettuare operazioni di pagamento (…) e che sia accettato da persone fisiche e giuridiche diverse dall'emittente";

[42] Ogni giorno il valore di questa moneta cambia: per tenere sotto controllo la valutazione giorno per giorno o in un determinato taglio temporale, si può consultare il sito https://www.money.it/+BitCoin-Euro-Quotazione che controlla in tempo reale l'andamento del valore del BitCoin;

[43] Ne parla per la prima volta l'ingegnere informtico Wei Dai nel 1998;

[44] K.L. PENROSE, *Banking on Bitcoin*, in *North Carolina banking Institute*, 2013, 530 ss.;

[45] G. DE MIZIO (2015), *"Trovato il creatore di Bitcoin? La criptovaluta andrà comunque per la sua strada"*, in *http://it.ibtimes.com/trovato-il-creatore-di-bitcoin-la-criptovaluta-andrà-*

crittografia che fanno funzionare il sistema di pagamento e possono essere detenute solo dal suo creatore.

Se il lettore prestasse attenzione al funzionamento del protocollo Bitcoin si accorgerebbe che di intermediari finanziari non se ne parla.

La struttura si orienta sul “wallet”, sul “block chain” e sul “mining”.

Il primo è una sorta di portafoglio virtuale di accumulo della valuta contenente due chiavi, una pubblica che non solo identifica il wallet ma funge da indirizzo: costituisce l’identificativo dell’utente del *network*, ma non fornisce alcuna informazione riguardo il legittimo proprietario, (è paragonabile alle credenziali identificative del conto corrente bancario) ed una privata, segreta, attraverso il cui accesso il titolare del portafoglio, dopo aver creato un proprio *account* su uno dei tanti siti che svolgono la funzione di interfaccia, può disporre della criptovaluta in esso depositata ed autorizzarne il pagamento all’utente proprietario di quella specifica chiave pubblica. Il sistema a crittografia asimmetrica, fa sì che la quantità di criptovaluta che il soggetto A vuole inviare al soggetto B affinchè solo lui possa disporne, debba essere trasmessa, crittografata asimmetricamente con la chiave pubblica conferitagli da B; in questo modo A, non disponendo della chiave privata di B che solo lui possiede,

comunque-per-la-sua-strada-1429717. A prova di ciò ci sono email del 2009 con testo “La versione beta dei *bitcoin* sarà live domani. È decentralizzata. Proveremo finché funziona” o ancora “Craig, penso che tu sia pazzo, ma credo in quello che stiamo provando a fare”. Le perquisizioni a casa dell’informatico hanno inoltre rivelato la presenza di due super-computer, dediti all’attività di *mining*;

non potrà più disporre del denaro digitale generato elettronicamente e protetto da crittografia.

Al contrario se B volesse notiziare A sull'esito dell'operazione criptata mantenendo il medesimo livello di riservatezza lo potrà fare usando la *chiave pubblica* di A il quale userà la propria chiave privata per la decriptazione dei dati ricevuti[46].

Di "wallet" esiste l'"hot wallet" ed il "cold wallet" dove l'"hot" è un software disponibile all'utente per l'invio e la ricezione di criptovalute attraverso una connessione internet: nonostante custodisca le chiavi pubblica e privata di criptazione per l'accesso al salvadanaio virtuale, è esposto a notevoli rischi informatici derivanti dal fatto che i server potrebbero essere oggetto di attacco cyber (ransomware) e quindi i dati in essi memorizzati e/o le criptovalute potrebbero facilmente essere trafugati.

Diverso è il meccanismo di funzionamento del "cold wallet". Anch'esso portafoglio elettronico memorizza e custodisce le chiavi di accesso, pubblica e privata, in un luogo non connesso alla rete. *Ergo* la chiave privata che consente l'accesso al saldo del portamonete non è registrata in alcun software ma direttamente nella disponibilità e nella custodia del possessore.

La seconda e più importante sfaccettatura del protocollo è il "block chain", tecnicamente *"catena di blocchi"*. E' una sorta di *"registro mastro"* di Bitcoin

[46] Nel caso contrario, invece, il sistema risulterebbe inefficace atteso che se si dovesse criptare un messaggio utilizzando la chiave privata, chiunque – in possesso della chiave pubblica associata – sarebbe in grado di decifrarlo;

non gestito a livello centralizzato ma a livello collettivo[47] dai nodi cioè da tutti coloro che aderiscono al *network* in quanto basato sulla tecnologia del "peer-to-peer*"* (da pari a pari)[48]; un database in cui sono riportate tutte le transazioni che si eseguono nell'intero sistema e verificabili da ogni singolo utente.

Il registro è suddiviso in blocchi di transazioni ed ogni nuovo blocco è legato al precedente creando, appunto, una *"catena dei blocchi"*.

Con questa tecnologia affinchè l'operazione in essere possa definirsi e divenire irreversibile è necessario che la stessa sia validata[49] da più del 50% della potenza computazionale (utenti aderenti) della rete a supporto del Bitcoin.

Si viene a creare una sorta di "catena di firme digitali" che permette a chi riceve un pagamento di verificare la concatenazione delle diverse transazioni sul medesimo "gettone" - *cybercoin* - che da "non confermate" divengono "confermate": si evita in questo modo, il fenomeno della doppia transazione - double-spending -.

Il terzo ed ultimo componente è costituito dal "mining", letteralmente minare, estrarre. Trattasi di una vera e propria operazione di fabbricazione di denaro

[47] In maniera distribuita: un sistema distribuito è costituito da un insieme di applicazioni, logicamente indipendenti, che collaborano per il perseguimento di obiettivi comuni attraverso una infrastruttura di comunicazione hardware e software. Esso garantisce una maggiore flessibilità nell'organizzazione delle attività, permettendo ai client di essere configurati in modo da svolgere attività tra loro differenziate e di ridurre il carico operativo sul sistema centrale;

[48] L'implementazione di Bitcoin si basa su uno schema proof-of-work per difendersi dalla contraffazione digitale ed utilizza tecnologie peer-to-peer su reti i cui nodi sono computer di utenti sparsi per tutto il mondo;

[49] Ognuno di questi blocchi viene sviluppato dalla comunità dei miner, che alla fineottengono una Proof of Work facilmente verificabile senza necessità di particolare potenza computazionale da parte di qualsiasi utente della rete Blockchain;

digitale, generato elettronicamente dai c.d. “miners” attraverso combinazioni di calcolo (algoritmi) e hardware progettati per lo scopo - Bitcoin Miner -, tra blocchi di transazioni – bitcoin*s*aumenti - e protetto da crittografia.

La manodopera del miner è remunerata sotto forma di ricompense se crea un nuovo blocco o di commissioni per aver incluso, nel blocco, una transazione in modo corretto.

Frequenti sono i casi di Crime-as-a-Service (*CaaS*), dove criminali informatici qualificati predispongono piattaforme tecnologiche che vendono o affittano ad altri criminali poco esperti di conoscenze tecniche per gestire la propria attività illecita.

3.1.1 Le criptovalute: un caso di scuola

Come potrebbe funzionare un acquisto nel dark web? *Avvenuto i*l pagamento in *bitcoins* da parte dell’acquirente, il venditore concentra la merce in un luogo segreto e invia al compratore il link con le coordinate di Google Maps tramite un qualunque sistema di messaggistica anonima; verificata la merce, il compratore invierà un codice di sblocco che permetterà al venditore di incassare i bitcoins, secondo un sistema che impedisce al compratore di riprendere i bitcoins qualora non invii il codice di sblocco. Il sistema ha dunque una garanzia ambivalente, sia per il compratore che per il venditore.

3.2 Da cosa dipende la legalità di una criptovaluta? i crimini finanziari

L'anonimato in rete (ogni operatore è individuato da una stringa alfanumerica) è diventato una prerogativa di diritto e di difesa dei nostri dati, delle nostre immagini, delle nostre corrispondenze, insomma della nostra vita.

Oggi tutto è registrato e rintracciabile in rete…il web è un mercato in cui l'utente ha l'imbarazzo della scelta su cosa acquistare ma non sempre gli scambi sono trasparenti e leciti.

Nei portali e-commerce attivi nel dark web, i tanto acclamati "black market" l'offerta di prodotti è variegata: traffico di esseri umani, racket, contrabbando di specie in via di estinzione, vendita di droghe illegali, prostituzione illegale, schiavitù infantile e qualsivoglia altra attività che origini transazioni finanziarie ritenute illegali.

Nella shadow economy o economia sommersa i "crimini finanziari[50]" si determinano in quanto le transazioni si perfezionano con lo scambio di valute digitali, criptovalute che consentono pagamenti anonimi o quasi.

Le monete virtuali sono presenti sul mercato on line con un proprio valore non certamente attribuito dall'Autorità Governativa ma stabilito dall'incontro di interessi, quello del compratore ad approvvigionarsi di merce che in una

[50] come definito dall'Australian Criminal Investment Commission (Financial Crimes, 2019) include attività che vanno dalla frode alla manipolazione attiva del mercato azionario o al riciclaggio dei proventi del crimine;

normale condizione di compravendita non potrebbe acquistare perché illecita e quello del venditore di monetizzare secondo trattative private.

Il sistema legittimizza i criminali finanziari a riciclare digitalmente **-** (cd. Cyberlaundering*)* proventi derivanti da attività illegali, trarre vantaggi da operazioni criminose mascherate con gravi ripercussioni sulle politiche monetarie e fiscali attuate dagli Stati e dalla Banca Centrale Europea che finiranno per delegittimare la democrazia.

Gli impatti che ne deriveranno intaccheranno il settore economico (quanto le criptomonete incideranno sul tasso inflazionistico), la politica monetaria nei suoi profili fiscale-finanziario-tributario anche in considerazione di un possibile regime di tassazione e di regolamentazione (chi sarà l'ente erogatore e l'ente pagatore, dove e quanto si potrà pagare, si potranno contrarre prestiti e/o mutui), legale (acquisto illecito di ogni materiale fino alla riscossione di quote di riscatto, sottoscrizione di contratti tra pubblici e privati nella forma di transazioni con moneta criptata), sociale (le interazioni virtuali saranno illimitate e sfuggiranno ad ogni forma di controllo).

Come mai il bitcoin sta diventando una merce tanto "preziosa" quanto limitata, un "metallo raro"? Perché il bitcoin non può essere prodotto all'infinito: aprioristicamente è lo stesso algoritmo generatore che ne ha fissato in 21 milioni la quantità massima da immettere sui mercati (fino al 2140) tanto che l'algoritmo utilizzato è strutturato in maniera inversamente proporzionale:

all'aumentare dei bitcoins in circolazione la produzione dei medesimi diventa più complessa e meno redditizia.

3.3 Assenza di una normativa giuridica ad hoc

Il protocollo Bitcoin autorizza lo scambio di monete tramite internet tra due entità che possiedono un indirizzo Bitcoin ed una connessione *peer-to-peer*, per cui se ne deduce che nessuna autorità può bloccarne il trasferimento. A questo punto sorge spontanea la domanda ma il Bitcoin è legale e come si concilia con quanto statuito all'art. 1277 del codice civile rubricato "Debito di somma di danaro"? E' regolamentata la circolazione ed il relativo utilizzo?

In Europa si guarda a queste nuove forme digitali di pagamento già dal 2022; la direttiva 2000/46/CE (recepita in Italia con legge 1° marzo 2002, n. 39), all'art. 1, offre per la prima volta una definizione di "moneta elettronica" (si riferisce anche ai bitcoins?) in questi termini: "*un valore monetario rappresentato da un credito nei confronti dell'emittente che sia memorizzato su un dispositivo elettronico, emesso previa ricezione di fondi di valore non inferiore al valore monetario emesso e accettato come mezzo di pagamento da soggetti diversi dall'emittente*".

La direttiva 2009/110/CE (recepita in Italia con d.lgs. 16 aprile 2012, n. 45) che ha abrogato la precedente, ha altresì introdotto una nuova definizione di moneta elettronica (sono compresi i bitcoins?) considerando tale *"ogni valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente, che sia*

emesso e accettato per effettuare operazioni di pagamento da persone fisiche e giuridiche diverse dall'emittente".

Se così stanno le cose la moneta virtuale è da intendersi paritaria ad un diritto di credito che il titolare vanta nei confronti dell'istituto emittente; circolando quindi secondo la regolamentazione dei titoli di credito al portatore non può collimare con la portata contenutistica dell'art. 1277 c.c.: *"I debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento e per il suo valore nominale".*

Ancor di più si può affermare, *rectius,* che il bitcoin è moneta virtuale e non elettronica (di cui la norma parla) che non ha corso legale. Entrambe le direttive quando citano l'aspetto elettronico della moneta lo fanno in riferimento al fatto che la stessa debba essere conservata elettronicamente, debba essere emessa previo deposito di fondi in una percentuale non inferiore al valore monetario emesso, debba essere accettata come mezzo di pagamento da soggetti differenti dall'emittente. Se il lettore riprendesse il paragrafo in cui si evidenziano le caratteristiche dei bitcoin, soffermandosi sulla fase del mining, si renderebbe immediatamente conto che stona, in qualche punto, con le direttive: dove nello specifico? Nella fase di fabbricazione della moneta che viene condotta senza la preventiva dazione di fondi il cui valore dovrebbe equivalere a quello del valore monetario emesso.

A colmare, apparentemente, il *gap* normativo interviene la direttiva europea 2007/64/CE che stabilisce le norme in materia di esecuzione delle operazioni

di pagamento semprechè i fondi siano moneta elettronica (non sono ancora compresi i bitcoins che come si è già dato conto sono moneta virtuale *strictu sensu*) ma lascia, per l'ennesima volta, non disciplinate le forme di emissione della moneta: si potrebbe quasi pensare che una direttiva europea metta in concorrenza le Banche Centrali con gli strumenti tecnologici emissori di valuta. L'annosa natura dei bitcoins e della loro regolamentazione nel mercato rimane ancora irrisolta seppure la Banca Centrale Europea ha riferito che, in sede di Comitato dei pagamenti della Commissione Europea, *"è stata avviata una discussione atta a comprendere come configurare il BTC verso uno schema di moneta legalmente riconosciuta in Europa*[51]*, anche in considerazione dell'ampia diffusione di tale modalità di pagamento e del fatto che la stessa permette "scambi" a costi di transazione decisamente inferiori rispetto ai normali servizi di pagamento disciplinati dalla direttiva del 2007".*

Nel 2015 la Corte di Giustizia dell'Unione Europea definisce la questione ed emette una sentenza *"The exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT"*[52] che esenta ogni tipo di criptovaluta e quindi anche i *bitcoins* dal pagamento dell'IVA, imposta sul valore aggiunto, riconoscendoli quali strumenti di pagamento legittimi in Europa.

[51] Resoconto della riunione del *Payment Committee* avvenuta il 21 marzo 2012, Dg. mercato interno e servizi –PC/005/12-, in *ec.europa.eu/internal_market/ payments/docs/pc/summary-2012_03_21_en.pdf*;

[52] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf*;*

3.3.1 Assenza di una normativa giuridica ad hoc: il caso Italia

Ritornando a casa nostra ossia in Italia, il d.lgs. 16 aprile 2012, n. 45, nel dare attuazione, parzialmente, alla direttiva 2009/110/CE ha ammesso l'emissione di moneta elettronica solo ad opera di soggetti iscritti in un apposito albo, con specifici requisiti quali la professionalità, livelli di capitale minimo, forme vincolate di controllo societario, autorizzati dalla Banca d'Italia.

Si diceva poc'anzi che la direttiva è stata recepita solo in parte: ebbene sì, perché, differentemente dalla norma europea, il legislatore italiano non ha tenuto in minimo conto la *condictio sine qua non* della dazione di fondi antecedenti l'emissione dello strumento di pagamento elettronico da parte dell'ente emittente. Un'ulteriore lacuna ancora non colmata.

Se in Italia manca una disciplina *ad hoc* sui bitcoins figuriamoci la normativa fiscale…se il bitcoin fosse riconosciuto come mezzo di pagamento - ex art. 1, comma 4. TUF - e non strumento finanziario quale è, l'utilizzatore sarebbe soggetto alla tassazione sulle plusvalenze ai sensi dell'art. 67, comma 1, lett. c-ter, del TUIR ed il miner equiparato ad un operatore finanziario regolarmente iscritto, ma così non è.

Essendo che la transazione in BTC un'operazione di scambio e che il BTC è convertibile in valuta corrente, dovrebbe rientrare tra le operazioni finanziarie soggette tanto ad imposta sui redditi quanto ad imposta sul valore aggiunto.

Se ancora, come qualcuno ha ipotizzato, il bitcoin fosse un bene**,** il piccolo miner potrebbe essere considerato un lavoratore autonomo che con la sua

attività genera reddito ed essere sottoposto alla tassazione sui redditi delle persone fisiche *(*corrispettivo per attività di lavoro autonomo non esercitate abitualmente o dalla assunzione di obblighi di fare, non fare o permettere, che è imponibile nel quadro dei redditi diversi al netto delle spese sostenute, con la valorizzazione al valore normale *di cui alla lett. l) dell'art. 67 TUIR),* disciplinato dal d.p.r. 31 dicembre 1986, n. 917 (TUIR) all'art. 67[53] o delle persone giuridiche, quelli di maggiori dimensioni un'impresa commerciale iscritta al registro delle imprese e soggetta ai rispettivi oneri.

L'utilizzatore finale del bene bitcoin dovrebbe pagare un valore aumentato dell'imposta sul valore aggiunto - IVA -, violando la direttiva Europea e quanto affermato dalla Corte di Giustizia che come già sottolineato considerano le operazioni con BTC non soggette a tassazione.

Atteso che il BTC *"consiste in un diritto a possedere una determinata quantità di una unità di conto (…)"* e che "*detti diritti sono regolati da regole condivise da chi partecipa a tali mercati (consuetudini), e nel caso delle criptovalute, il*

---

[53] Costituiscono redditi diversi, tra gli altri, *"c-ter) le plusvalenze, diverse da quelle di cui alle lettere c) e c-bis), realizzate mediante cessione a titolo oneroso ovvero rimborso di titoli non rappresentativi di merci, di certificati di massa, di valute estere, oggetto di cessione a termine o rivenienti da depositi o conti correnti, di metalli preziosi, sempreché siano allo stato grezzo o monetato, e di quote di partecipazione ad organismi d'investimento collettivo. Agli effetti dell'applicazione della presente lettera si considera cessione a titolo oneroso anche il prelievo delle valute estere dal deposito o conto corrente; (…)"* e anche *"c-quinquies) le plusvalenze ed altri proventi, diversi da quelli precedentemente indicati, realizzati mediante cessione a titolo oneroso ovvero chiusura di rapporti produttivi di redditi di capitale e mediante cessione a titolo oneroso ovvero rimborso di crediti pecuniari o di strumenti finanziari, non ché quelli realizzati mediante rapporti attraverso cui possono essere conseguiti differenziali positivi e negativi in dipendenza di un evento incerto*".

diritto è costituito e incorporato in una stringa alfanumerica contenente una determinata quantità, trasferibile a terzi", tale parte della dottrina ritiene che le operazioni in esame ricadano nella fattispecie di cui alla lett. f), art. 135 della direttiva, che prevede l'esenzione per *"le operazioni, compresa la negoziazione ma eccettuate la custodia e la gestione, relative ad azioni, quote parti di società o associazioni, obbligazioni e altri titoli, ad esclusione dei titoli rappresentativi di merci e dei diritti o titoli di cui all'articolo 15, paragrafo 2 (della medesima direttiva)"* ed in particolare tra quegli *"altri titoli"* indicati dal legislatore europeo.

3.3.2 Assenza di una normativa giuridica ad hoc: monitoraggio fiscale, patrimoniale e normativa antiriciclaggio

Assodato quanto esaminato nei paragrafi precedenti si rende necessaria un'altra considerazione. Se l'individuo detiene BTC in un portafoglio on line fornito da una piattaforma ubicata all'estero, magari anche al di là dei confini dell'Unione Europa, sviluppa attività di scambio e quindi genera reddito, deve dichiararlo compilando il quadro RW della dichiarazione dei redditi o del modello unico specificandone la natura e l'ammontare dei valori detenuti all'estero sia ai fini di monitoraggio che impositivi osservando le regole di tassazione stabilite dall'IVAFE? (imposta sul valore di prodotti finanziari, conti correnti e libretti di risparmio detenuti all'estero da persone fisiche residenti in Italia). E come ci si regola con la normativa antiriciclaggio - D.lgs. n. 231/2007 - che all'art. 1, comma 2, lett. qq. descrive la criptovaluta come una "*rappresentazione digitale di valore, non emessa né garantita da una banca*

centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente" e che nel caso di specie vedrebbe l'applicazione del concetto di "titolare effettivo" ossia di persona fisica per conto della quale è realizzata un'operazione obbligata agli adempimenti di legge (dichiarazione dei proventi e soggetta all'obbligo dell'adeguata verifica della clientela) senza possibilità di schermatura da parti di terzi per occultare le proprie posizioni patrimoniali?

E con il reato presupposto di cyberlaundering o meglio cyber riciclaggio? Navigando in rete con l'ausilio di un device elettronico il cyber criminale acquista beni e/o servizi provenienti da reato (attività delittuosa non colposa) che paga con moneta virtuale; l'origine della provvista deriva da attività illecita (prostituzione, terrorismo, estorsione, ecc…), le condotte antigiuridiche sono la sostituzione o il trasferimento di quegli stessi beni frutto di attività illecita, l'occultamento e/o la dissimulazione della vera natura dei beni, l'acquisizione, il possesso o l'utilizzo dei predetti al fine di ripulire capitali provenienti da fatti illeciti: cyberlaundering.

E' una fattispecie delittuosa di recente formazione che coniuga il reato di riciclaggio "money laundering" ed il "cybercrime" reato cibernetico. "*Chiunque, fuori dei casi di concorso di reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da*

euro 5.000 a euro 25.000…" recita l'art. 648 – ter del c.p. rubricato "Impiego di denaro, beni o utilità di provenienza illecita".

Il reato presupposto della fattispecie criminosa ossia del reato di riciclaggio – ex. art. 648 bis del codice penale *"Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto [non colposo]; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000"* -, è l'aver precedentemente commesso un fatto delittuoso che non necessariamente debba essere accertato con sentenza definitiva ossia passata in giudicato – è sufficiente che emerga dagli atti processuali o che si sia perfezionato con la condotta del soggetto agente -, o altre operazioni che eludano il collegamento con il fatto criminoso e che ne impediscano la titolarità, la provenienza e la reale destinazione.

Le operazioni bancarie oltre confine rendono obbligatoria, nella dichiarazione dei redditi, la denuncia di ogni transazione verso le agenzie di excange, specie se la moneta elettronica, conservata in portafogli offerti da piattaforme straniere, alimenta le "riserve estere" di criptovalute. La medesima dichiarazione dovrebbe effettuarsi con le stesse finalità impositive e di monitoraggio nell'ipotesi in cui si volesse convertire la riserva estera in moneta elettronica presso una exchange platform e risalire così al wallet utilizzato ed all'utente certo.

E’ vero che il bitcoin è una moneta immateriale, altamente volatile ma è altrettanto vero che l’artefatto tecnologico si basa su una block chain che conserva, registrate al suo interno tutte le movimentazioni eseguite dalla nascita del protocollo Bitcoin e/o versioni ridotte di singole transazioni di cui è possibile verificarne la tracciabilità. Per questo sarebbe più opportuno parlare di pseudo anonimato piuttosto che di anonimato totale tenuto conto chequando si attenziona il tracciamento del bitcoin si guarda alla transazione verae propria ed alla sua rispettiva registrazione ma non, invece, al possibile collegamento esistente tra la moneta ed il soggetto utilizzatore e/o detentore. Questo è il grande limite del bitcoin.

CONCLUSIONI

Con questo contributo si è tentato di tratteggiare i contorni tecnico-giuridici del sommerso: dall'analisi alla formazione del fenomeno fino all'impiego delle Forze di Polizia nei servizi di controllo delle azioni dei criminali economici atta a "scovare" le attività illegali dei mercati virtuali: "black market" in cui il "quid pluris" è rappresentato per il venditore da una piattaforma di e-commerce capace di generare un apprezzabile volume d'affari e per il compratore dalla facilità nell'acquistare qualsiasi bene senza identificarsi ma semplicemente facendo uso di una "identità virtuale".

Accedere al "deep web" piuttosto che alla parte più oscura della rete, il "dark web" non presenterebbe profili di rilievo giuridico se la condotta del soggetto agente nei "black markets" non fosse indirizzata all'acquisto o allo scambio di beni e servizi di natura illecita.

L'anonimato tanto nella navigazione quanto nelle procedure di pagamento, l'invisibilità dei cybercriminali degli "spazi virtuali", l'opacità e la volatilità delle monete elettronico-digitali impiegate quali mezzi di pagamento virtuali, legislazioni lacunose rendono difficoltosa ogni forma di monitoraggio dell'economia monetaria. Tanto che in più occasioni le Forze di Polizia e nello specifico la Guardia di Finanza hanno denunciato il pericolo di creazione di paradisi fiscali virtuali favoriti da forme di evasione fiscale reale le cui movimentazioni di capitali potrebbero essere impiegati anche per il fiancheggiamento ed il sovvenzionamento di attività terroristiche.

Ma come difendere l'economia dal sommerso? Attraverso il monitoraggio delle transazioni non contabilizzate e quindi di difficile rintracciabilità avvenute nei canali non ufficiali che spesso sfociano in operazioni di riciclaggio di valuta di dubbia provenienza, dei money transfer, attività private di cui i migranti si servono per trasferire le rimesse all'estero, di zone off-shore e di paradisi fiscali che per gli attraenti regimi fiscali e legali che offrono incoraggiano riciclaggio di denaro e reati finanziari.

A supporto dell'attività di intelligence, sostanziali saranno piattaforme, sistemi di analisi visuale delle informazioni assunte, hardware di acquisizione forense, sistemi informatici automatizzati, motori di ricerca appositamente configurati per l'accesso al dark web ed alle fonti aperte. Aspetti tecnici che dovranno essere suffragati da un'adeguata preparazione professionale.

La navigazione in rete denota una crescita esponenziale dei cyber attacchi: reati informatici che colpiscono i privati, le organizzazioni pubbliche e private, le Pubbliche Amministrazioni, le Istituzioni.

Assumendo il fenomeno connotazione internazionale sarebbe auspicabile una costante cooperazione con i Paesi aderenti alle organizzazioni internazionali in un proficuo confronto con i centri di ricerca, con le strutture di "law enforcement", con gli addetti alle tecnologie ed alla sicurezza delle comunicazioni, con il mondo accademico.

BIBLIOGRAFIA

F. VITA, *Senza banche. Bitcoin la moneta di internet*, 2013, 83 ss.

J.B. TURPIN, *Bitcoin: the economic case for a global, virtual currency operating in an unexplored legal framework*, in *Indiana Journal of global legal studies*, 2014, 344 ss.

P.L. BURLONE-R. DE CARIA, Bitcoin *e le altre criptomonete. Inquadramento giuridico e fiscale*, Istituto Bruno Leoni, 2014, *http://www.brunoleonimedia.it.*

M. SPAGNUOLO-F. MAGGI-S. ZANERO, *Bitlodine: extracting intelligence from del Bitcoin network*, pubblicazione del Politecnico di Milano.

I.W. SCHIAROLI, *Dark web e bitcoin, la nuova era della rete*, Roma, 2012, 14 ss. e, più nel dettaglio, J.J. DOGUET, *The nature of the form: legal and regulatory issues sorrounding the Bitcoin digital currency system*, in *Louisiana law review*, 2013, 1126 ss.

A. BIRYUKOV-D. KHOVRATOVICH-I. PUSTOGAROV, *Deanonymisation of clients in Bitcoin P2P network*, 5 luglio 2014, 2 ss.

I. GRIGG, *Triple entry accounting*, 2005, 41 ss.

N.M. KAPLANOV, *Nerdy money: Bitcoin, the private digital currency and the case against its regulation*, in *Consumer law review*, 2012-2013, 116 ss. e, più nel dettaglio, N. PLASSARAS, *Regulating digital currencies*, in *ChicagoJournal of International Law*, 2013-2014, 384 ss.

G. ARANGÜENA-S. CAROLI-L. NICOLI-M. RIZZATI-F. CHIARI, *Bitcoin. L'altra faccia della moneta*, cit., 37 ss.

A. TETI, *Bitcoin la moneta del Cyberspazio*, in *Gnosis – rivista italiana di intelligence*, 2, 2012, 68.

M. SMITH, *More money, more problems: the bitcoin virtual currency and the legal problems that face it*, in *Journal of law technology and the internet*, 2012, 427 ss.

G. ARANGÜENA, *"*Bitcoin*: una sfida per* policymakers *e regolatori"*,in *http://www.dimt.it/2014/07/29.*

J.J. DOGUET, *The nature of the form*, cit., 1131 ss.;

D.A. DION, *I'll gladly trade you two bits on Tuesday for a byte today: bitcoin regulating fraud in the e-conomy of hacker-cash*, in *Journal of law, technology and policy*, 2013, 174 ss.

J. POLIS (2014), "*Jared Polis Became the First Congressman to Accept Bitcoin Donations After FEC's Approval"*, in *http://reason.com/ blog/2014/05/11/jared-polis-first-congressman-to-accept*, P. RON (2014), "*Bitcoin could 'destroy the dollar'"*, in *http://money.cnn.com/2013/12/04/technology/bitcoin-libertarian/*, J. MANCHIN (2014), *"Letter addressed to FED chairmen"*, in *http://www.manchin.senate.gov/public/index.cfm/2014/2/manchin-demands-federal-regulators-ban-bitcoin.*

A. SERRA, *Considerazioni in tema di pagamenti elettronici e moneta elettronica*, in *Contratto telematico e pagamenti elettronici*, a cura di Ricciuto, Padova, 2004, 66 ss. e B. INZITARI, *La natura giuridica della moneta*

elettronica, in *La natura giuridica della moneta elettronica: profili giuridici e problematiche applicative*, a cura di Sica, Zencovich, Milano, 2006, 24.

F. GUARRACINO, *Titolo di credito elettronico e documento informatico*, in *Banca, borsa, tit. cred.*, 1, 2001, 514 ss.

G. ARANGÜENA-S. CAROLI-L. NICOLI-M. RIZZATI-F. CHIARI, *Bitcoin. L'altra faccia della moneta*, cit., 112 ss.

G. ARANGÜENA-S. CAROLI-L. NICOLI-M. RIZZATI-F. CHIARI, *Bitcoin. L'altra faccia della moneta*, cit., 119 ss.

Y. PEREZ (2015), *"European Exchanges React to Bitcoin VAT Exemption"*, in *http://www.coindesk.com/european-exchanges-react-to-bitcoin-vat-exemption/.*

D. ESZTERI, *Bitcoin: anarchist money or the currency of the future?*, in *Studia Iuridica Auctoritate Universitatis*, 23, 2013, 40 ss.

R. RAZZANTE, *Manuale di cybersicurezza,* Pacini ed., 2023

R. RAZZANTE, *Manuale di Legislazione e prassi antiriciclaggio*, Giappichelli, 2023

S. CAPACCIOLI, *Introduzione al trattamento tributario delle valute virtuali*, cit., 54.

S. CAPACCIOLI, *Introduzione al trattamento tributario delle valute virtuali*, cit., 65 ss.

G. TREVERTON, *Reshaping National Intelligence for an Age of Information*. In: RAND Studies in Policy Analysis, 2001, 93-104.

G. CSURGAI, *Geopolitical and Geo-Economic Analysis of the S.W.F.*, LAP, Saarbruchen 2011.

L. MISES, *Human Action*, Yale University Press, New Haven 1949.

F.A. HAYEK, *The Use of Knowledge in Society*, in «American Economic Review», XXXV, 4, 1945, pp. 519-30.

Fonti Normative

Legge 3 agosto 2007, n. 124. “Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto”, pubblicata nella *Gazzetta Ufficiale* n. 187 del 13 agosto 2007. Articolo 3, commi 1 e 2.

Decreto Legislativo 30 giugno 2003, n. 196 recante il “Codice in materia di protezione dei dati personali”.

Decreto Legislativo 19 marzo 2001, n. 68 “Adeguamento dei compiti del Corpo della Guardia di finanza, a norma dell'articolo 4 della legge 31 marzo 2000, n. 78”.

Decreto Legislativo 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 attivita' criminose e di finanziamento del terrorismo nonche' della direttiva 2006/70/CE che ne reca misure di esecuzione”* novellato dal Decreto Legislativo 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 attivita' 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. (17G00104)".

Direttiva 2000/46/CE del Parlamento europeo e del Consiglio del 18 settembre 2000, relativa a l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica. (G.U.C.E. 27 ottobre 2000, n. L 275), recepita in Italia con legge 1° marzo 2002, n. 39.

Direttiva 2009/110/CE del Parlamento europeo e del Consiglio del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE, recepita in Italia con d.lgs. 16 aprile 2012, n. 45.

D.P.R. 31 dicembre 1986, n. 917, TUIR – Testo Unico delle Imposte sui Redditi

TUF – Testo Unico della Finanza

Fonti Giurisprudenziali

Cassazione penale, sez. Feriale, sentenza 16-12-2013 n. 50620 "È configurabile il delitto di associazione per delinquere finalizzata alla realizzazione di accessi abusivi a sistemi informatici da parte di un sodalizio criminoso operante esclusivamente in rete, anche quando non risulti individuabile l'esistenza di una struttura di vertice del gruppo".

Cassazione, sez. III, sentenza 15-05-2013 n. 20921 in tema di pornografia minorile.

Corte di Giustizia dell'Unione Europea, 22-10-2015 "*The exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT"*, in *http://curia.europa.eu/jcms/upload/ docs/application/pdf/2015-10/cp150128en.pdf".*

Tribunale di Brescia, sez. II penale, sentenza 17-11-2020 n. 2233 relativa all'operazione Berlusconi Market.

Altri Contributi

Relazione annuale 2019 della Direzione nazionale antimafia e antiterrorismo.

Rivista Trimestrale della Scuola di Perfezionamento per le Forze di Polizia.

Webgrafia

https://sociologicamente.it/intelligence-economica-influenzare-l-ambiente-economico-globale/.

https://formiche.net/2021/10/intelligence-economica-borghi/.

https://www.renovatioimperii.org/per-una-intelligence-economico-finanziaria/.

https://www.zerounoweb.it/techtarget/searchsecurity/dark-web-cose-e-come-evitarne-i-trabocchetti/.

https://en.wikipedia.org/ wiki/Tor_(network.

https://gnosis.aisi.gov.it/Gnosis/Rivista29.nsf/servnavig/80.

https://blog.cerbeyra.com/threat-intelligence/come-fare-intelligence-dark-web-per-difendere-azienda/.
https://europaatlantica.it/economy-and-finance/2021/11/criptovalute-possibili-rischi-e-sviluppi/.
https://www.ilsole24ore.com/art/chi-sono-e-cosa-fanno-detective-dark-web-caccia-dati-rubati-AC2QIfx?refresh_ce=1.
https://www.cybersecurity360.it/nuove-minacce/economia-sommersa-nel-dark-web-una-minaccia-crescente-come-gestire-il-rischio/.
https://focus.namirial.it/differenze-vantaggi-token-criptovalute/.
https://www.ictsecuritymagazine.com/articoli/economia-illegale-e-crime-as-a-service/.
https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/economia-e-intelligence.html.
https://rivistapaginauno.it/workshop-osint-open-source-intelligence-investigazioni-digitali-nel-surface-deep-e-dark-web/.
https://www.reportdifesa.it/guardia-di-finanza-il-nucleo-speciale-tutela-privacy-e-le-frodi-tecnologiche-regole-e-consigli-per-evitare-attacchi-cyber/.
https://www.dirittoeconomiaimpresa.it/bitcoin-e-criptomonete.