Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno XII, n. 1, 2022
data di pubblicazione: 3 agosto 2022

Saggi

Cybercrime: una nuova minaccia per la Pubblica Sicurezza

di Vittorio Guarriello, Emanuele Macrì
e Silvio Marco Guarriello*

Abstract: The present essay aims to describe the main aspects of Cybercrime and the tools currently available to the investigative bodies to combat it, also bringing out the reasons for which the issues of cyber-security and cybercrime closely concern every citizen. In particular – combining the different professional experiences of people who daily are confronted with the themes of cybersecurity and cybercrime – will be highlighted the dangers to Public Security arising from cybercrime and, in particular, from the Deep Web and the Dark Web. Moreover, it will be illustrated an operation of Judicial Police conducted by the Carabinieri relative to a drug trafficking in which cryptocurrencies were used as a payment method and it will be deepened the use of new technologies and cryptocurrencies by organised crime, also for the purposes of money laundering and gambling.

* Vittorio Guarriello è dottore in Giurisprudenza, abilitato all'esercizio della professione forense. Emanuele Macrì è Capitano dell'Arma dei Carabinieri (ora è Comandante della Compagnia Carabinieri di Cagliari), dottore in Giurisprudenza; all'epoca dell'attività di Polizia Giudiziaria analizzata nel contributo rivestiva l'incarico di Comandante della Compagnia Carabinieri di Santa Maria Capua Vetere (CE). Silvio Marco Guarriello è magistrato, attualmente Procuratore Aggiunto della Repubblica di Foggia; già Sostituto Procuratore della Repubblica presso la Direzione Distrettuale Antimafia ed Antiterrorismo di Salerno, nonché a lungo docente a contratto di Ordinamento giudiziario presso il Dipartimento di Giurisprudenza dell'Università degli Studi della Campania "Luigi Vanvitelli". Pur nella concezione comune del contributo, si devono attribuire a Vittorio Guarriello i paragrafi nn. 1, 2, 3, 4, e 5; va attribuito a Emanuele Macrì il paragrafo n. 6, mentre si deve a Silvio Marco Guarriello il paragrafo n. 7; le conclusioni, da ultimo, sono frutto di un'elaborazione comune.

Democrazia e Sicurezza – Democracy and Security Review
ISSN: 2239-804X

anno XII, n. 1, 2022
data di pubblicazione: 3 agosto 2022

Saggi

1. Introduzione

La sempre più veloce evoluzione tecnologica e l'esponenziale diffusione dei servizi internet hanno comportato, come è noto, la nascita di un vero e proprio "spazio digitale".

Invero, pur non avendo consistenza fisica, il *web* contiene oramai tantissime informazioni e dati sensibili riguardanti la vita, le abitudini e le preferenze di ciascuno di noi. Per di più, mediante i servizi di *home banking*, i correntisti degli istituti di credito hanno la possibilità di disporre in pochi secondi del proprio patrimonio mobiliare.

Tutto ciò, inoltre, ha implicato che ogni singolo individuo vede affiancata la propria identità personale, da un'identità "digitale", ossia tutto quell'insieme di informazioni di carattere personale, professionale e finanziario contenute nella rete internet.

Ovviamente, sia la singola identità digitale sia lo spazio digitale nel suo complesso necessitano di forme di tutela al pari dei beni giuridici del mondo "fisico". Parimenti, i beni giuridici che vengono tradizionalmente tutelati dai vari ordinamenti (l'onore, la reputazione, il patrimonio, l'ordine pubblico) debbono essere analogamente tutelati dalle forme di pericolo e/o lesione che possono derivare loro proprio dal sempre più diffuso utilizzo di strumenti tecnologici.

Purtroppo, come ogni fenomeno umano, anche l'implementazione della tecnologia informatica ha avuto i suoi risvolti negativi. Difatti, essa ha offerto la possibilità anche a malintenzionati e criminali di aumentare le possibilità di compiere attività illecite, potendosi rendere anonimi con maggiore facilità e riuscendo a comunicare con luoghi e persone distanti fisicamente.

Per tali ragioni, il crimine informatico rappresenta attualmente uno dei pericoli maggiori per la Pubblica Sicurezza degli Stati[1], ma anche per la tranquillità

[1] L. ROSINI, *Il computer crime e le strategie di contrasto*, in «Rivista di Criminologia, Vittimologia e Sicurezza», n. 1, 2007, pp. 4-5.

individuale del singolo cittadino. Nondimeno, sovente i temi afferenti i reati informatici e la *cybersecurity* vengono reputati argomenti settoriali e distanti dalla vita quotidiana delle persone comuni, appannaggio esclusivamente degli addetti ai lavori o degli appassionati della materia.

Nel presente elaborato – unendo le diverse esperienze professionali di persone che giornalmente, pur non essendo tecnici informatici, si confrontano con il tema del *cybercrime* – si tenterà, senza alcuna pretesa di esaustività, di illustrare i principali aspetti del crimine informatico e dei mezzi attualmente a disposizione degli organi inquirenti per contrastarlo, mettendo in luce, altresì, i motivi per i quali i temi della sicurezza informatica e dei *computer crimes* riguardano da vicino ciascuno di noi e, più in generale, la pubblica sicurezza e l'ordinato svolgersi della vita civile.

2. Il *cybercrime*

Con il termine *cybercrime* viene definito il fenomeno criminale caratterizzato dall'illecito utilizzo della tecnologia informatica, sia di tipo *hardware* sia di tipo *software*, finalizzato alla commissione di uno o più reati[2]. Le tipologie di *computer crimes* sono di vario genere e possono ledere un'ampia gamma di beni giuridici: senza presunzione di completezza, si citano frode informatica, *phishing* (illecita sottrazione di dati personali mediante artifizi e raggiri), *cyberstalking*, pedopornografia *online*, intercettazioni non autorizzate, divulgazione di materiale protetto dal diritto d'autore, compravendita sul *web* di beni e/o sostanze illegali, violazioni di sistemi di sicurezza, furti di dati, divulgazione di informazioni coperte da segreto militare o commerciale, gioco d'azzardo *online*.

Dal punto di vista concettuale, la dottrina e la giurisprudenza assolutamente prevalenti effettuano una distinzione tra reati informatici "in senso stretto" (o

[2] V. SORCE, *Informatica e reato*, in G. TADDEI ELMI (a cura di), *Corso di informatica giuridica*, Simone, Napoli 2016, p. 145.

propri) e reati informatici "in senso lato" (altrimenti definiti reati eventualmente informatici).

Segnatamente, i reati informatici in senso stretto sono quelle figure di illecito penale nelle quali il *profilo informatico* (l'elaboratore, il *software*, la connessione etc.) rappresenta un elemento imprescindibile della condotta e/o dell'evento: non potrà dunque esistere una fattispecie di reato "comune"[3] omologa, in quanto in assenza dello strumento tecnologico non è neanche possibile immaginare una figura di reato analoga[4]. Di converso, i reati informatici in senso lato sono quelle fattispecie delittuose nelle quali l'elemento informatico delinea particolari ed eventuali modalità di esecuzione del reato ma non ne caratterizza la tipizzazione, sostanziandosi in un mero ampliamento delle modalità di commissione di illeciti già precedentemente tipizzati che, pena la violazione del divieto di analogia e del principio di tassatività, non avrebbero potuto essere ricondotte alla disciplina prevista per le fattispecie tradizionali[5].

Con maggiore impegno esplicativo, assumendo come esempio paradigmatico di reato informatico proprio l'accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 *ter* c.p., è di solare evidenza come l'elemento tecnologico assuma un rilievo caratterizzante nella tipizzazione della fattispecie, sicché esso viene definito un reato informatico in senso "stretto" in quanto la portata applicativa della norma è limitata esclusivamente al solo ambito tecnologico.

[3] Giova precisare che, in questo caso, con l'espressione «reato comune» non ci si intende riferire alla tradizionale categoria penalistica delle fattispecie che possono essere poste in essere da chiunque, a prescindere dalla qualifica soggettiva rivestita, ma agli illeciti penali perpetrabili anche senza l'utilizzo di strumenti informatici o telematici.

[4] Cfr. R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), *Cybercrime*, *Diritto e procedura penale dell'informatica*, Utet Giuridica, Milano 2019, pp. 141-192.

[5] V. MILITELLO, *Informatica e criminalità organizzata* in «Rivista trimestrale di Diritto penale dell'economia», 1990. p. 85 ss.

In altri termini, è impossibile immaginare un accesso abusivo ad un sistema informatico o telematico in assenza dell'elemento tecnologico[6].

Viceversa, può assurgere ad esempio idealtipico di reato eventualmente informatico la commissione dell'illecito penale di atti persecutori mediante strumenti informatici o telematici di cui all'art. 612-*bis*, comma 2 c.p.

Invero, nel reato di cui all'art. 612-*bis* c.p., rubricato «Atti persecutori», con il quale vengono sanzionate le condotte di molestia e/o minaccia reiterate in maniera tale da ingenerare nella vittima il fondato timore per l'incolumità propria, di un prossimo congiunto o di una persona alla quale essa è legata da relazione affettiva; un perdurante stato d'ansia e/o un mutamento delle sue abitudini di vita, è previsto al secondo comma un aumento di pena se il fatto è stato commesso attraverso strumenti informatici o telematici, stante la pervasività dei contenuti diffusi mediante gli stessi. Tuttavia, in quest'ultimo caso, l'elemento informatico viene considerato solamente uno degli strumenti attraverso i quali è realizzabile il reato, atteso che le condotte tipizzare dalla fattispecie sono pacificamente realizzabili anche in assenza di qualsivoglia strumento informatico o telematico.

Per tale ragione, è possibile definire la condotta di s*talking* realizzata mediante strumenti tecnologici un reato "eventualmente informatico".

Ovviamente, in ragione le potenzialità offerte dalle tecnologie informatiche hanno enormemente aumentato la facilità di realizzazione e la pervasività di taluni reati "tradizionali".

Difatti, parte della dottrina ha definito taluni reati eventualmente informatici come reati *reziari*[7], in ragione della circostanza che è l'infrastruttura del *web* a rappresentare il mezzo determinante alla loro rapida ed esponenziale diffusione, sicché gli autori di tali illeciti penali sono paragonati a *moderni reziari informa-*

[6] E. Tucci, *I reati informatici e la* digital forensics, in AA.VV., *L'informatica per il giurista*, Maggioli, Santarcangelo di Romagna 2019, p. 293 ss.

[7] C. Sarzana di Sant'Ippolito, *Informatica, internet e diritto penale*, Giuffré Francis Lefebvre, Milano 2010, p. 758.

tici, la cui arma che consente loro di perpetrare illeciti in ogni parte del globo è costituita proprio dalla aspazialità della rete internet.

Ebbene, l'ampia tipologia di reati realizzabili mediante le tecnologie informatiche ci consente di comprendere per quali motivazioni il *cybercrime* rappresenta attualmente uno dei maggiori fattori di criticità per l'ordine pubblico degli Stati.

Invero, gli strumenti informatici hanno offerto nuove efficaci modalità di commissione dei reati tradizionali, consentendo di compiere azioni criminose in maniera maggiormente rapida e con un minore rischio di identificazione, permettendo di aggredire in un brevissimo lasso temporale una pluralità di soggetti e/o beni giuridici siti anche in luoghi distanti tra loro.

Inoltre, una delle problematiche principali connesse ai *computer crimes* è la circostanza che la rete internet, essendo caratterizzata da aspazialità, rende difficoltoso identificare e collocare geograficamente i soggetti che vi operano.

Infine, le moderne tecnologie, oltre a rappresentare un formidabile strumento per i soggetti abitualmente dediti alla commissione di illeciti e le organizzazioni criminali, facilitano, stante la possibilità offerta dal *web* interloquire con chiunque ed il minor coinvolgimento emotivo che un soggetto avverte nella commissione di un illecito *online*, l'avvicinamento o la cooptazione in ambienti criminali di soggetti che nel mondo "fisico" sarebbero estranei a tali contesti. Infatti, un *hacker* che sottrae illecitamente dati a un'Istituzione governativa con tutta probabilità avvertirà come meno "criminale" la propria condotta rispetto a quella di colui che si introduce fisicamente in un ufficio pubblico al fine di trafugare documenti riservati.

Allo stesso modo, come si vedrà nel prosieguo della trattazione, è maggiormente agevole che soggetti, magari di giovanissima età, che nel loro contesto di vita sono estranei ad ambienti criminali possano organizzarsi al fine di compiere attività illecite (es. traffico di sostanze stupefacenti).

Le considerazioni precedentemente svolte, ci consentono, quindi, di comprendere le ragioni per le quali il crimine informatico risulta essere al giorno d'oggi, uno dei maggiori pericoli per la sicurezza delle Nazioni e l'importanza che hanno assunto, al fine di approntare efficaci strategie di contrasto allo stes-

so, il coordinamento internazionale tra le varie Autorità preposte e lo studio approfondito delle tematiche tecniche e giuridiche ad esso connesse.

Infatti, la Pubblica Sicurezza, come sancito anche dalla Corte Costituzionale[8], attiene «alla funzione inerente la prevenzione dei reati o al mantenimento dell'ordine pubblico»[9] e, ai sensi dell'art.159, comma 2 del d.lgs. 112/1998, concerne «le misure preventive e repressive dirette al mantenimento dell'ordine pubblico, inteso come il complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale, nonché alla sicurezza delle Istituzioni, dei cittadini e dei loro beni».

Conseguentemente, appare evidente che qualora il diffuso utilizzo di nuovi strumenti tecnologici, e i conseguenti fenomeni sociali, offrano nuove e più agevoli modalità di commissioni di illeciti o costituiscano la scaturigine di pericoli per le Istituzioni e la cittadinanza, essi diventano automaticamente una tematica assolutamente rilevante per le autorità Statali, sotto il profilo della tutela della Pubblica Sicurezza, alla stregua di altre diffuse e pericolose forme di criminalità.

Nondimeno, la già citata aspazialità della rete e la facilità di comunicazione che offre anche a soggetti fisicamente distanti fra loro, rende necessario un coordinamento sovrannazionale, atteso che misure di carattere nazionale risulterebbero facilmente eludibili da parte di coloro che commettono crimini *online* e, quindi, fallimentari.

3. *Cybercrime* ed evoluzione della criminalità

Le moderne tecnologie, come è risaputo, hanno assunto una notevole importanza nella vita quotidiana della maggior parte degli individui, caratteriz-

[8] Cfr. V. LOPILATO, *Manuale di diritto amministrativo. Parte speciale e giustizia amministrativa*, Giappichelli, Torino 2021, pp. 1278-1279.

[9] Corte cost., 24-27 marzo 1987, n. 77 e 23 giugno - 22 luglio 2010, n. 278.

zando l'attuale società in tutti suoi aspetti. Basta considerare, a tal proposito, quante delle attività parte della *routine* quotidiana di ciascuna persona vengono poste in essere mediante l'ausilio di dispositivi informatici. Ciò ha, di conseguenza, comportato un esponenziale aumento dei reati connessi al loro uso.

Ovviamente, anche le organizzazioni criminali, in verità sempre pronte a sfruttare le occasioni di guadagno e/o gli strumenti utili all'agevolazione dei loro traffici illeciti, hanno adoperato le nuove tecnologie per perpetrare nuove tipologie di crimini o ammodernare le modalità di esecuzione delle loro attività delittuose ed è stata accertata anche l'esistenza di gruppi criminali organizzati precipuamente dediti alla commissione di reati in rete. In particolare, lo sviluppo del *web* ha consentito alle consorterie criminali maggiormente capaci di intercettare i cambiamenti in atto di incrementare notevolmente i margini di profitto, aumentandone la pericolosità. Difatti, come ricordato anche dalla Direzione Nazionale Antimafia in un *report* pubblicato nel luglio 2019[10], sovente la criminalità organizzata tradizionale sfrutta i servizi *online* per riciclare ingenti somme di denaro provento di attività illecite, stante l'estrema facilità con cui è possibile movimentare capitali, anche in maniera totalmente anonima, nei paradisi fiscali tramite le moderne tecnologie. Per di più, non di rado si è registrato un utilizzo da parte di criminali di criptovalute, come i *bitcoin,* per ricevere o effettuare pagamenti connessi ad attività illegali, atteso che risulta estremamente difficoltoso identificare i soggetti della transazione e l'assenza di un ente intermediario centralizzato rende difficili i sequestri patrimoniali[11].

Ancora, le moderne tecnologie offrono la possibilità, grazie ad avanzate tecniche crittografiche, di adoperare strumenti di messaggistica istantanea, quali Telegram, Viber, Whatsapp e Surespost*,* non facilmente intercettabili dalle For-

[10] Cfr. M. LUDOVICO, *Criptovalute, allarme Antimafia: "Paradiso finanziario virtuale"*, in *Il Sole 24 Ore*, 11 agosto 2019, https://www.ilsole24ore.com/art/criptovalute-allarme-antimafia-paradiso-finanziario-virtuale-ACXWNXd (consultato il 30 gennaio 2022).

[11] F. BOSI, *Riciclaggio, Money Muling e The Onion Router: l'attività di Polizia al tempo delle criptovalute e del Dark Web*, in «Antiriciclaggio e Compliance. Rivista Italiana dell'Antiriciclaggio», n. 2, 2020, p. 315 ss.

ze di Polizia. Come di recente affermato anche dalla Direzione Investigativa Antimafia nella propria relazione afferente il secondo semestre del 2018, i tecnici informatici e gli *hacker* rappresentano oramai alcune delle figure professionali più ricercate dalle mafie[12].

Il fenomeno che desta maggiore preoccupazione è, però, la nascita di nuovi sodalizi criminali, estremamente pericolosi, esclusivamente dediti alla commissione di reati informatici, dei quali, sovente, non si hanno conoscenze sufficientemente approfondite. L'Interpol, in un proprio rapporto[13], ha stimato che il costo sociale dei *computer crimes* ha oramai superato anche quello legato al traffico di sostanze stupefacenti. Secondo varie forze di polizia, dietro la maggior parte degli attacchi informatici posti in essere su larga scala, come quello alla borsa di Tel Aviv o alla compagnia aerea di bandiera israeliana El Al, e dei furti di dati sensibili ai danni di multinazionali o agenzie governative si nasconderebbero veri e propri *clan* di criminali informatici operanti in una dimensione transnazionale. Inoltre, le plurime attività investigative espletate al riguardo a partire dagli attentati al World Trade Center dell'11 settembre 2001 hanno evidenziato che la rete internet viene, sempre più spesso, utilizzata da organizzazioni terroristiche sia al fine di compiere azioni di propaganda e/o scambiare informazioni e pianificare le loro azioni sia all'uopo di danneggiare o distruggere i sistemi informatici di Stati, aziende ed individui, mediante attacchi *hacker* (c.d. *cyber*-terrorismo)[14].

Oltre a ciò, una vicenda esemplificativa della pericolosità del *cybercrime* per la sicurezza delle Istituzioni è quella mediaticamente nota come "Caso Occhionero" e, avente ad oggetto un'attività di *cyber*-spionaggio posta in essere da due

[12] Cfr. E. BARBARO, *Relazione Dia. O' sistema della camorra napoletana*, in *Terre di Frontiera*, 27 luglio 2019, https://www.terredifrontiera.info/relazione-dianapoli/ (consultato il 30 gennaio 2022).

[13] Cfr. R. NATALE, *Cybercrime: la mafia s'è spostata sul web. Per l'Interpol costa all'Europa 750 miliardi l'anno,* in *Key4biz*, 9 maggio 2012, *https://www.key4biz.it/News-2012-05-09-eSecurity-attacchi-informatici-interpol-Khoo-Boon-Hui-pirateria-hacker-210273/25291/* (consultato il 30 gennaio 2022).

[14] G. URICCHIO, *Il Cyberterrorismo*, in M. IASELLI (a cura di), *Investigazioni digitali*, Giuffrè Francis Lefebvre, Milano 2020, p. 683 ss.

ingegneri informatici a danno di esponenti di vertice delle istituzioni, enti pubblici e aziende private anche operanti in settori particolarmente sensibili (es. Ente nazionale per l'aviazione civile, Ministero degli esteri, Ministero dell'economia e delle finanze).

La predetta attività criminale si sostanziava nel furto di dati e informazioni riservate attuato mediante l'inocluazione di un particolare *software* di tipo *trojan*, denominato *Eye Piramid*, nel dispositivo "bersaglio" che, in seguito venivano trasferiti su appositi *server cloud* allocati all'estero (nello specifico, in territorio statunitense), attuando, quindi una vera e propria attività di dossieraggio avente come vittime soggetti istituzionali di assoluto rilievo.

Difatti, veniva loro contestato di aver abusivamente acquisito «notizie che nell'interesse politico interno o della sicurezza pubblica devono rimanere riservate e di cui in ogni caso vietata la divulgazione ovvero dati personali e sensibili relativi ad intestatari ed utilizzatori dei sistemi informatici e telematici violati» e di aver provato ad accedere a un sistema informatico «contenente informazioni e dati relativi alla sicurezza pubblica nel settore dell'aviazione civile»[15].

Inoltre, il Giudice per le Indagini Preliminari che ha applicato nei confronti dei due indagati una misura cautelare personale, nel motivare l'adozione di tale provvedimento restrittivo della libertà personale, evidenziava come essi, in particolare uno di loro, fossero venuti a conoscenza del procedimento penale instaurato a loro carico ed avessero la volontà di carpirne i particolari ed influenzarne gli esiti.

Ancora, le immense opportunità di guadagno offerte dal gioco d'azzardo sul *web* o dalla commissione di illeciti come il *phishing* e le frodi informatiche su carte di credito o conti correnti bancari non vengono sfruttate solo dalla criminalità organizzata tradizionale, ma sono nati nuovi gruppi delinquenziali, spesso dotati di elevatissime competenze tecniche nel settore tecnologico. Si sta, quin-

[15] Trib. Roma, sez. Giudici per le Indagini Preliminari, ordinanza di applicazione della misura della custodia cautelare in carcere, proc. n. 21245/16 RGNR, p. 2 ss., reperibile all'indirizzo https://doczz.it/doc/499729/ordinanza-di-custodia-cautelare-occhionero (consultato il 30 gennaio 2022).

di, verificando un radicale cambiamento dei settori d'interesse e delle modalità d'azione delle mafie, unitamente alla nascita di nuove, e semisconosciute, consorterie criminali, circostanza che rende sempre più necessari e rilevanti, come già più volte ripetuto, una sinergia a livello internazionale tra le varie forze di Polizia nel contrasto al *cybercrime* e l'approfondito studio del fenomeno da parte delle Autorità Statali.

Ulteriore fattore di criticità che dimostra, ancora una volta, la necessità di una costante e crescente attenzione al fenomeno, è la circostanza che a cagione dell'emergenza epidemiologica da Covid-19, molte attività sono state svolte *on-line* e moltissimi soggetti, tra cui purtroppo anche malintenzionati, hanno acquisito una maggiore dimestichezza con l'utilizzo delle tecnologie informatiche e ciò ha avuto un'ovvia ripercussione anche nell'ambito dei reati informatici.

Al riguardo, la Direzione Centrale della Polizia Criminale ha evidenziato come nel corso dell'anno 2021, infatti, i reati informatici – in un *trend* generale di calo della commissione degli illeciti penali – siano stati tra le poche categorie di crimini a registrare un aumento.

Ciò è dimostrato anche dalle varie operazioni di Polizia Giudiziaria che hanno portato all'oscuramento di vari "canali" della nota applicazione di messaggistica istantanea denominata Telegram, all'interno dei quali venivano posti in commercio i più disparati contenuti illeciti e, tra quelli che hanno destato maggiore preoccupazione in questo periodo, *Green Pass* e *Super Green Pass* falsi.

Proprio l'utilizzo di Telegram a fini illegali ha destato la preoccupazione di taluni osservatori. Difatti tale applicazione, in ragione della crittografia *end to end*[16] adoperata, che è dotata di particolare sicurezza, anche al fine di sfuggire alle restrizioni imposte all'utilizzo di tale sistema in Russia tra il 2018 e il

[16] La crittografia *end to end* è un metodo di codifica dei messaggi, utilizzata da alcuni servizi di messagistica istantanea, basata su algoritmi di crittografia asimmetrica e sulla decentralizzazione delle chiavi crittografiche, tale da consentire solo ai soggetti che stanno comunicando la lettura "in chiaro" del testo dei messaggi.

2020[17], assicura una notevole *privacy* ai suoi utenti ma, al contempo, il suo utilizzo risulta particolarmente semplice e intuitivo, di talché , soprattutto per determinati tipi di reati (es. diffusione illecita di contenuti protetti dal diritto d'autore), il suo utilizzo viene preferito rispetto a quello di un sistema maggiormente complesso come il *dark web*.

Di conseguenza, alcuni esperti del settore hanno fatto notare che sembra quasi crescere nella società una "richiesta di *cybercrime*", vale a dire che moltissime persone, anche non in possesso di capacità tecniche, hanno compreso le potenzialità, anche illecite, che le tecnologie offrono, quindi anche "l'offerta" si è adeguata, predisponendo strumenti utili alla commissione di *computer crimes*, connotati da una maggiore semplicità di utilizzo.

Ebbene, l'evidenziato fenomeno consente di comprendere sempre di più come, oramai, la tematica dei reati informatici interessi tutti i settori sociali ed è necessaria una sempre più incisiva opera non solo di repressione nei confronti di tale fenomeno, ma anche di prevenzione e sensibilizzazione.

Più in particolare, è necessario far comprendere a tutti i cittadini quali sono i pericoli insiti all'utilizzo della moderna tecnologia informatica e, soprattutto, che, anche quando pensano di poter utilizzare il *web* a fini distorti e/o illeciti (es. *streaming* illegale) rischiano di divenire vittima di gravi reati, perpetrati da organizzazioni criminali connotate da particolare pericolosità.

4. *Deep web* e *dark web*

Nell'ambito delle tematiche afferenti al *cybercrime,* uno dei fenomeni emergenti che desta maggiore preoccupazione e del quale spesso si sente parlare sui *mass media* è il c.d. *deep web* ("*web* profondo"), ossia l'insieme delle risorse internet non indicizzate dai motori di ricerca tradizionali. Tuttavia, prima di af-

[17] L. CRAPANZANO, *I rischi oscuri del dark web*, in *Unione polizia locale italiana*, 19 aprile 2021, https://www.unionepolizialocaleitaliana.it/sito/wp-content/uploads/2021/04/202115-L.Crapanzano-Il-dark-web.pdf (consultato il 30 gennaio 2022).

frontare in maniera compiuta l'argomento è necessario effettuare una premessa: non tutto ciò che è tecnicamente definibile come *deep web* è riconducibile ad attività criminali o pericolose e che, spesso, viene operata un'impropria sovrapposizione tra le espressioni *deep web* e *dark web* ("*web* oscuro").

Invero, afferiscono al *web profondo* anche una serie di risorse *online* assolutamente lecite e di uso comune, tra cui anche le grandi reti governative e militari[18]. A tal proposito, basta considerare, ad esempio, le pagine ad accesso ristretto dei siti che richiedono una registrazione o impediscono che siano direttamente indicizzate dai motori di ricerca, quali i profili privati dei *social network* o gli *account* dei portali di *home banking*, che non sono direttamente indicizzate sui motori di ricerca ma costituiscono alcuni degli utilizzi legali più diffusi di internet. Differente è, invece, il discorso relativo al c.d. *dark web*, ossia quelle risorse virtuali alle quali è possibile accedere esclusivamente sfruttando appositi *software*,i più diffusi dei quali sono Tor, I2P e Freenet; esso costituisce un sottoinsieme del *deep web*. La "rete oscura" è, infatti, sovente sfruttata dalle organizzazioni criminali per i propri traffici illeciti, pur essendo essa adoperata anche per fini legittimi, come l'elusione della censura nei regimi dittatoriali. La modalità di accesso maggiormente diffusa per l'accesso al *dark web* è costituita dal *software* TOR (acronimo di *The Onion Router*), un protocollo di comunicazione basato su un sistema crittografico, definito *onion routing*, che consente di rendere anonimi sia il *client* che il *server*[19], facendo "rimbalzare" i pacchetti di dati

[18] E. FLORINDI, *Deep Web e bitcoin. Vizi privati e pubbliche virtù della navigazione in rete*, Imprimatur, Reggio Emilia 2016, p. 4.

[19] In ingegneria informatica viene definito *server* l'elaboratore che svolge, all'interno di una rete di calcolatori elettronici, funzioni di servizio per ogni terminale collegato (i *client*). Per estensione, assume lo stesso nome anche il programma, generalmente sempre attivo, che esegue determinate funzioni quando queste sono richieste da altri programmi. Il *client*, invece, è l'unità periferica di un sistema organizzato a rete, nella quale si svolgono una serie di operazioni di elaborazione: queste consentono una certa autonomia operativa all'unità stessa, che tuttavia, per il suo funzionamento complessivo ottimale, necessità di una serie di risorse messe a disposizione da un'unità centrale (il *server*). Cfr. *Server* (voce), in *Enciclopedia Treccani on line*, http://www.treccani.it/enciclopedia/server/ (consultato il 30 gennaio 2022).

trasmessi tra i vari nodi della rete, in guisa tale da impedire a un eventuale osservatore esterno di comprenderne origine e destinazione.

All'interno del *dark web* è possibile reperire qualsivoglia tipologia di contenuto illecito. I principali tipi di servizi criminali offerti nella rete occulta sono la condivisione di materiale pedopornografico e la compravendita di sostanze stupefacenti e di armi irregolari, ma sono state riscontrate addirittura piattaforme ove risultava possibile assoldare un *killer*.

Le predette tipologie di illecite compravendite avvengono, nella maggior parte dei casi, adoperando apposite piattaforme (c.d. *hidden markets)* a cui, sovente, è possibile accedere esclusivamente conoscendo l'indirizzo della risorsa sulla rete, atteso che, spesso, non sono indicizzate neanche nei motori di ricerca del *dark web* e che, comunque, i gestori di tali siti illeciti sono soliti chiuderli e riaprirli di frequente, mutandone la posizione sull'architettura di rete, anche allo scopo di eludere eventuali investigazioni a loro carico.

Altra peculiarità del *dark web* è, poi, quella di non consentire pagamenti in valuta normale, al fine di mantenere l'anonimato degli utenti. Al suo interno, difatti, possono essere effettuate esclusivamente transazioni in criptovalute.

Dal punto di vista giuridico, il mero utilizzo di una *darknet* non presenta profili di rilievo penale, non configurando alcun accesso abusivo ad un sistema informatico. Tuttavia, accedendo ad un orientamento esegetico della Corte di Cassazione, l'utente che si iscrivesse a una piattaforma del *dark web* ove vengono poste in essere attività illegali risponderebbe del reato di associazione per delinquere *ex* art. 416 c.p., in quanto nelle piattaforme della "rete oscura" l'utente viene sovente sottoposto a una "prova di iniziazione" al fine di creare un vincolo fiduciario con gli altri utenti, di talché «la deliberata sottoposizione a questo esame preliminare dimostra come l'utente sia indefettibilmente al corrente del fine illecito perseguito dal gruppo e, pertanto, deve considerarsi un associato del sodalizio criminoso a tutti gli effetti»[20]. Inoltre, è stato da taluni proposto di

[20] Cass., sez. III pen., 15 maggio 2013, n. 20921. Cfr. L. Dell'Aquila, *Il Deep Web e il Dark Web*, in *Cyberlaws*, 14 gennaio 2019, https://www.cyberlaws.it/2019/%EF%BB%BFdeep-dark-web-profili-legali/

pervenire ad una definizione legislativa delle piattaforme del *dark web* ove vengono venduti prodotti illeciti, in modo tale da rendere illegale tali condotte[21].

Di recente, le forze di Polizia, nell'ambito delle attività di contrasto ai crimini informatici, hanno realizzato una serie di operazioni che hanno disarticolato consorterie criminali operanti nel *dark web.* Tra le più importanti è possibile annoverare la chiusura da parte del Federal Bureau of Investigation (FBI) statunitense del sito di commercio elettronico, funzionante esclusivamente attraverso i servizi di anonimato del *software* T.O.R., denominato *Silk Road*[22]*,* nel quale venivano vendute svariate tipologie di merci illegali ed il sequestro del principale *marketplace* occulto italiano denominato *Babylon,* gestito da un soggetto originario di Scafati (SA), ad opera della Polizia di Stato coordinata dalla Direzione Distrettuale Antimafia di Roma, nel quale erano commerciati armi, droga, materiale pedopornografico, servizi di *Pay Tv* in violazione della normativa disciplinante il diritto d'autore, passaporti falsi e codici per la clonazione di carte di credito.

Le sopracitate operazioni di polizia giudiziaria consentono di mettere in evidenza il sempre crescente monitoraggio da parte delle Forze dell'Ordine delle attività illecite che avvengono nelle *darknet.* Tuttavia si rendono necessari maggiori strumenti normativi e investigativi, quali ad esempio modalità di identificazione e blocco delle transazioni illecite poste in essere mediante l'utilizzo di criptovalute maggiormente consolidate e rapide, al fine di avere a disposizione mezzi di contrasto alle attività criminali adeguati all'evoluzione tecnologica.

5. Gli strumenti di contrasto

Naturalmente, nel corso degli anni, il Governo italiano e le istituzioni sovranazionali non sono rimasti inermi di fronte alla crescente diffusione del *cy-*

[21] A. ANSELMI, *Onion Routing, cripto-valute e crimine organizzato*, Pacini Giuridica, Pisa 2019, p. 75 ss.

[22] V. LAGI, *Deep Web, Dark Web e indagini informatiche*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), *Cybercrime*, cit., p. 1942.

bercrime. Invero, sono state emanate misure di carattere legislativo tese al suo contrasto e istituiti organi investigativi specializzati nell'ambito dei reati informatici.

Il primo intervento legislativo di carattere sistemico in materia in Italia è costituito dalla legge n. 547/1993 che, oltre ad introdurre nell'ordinamento il reato di accesso abusivo a sistema informatico o telematico, ha sostanzialmente novellato alcune fattispecie previgenti, prevedendone, tra le modalità di commissione, quella mediante strumenti tecnologici.

Inoltre, è opportuno citare la Convenzione di Budapest sulla criminalità informatica del 2001, recepita nell'ordinamento giuridico italiano con la legge 18 marzo 2008, n. 48, e che, allo stato, è l'unica convenzione internazionale vincolante vigente in materia: con essa è stata operata una vera e propria opera di definizione normativa dei termini più diffusi nell'ambito del *cybercrime*, quale quella dei termini dato e sistema informatico e fornitore di servizi (*internet service provider)* e ha imposto l'obbligo per gli Stati membri di istituire meccanismi di responsabilità per le persone giuridiche in caso di comportamenti commissivi relativi ai reati informatici.

Tra le innovazioni maggiormente importanti che ha apportato nel nostro ordinamento il recepimento della convenzione di Budapest ad opera della predetta legge n. 48/2008 si cita la modifica dell'art. 51 c.p.p., mediante l'inserimento del comma 3-*quinquies*, a tenore del quale è attribuita al pubblico ministero presso il Tribunale capoluogo di Corte d'appello la competenza in materia di reati informatici in senso stretto. Mediante tale scelta legislativa, si è inteso centralizzare le indagini in materia di *computer crimes*, in ragione della consapevolezza che tali fenomeni criminali sovente non sono circoscrivibili entro ambiti territoriali limitati e all'uopo di consentire anche ai magistrati inquirenti di acquisire una maggiore specializzazione tecnica al riguardo.

Per quanto concerne gli organi deputati alla tutela della sicurezza cibernetica, in Italia si è assistito a una sempre maggiore specializzazione dei reparti delle Forze dell'ordine in materia ed è opportuno evidenziare come ogni Forza di Polizia e Forza Armata si sia dotata di reparti specializzati nel contrasto ai reati informatici e alla tutela della *cybersecurity*.

Infatti, la Polizia di Stato opera nel settore del contrasto al *cybercrime* con la specialità della Polizia Postale e delle Comunicazioni, in seno alla quale è incardinato il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAICIP), deputato alla prevenzione e della repressione dei crimini informatici, di qualsivoglia matrice, aventi ad obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale; inoltre, in seguito alla recente riorganizzazione degli Uffici e delle Direzioni centrali del Dipartimento della Pubblica Sicurezza (c.d. "atto ordinativo unico"), è stata istituita presso il predetto Dipartimento la Direzione centrale per la Polizia scientifica e la sicurezza cibernetica, deputata, tra l'altro, alla gestione del Cert (*Computer Emergency Response Team),* il centro di supporto dei sistemi di sicurezza informatica e cibernetica del Ministero dell'interno[23].

Il Corpo della Guardia di Finanza opera in materia mediante un reparto specializzato, ossia il Nucleo speciale tutela privacy e frodi tecnologiche. L'Arma dei Carabinieri ha, invece, istituito presso il Raggruppamento Carabinieri investigazioni Scientifiche il Reparto tecnologie informatiche. Anche l'Esercito italiano si è dotato di un apposito Reparto sicurezza cibernetica. Parimenti, sono istituiti presso gli stormi dell'Aeronautica Militare appositi *Computer Incident Response Team* ed esiste un Centro operativo cibernetico nell'ambito del Reparto Sistemi informativi automatizzati. La Marina militare ha istituito presso il proprio Stato maggiore un Ufficio sicurezza cibernetica, informatica e delle comunicazioni. Ancora, presso lo Stato maggiore della Difesa operano il Comando operazioni in rete e le Cellule operative cibernetiche.

Infine, con il decreto-legge n. 82/2021, convertito con modificazioni dalla legge n. 109/2021, è stata istituita l'Agenzia nazionale per la *cybersecurity*, avente il compito di coordinare le attività di tutti i soggetti pubblici coinvolti nella materia; di implementare la capacità di prevenzione nell'ambito della sicurezza

[23] Cfr. F. BECHIS, *Direzione cyber, cos'è e cosa farà la nuova struttura del Viminale*, in *Formiche.net*, 27 aprile 2021, https://formiche.net/2021/04/direzione-cyber-struttura-viminale/ (consultato il 30 gennaio 2022).

informatica e di tutelare gli interessi nazionali in tale settore. Essa è, inoltre, espressamente designata quale Autorità nazionale nell'ambito della *cyber*-sicurezza.

Per quanto concerne la magistratura inquirente, appare degna di nota la scelta della Procura della Repubblica presso il Tribunale ordinario di Milano di istituire un apposito *pool* di Sostituti Procuratori, oggi incardinato presso il IV dipartimento (frodi e tutela del consumatore)[24] e che si avvale della Squadra reati informatici, ossia un *team* di Polizia giudiziaria interforze (Carabinieri, Guardia di Finanza, Polizia di Stato e Polizia Locale), istituito presso la locale Sezione di Polizia Giudiziaria e posto alle dirette dipendenze funzionali del Procuratore Aggiunto coordinatore del *pool* reati informatici.

A livello sovranazionale, l'Europol[25] ha istituito l'European Cybercrime Center, ossia un'unità specializzata al contrasto alla criminalità informatica, e un Dark Web Team, finalizzato a collaborare con le varie Forze di Polizia nazionali a livello globale per contrastare le attività illecite poste in essere nel "*web* oscuro"[26].

L'Interpol[27], invece, ha costituito al proprio interno il Cyber Fusion Center che riunisce esperti informatici delle forze dell'ordine e dell'industria per raccogliere e analizzare tutte le informazioni disponibili sulle attività criminali nel *cyber*-spazio e fornire ai paesi membri informazioni coerenti e fruibili e aiuto per condurre indagini sui crimini informatici, garantendo alla polizia le informazioni aggiornate e pertinenti sulle minacce per guidare le loro azioni

[24] Originariamente, i reati informatici erano trattati dal Dipartimento avente competenza sui reati contro il patrimonio; dal 2012 al 2018 tali reati sono rientrati nelle competenze del Dipartimento Antiterrorismo.

[25] Europol è l'autorità di contrasto al crimine dell'Unione europea, ha sede a L'Aia (Paesi Bassi) e sostiene gli Stati membri dell'Ue nella loro lotta contro il terrorismo, il crimine informatico e altre forme gravi e organizzate di criminalità, collaborando anche con molti stati partner *extra* Ue e organizzazioni internazionali.

[26] F. BOSI, *Riciclaggio, Money Muling e The Onion Router*, cit., p. 315 e ss.

[27] Il nome completo è International Criminal Police Organization ed è un'organizzazione intergovernativa con 194 Paesi membri. Ha la funzione di aiutare tutte le forze di Polizia.

Inoltre, taluni reati informatici potranno rientrare nelle competenze della Procura Europea (*European Public Prosecutor's Office*), qualora rientrino nelle categorie di cui all'art. 22 del regolamento Ue 2017/1939.

Orbene, dalla suesposta disamina, si evince come, in ragione della costante evoluzione del *cybercrime*, anche le Istituzioni governative e sovranazionali siano state obbligate a un costante adeguamento della normativa in materie e di istituire organi sempre più efficaci e specializzati nel contrasto di tale fenomeno criminale.

6. L'abuso delle moderne tecnologie, piegate a finalità illecite. L'operazione di contrasto dei Carabinieri della Compagnia di Santa Maria Capua Vetere coordinati dalla Direzione Distrettuale Antimafia di Napoli, del febbraio 2019.

Un fenomeno in rapida ascesa è l'utilizzo di moderne tecnologie e strumenti informatici per eludere o intralciare le attività d'indagine delle Forze dell'Ordine, mediante: l'occultamento o la schermatura del proprio indirizzo IP, al fine di rendersi irrintracciabili[28]; l'utilizzo della moderna messaggistica istantanea, Whatsapp, Telegram, Surespot, ecc. a scopi illeciti[29]; l'uso distorto, da parte di soggetti sottoposti a indagine, dei sistemi *cloud*, Dropbox o Google Drive, per occultare dati e documenti mantenendone al contempo la disponibilità; ed ancora, l'utilizzo delle criptovalute, come per esempio il *Bitcoin,* per fi-

[28] Tra le modalità maggiormente adoperate per rendere anonimi gli indirizzi IP – che, di regola, identificano univocamente un dispositivo connesso alla rete internet – si annoverano l'uso dei *proxy*, le VPN (*Virtual Private Networks*), il sistema TOR (*The Onion Router*), che rendono difficoltoso risalire a quale sia il dispositivo da cui è partita la richiesta di accesso a una determinata risorsa disponibile in Rete.

[29] Tali applicativi adottano un sistema di crittografia mediante il quale il testo delle comunicazioni è nella disponibilità dei soli mittenti e destinatari delle stesse e non anche dei gestori del sistema;

nalità illecite e, segnatamente, al fine di ostacolare l'identificazione della provenienza del denaro[30].

Una recente attività investigativa ha fatto emergere un fenomeno criminale – che ha destato in maniera significativa l'attenzione degli organi di stampa nel corso dell'emergenza epidemiologica da Covid-19, ma purtroppo, già diffuso – esemplificativo di come soprattutto le nuove generazioni cresciute nell'era del digitale siano in grado di perpetrare "vecchi" reati impiegando di nuovi mezzi[31].

Invero, in data 20 febbraio 2019, nei comuni di Santa Maria Capua Vetere e San Prisco – in provincia di Caserta – i Carabinieri della Compagnia di Santa Maria Capua Vetere hanno dato esecuzione a un'ordinanza di custodia cautelare, emessa dal Giudice per le indagini preliminari presso il Tribunale ordinario di Napoli, su richiesta della locale Direzione distrettuale antimafia, nei confronti di cinque persone (tre delle quali sottoposte alla custodia cautelare in carcere e due ristrette agli arresti domiciliari), gravemente indiziate, a vario titolo, dei reati di associazione per delinquere finalizzata al traffico illecito di sostanze stupefacenti del tipo *marijuana* e *hashish* e detenzione ai fini di spaccio e spaccio di stupefacenti in concorso (artt. 74 e 73 d.P.R. n. 309/1990, artt. 81 cpv. e 110 c.p.)[32].

[30] La Direzione Nazionale Antimafia, in un suo *report* del luglio 2019, ha espresso alcune valutazioni in ordine alla permeabilità del sistema delle criptovalute a fenomeni di riciclaggio e autoriciclaggio, evidenziando che il *bitcoin* risulta la prima moneta per i pagamenti realizzati sul *darknet*, ovvero per i commerci illegali e che tra i principali fattori di criticità per gli organi inquirenti, si riscontrano «la complicata identificabilità degli indagati, la complessa acquisizione di prove circa le movimentazioni di valuta virtuale e la riconducibilità a soggetti specifici». Cfr. *Criptovalute, l'Antimafia: "Paradiso finanziario per riciclare e ripulire il denaro"*, in *Ilfattoquotidiano.it*, 7 agosto 2019, *https://www.ilfattoquotidiano.it/2019/08/07/criptovalute-lantimafia-paradiso-finanziario-per-riciclare-e-ripulire-il-denaro/5373822/* (consultato il 30 gennaio 2022).

[31] Cfr. S. PICHINI, *Consumo di droghe e COVID-19*, in *EpiCentro*, 18 maggio 2020, *https://www.epicentro.iss.it/coronavirus/sars-cov-2-dipendenze-droghe* (consultato il 30 gennaio 2022).

[32] La suesposta ordinanza di custodia cautelare ha costituito l'esito di un'articolata attività investigativa, inizialmente coordinata dalla Procura della Repubblica presso il Tribunale di Santa Maria Capua Vetere e, successivamente, attesa la sussistenza di un reato associativo ricompreso tra quelli enumerati all'art. 51, comma 3 *bis* c.p.p., dalla Direzione distrettuale antimafia di Napoli.

Le indagini espletate a monte del provvedimento giudiziario – tra la fine del 2015 e la fine del 2018 – hanno fornito agli inquirenti lo spaccato di una tragica realtà di giovani e giovanissimi *pusher*, diretti ed organizzati da un "capo", il quale interagiva con i propri sodali e con gli acquirenti di sostanza stupefacente anche mediante un sistema informatico di messaggistica criptato – denominato Surespot[33] – e provvedeva, in parte, all'approvvigionamento di stupefacenti (in particolare, di *marijuana*), attraverso il servizio postale, formalizzando via internet[34] gli accordi con i fornitori e pagando gli stessi in moneta virtuale di tipo *Bitcoin*, acquistata preventivamente con carte di credito.

Le suesposte modalità operative del sodalizio criminoso sono emerse da un'intensa attività di riscontro – espletata attraverso intercettazioni telefoniche e assunzione di dichiarazioni dei consumatori di sostanze stupefacenti del tipo *hashish* e *marijuana* – che ha consentito di appurare l'esistenza e l'operatività di un'associazione a delinquere composta da undici giovani, sei dei quali minorenni all'epoca dei fatti.

I membri del gruppo criminale dediti allo spaccio di sostanze stupefacenti operavano prevalentemente nei pressi di luoghi di aggregazione dei loro coetanei, in particolare nei pressi delle ville comunali e all'esterno degli istituti scolastici della zona, mentre il loro capo-promotore individuava per sé e per i propri sodali compiti ben precisi nell'approvvigionamento, confezionamento e spaccio delle suddette sostanze, prendendone nota in agende e quaderni. Tale documentazione dattiloscritta e manoscritta -recante i nominativi dei clienti, l'indicazione delle somme di denaro e dei metodi di pagamento *online* – rinvenuta nel corso di una perquisizione eseguita presso la sua abitazione – è risultata estremamente utile ai fini della ricostruzione del *modus operandi*

[33] Dall'analisi della documentazione rinvenuta, è emerso che il capo del sodalizio criminale, a mo' di promemoria, indicava ai propri correi di «installare Surespot», associando al nominativo di ognuno di essi una combinazione alfanumerica (es. M4, M5 ecc.), al fine di evitare la corretta identificazione dell'utilizzatore dell'applicativo.

[34] Nelle more dell'attività d'intercettazione telefonica, emergevano contatti intercorrenti tra il capo del sodalizio e un soggetto, presumibilmente residente in Torino.

dell'organizzazione criminale e a comprovare l'evidente radicamento sul territorio della stessa.

L'opera degli inquirenti ha così disvelato un articolato scenario criminale nell'ambito del quale i soggetti poi attinti dalle misure restrittive sfruttavano le *chat* crittografate e l'anonimato garantito dall'utilizzo delle criptovalute al fine di perpetrare gravissimi reati in danno della salute pubblica e, in particolare, quella delle nuove generazioni; ha però, al contempo, evidenziato che anche se coloro i quali si rendono responsabili della commissione di illeciti penali adottano strumenti sempre più tecnologici e sofisticati, le attività di contrasto nei loro confronti poste in essere da Forze dell'Ordine e Magistratura restano, comunque, incessanti ed efficaci.

7. *Cybercrime* e criminalità organizzata

Le organizzazioni criminali sono sempre pronte a cogliere nuove opportunità di guadagno illecito e uno dei tratti caratterizzanti delle mafie tradizionali italiane (cosa nostra, camorra, 'ndrangheta e sacra corona unita) è avere una rilevante capacità di adattamento ai mutamenti sociali ed economici: così come hanno seguito la trasformazione dalla società agricola a quella industriale, attualmente l'evoluzione verso la globalizzazione, insieme all'imponente innovazione tecnologica, è stata colta come occasione per inserirsi, mantenendo le proprie connotazioni criminali tipiche, in tale nuovo contesto che, mutando le dinamiche economiche relazionali e tecnologiche, consente il ricorso a nuove forme di delitto.

La novità della *evoluzione nella modernità* delle mafie è stata colta dall'Onu[35], dall'Interpol, da Europol e dalla Direzione nazionale antimafia e

[35] L'Onu ha istituito l'Ufficio e contro la droga e il crimine (UNODC) che si occupa dei temi mondiali relativi a droghe, criminalità organizzata, corruzione e terrorismo. L'UNODC offre assistenza pratica e incoraggia approcci transnazionali all'azione attraverso i programmi globali e una rete di uffici.

antiterrorismo che hanno individuato il *cybercrime* come un importante settore di espansione delle attività delle organizzazioni criminali. Tali reati, commessi avvalendosi di moderni strumenti tecnologici, consentono alle mafie di ottenere molteplici vantaggi: fra questi, quelli di acquisire rapidamente ingenti profitti illeciti, occultare le attività illecite e/o i relativi proventi, ridurre al minimo l'esposizione fisica dei propri affiliati che, anzi, spesso operano più agevolmente in forma anonima. In sostanza, il *cybercrime* amplia l'*ambiente* di consumazione dei reati, rende più difficile individuare sia i reati che gli autori e, in assenza di manifestazioni eclatanti e violente dell'azione criminale desta meno allarme sociale.

Quando si parla di *cybercrime* ci si riferisce sia ai *reati informatici "propri"*, detti anche *reati informatici in senso stretto*, ossia i fatti penalmente rilevanti la cui condotta criminosa si connota per avere ad oggetto direttamente i sistemi e le apparecchiature informatiche, sia ai *reati informatici "impropri"* o *reati eventualmente informatici*, definizione che si riferisce ai reati comuni quando vengono commessi mediante l'utilizzo degli strumenti telematici. Calando tali definizioni nella materia oggetto di trattazione in questa sede, se ne trae un primo elemento di riflessione: la potenzialità espansiva del crimine informatico, che è riferibile ad ogni tipo di delitto, amplia in maniera esponenziale la già rilevante forza delle organizzazioni criminali; le mafie infatti non hanno colto solo la possibilità di commettere i *reati informatici propri*, ma anche la potenzialità dell'informatica nell'agevolare la commissione di tutti gli altri reati.

Pertanto, si sono evidenziati vari elementi di pericolosità del connubio *cybercrime*-mafie. In primo luogo, si è notato come tale tipologia di delitti consente che l'operatività criminale si distacchi sempre più dal territorio di provenienza agevolandone le condotte anche in ambito transnazionale, senza che vengano meno le caratteristiche proprie delle organizzazioni mafiose. Inoltre, la diffusione di internet in una economia globalizzata ha offerto un contesto planetario che rende più difficile la repressione e nel quale gli affari illeciti possono essere condotti in assenza di adeguati controlli, oltre che per la già indicata ragione dell'anonimato garantito dal *web*, anche per la disarmonia delle varie norme nazionali (in particolare nelle materie di: conservazione dei dati informatici; trac-

ciabilità dei flussi finanziari; tipologia di condotte sanzionate; cooperazione giudiziaria fra Stati). Un aspetto di rilievo è rappresentato dal fatto che il *web* consente una più agevole attività di riciclaggio degli enormi proventi illeciti delle mafie che acquisiscono, o trasferiscono, risorse economiche via *web*: tutto ciò avviene con estrema velocità, sia avvalendosi dei normali canali finanziari sia con il ricorso alle "criptovalute" (che non rendono neanche più necessario l'utilizzo di complesse operazioni finanziarie per il tramite delle relative e tradizionali istituzioni ed agevolano l'anonimato delle transazioni).

Dunque il *cybercrime*, già di per sé uno dei pericoli più seri a livello mondiale stante l'elevata informatizzazione delle istituzioni, delle economie e della vita quotidiana di ognuno, in un sistema planetario che sostanzialmente utilizza un'unica infrastruttura di base, diventa ancor più pericoloso ove lo stesso diviene l'*ambiente* per l'operatività delle mafie che, già di loro, sono caratterizzate da un alto livello di capacità delittuosa.

Giova, quindi – ai fini della compiutezza della presente trattazione – passare in rassegna alcune delle principali attività illecite, o connesse al crimine, che le mafie commettono avvalendosi della rete. Le stesse sono state evidenziate dalla storia giudiziaria concreta anche se le relative indagini, per brevità e tenuto conto dell'oggetto del presente scritto, non saranno specificamente indicate.

Tuttavia, prima di trattare delle tipologie ricorrenti dei reati informatici è opportuno soffermarsi sulla specificità dell'*ambiente* informatico. Accanto al *web* ordinario, quello cui si accede con i normali motori di ricerca di uso comune, esiste il c.d. *deep web* o "*web* sommerso" che, pur utilizzando le medesime infrastrutture tecnologiche, non è visibile con i programmi informatici di uso comune. Infatti, sono pochi i motori di ricerca all'interno del *deep web*, e quindi è difficile rintracciare i siti utilizzati per finalità criminali; oltretutto molti di questi siti sono accessibili solo a seguito della presentazione da parte di chi ne è gestore o membro. Tale connotazione dell'indicato *ambiente* informatico agevola l'anonimato e consente transazioni delittuose in sicurezza: è possibile commerciare anonimamente droga, armi, materiale pedopornografico senza che i siti *web* e i contraenti che se ne avvalgono corrano il rischio di essere individuati.

Altro aspetto di rilievo è la diffusione delle *criptovalute* che consente il pagamento della merce in forma anonima e a distanza, senza che sia necessario che le persone si incontrino dal vivo, si sposti denaro contante o si ricorra ai normali canali finanziari. Ciò agevola la possibilità di rendere non tracciabili i flussi economici, la loro provenienza e destinazione.

È di tutta evidenza che già le descritte connotazioni rendono il *web* come un ambiente ideale per il crimine: esso, comunque, può essere utilizzato in vario modo per scopi delittuosi, sia per commettere varie tipologie di reati sia per agevolarne la commissione, sia per occultarne i proventi. Di tutto ciò si fornirà una breve descrizione; inoltre, in questa sede, si terrà presente che, in genere, tali condotte possono essere commesse anche individualmente ma, ove utilizzate dalle mafie, le stesse diventano ancora più pericolose stante la potenzialità criminale garantita dalle strutture organizzative, di uomini e mezzi – oltre che dalla forza di intimidazione – di cui sono dotate. Le principali direttrici lungo le quali si intersecano il *cybercrime* e le mafie sono: sicurezza delle comunicazioni finalizzate alla commissione dei crimini e all'operatività delle mafie; spionaggio; frodi informatiche; riciclaggio.

L'utilizzo di internet consente comunicazioni segrete e in tempo reale, anche a grandi distanze, eliminando i rischi e gli inconvenienti connessi agli spostamenti per incontri personali, all'utilizzo dei telefoni ed alle lentezze dovute al trasferimento di messaggi cartacei. Le indagini hanno dimostrato che ciò avviene in vari modi. Ad esempio è possibile creare caselle di posta elettronica di uso comune con le quali ci si limita a comporre messaggi che non vengono inviati ma salvati: gli associati, in possesso delle credenziali di accesso si limitano ad entrare nella casella, leggendone i messaggi senza che lo stesso sia mai stato inviato, eludendo così anche eventuali intercettazioni della posta elettronica. Molto utilizzati sono anche le comunicazioni via *chat,* in qualunque altra forma telematica e anche con programmi di criptazione, anche video, difficilmente intercettabili: si pensi che con gli ordinari strumenti di uso comune si può effettuare anche una riunione criminale in audio/video conferenza, magari fra criminali, anche latitanti, da varie parti del mondo. Inoltre, sempre ai fini della segretezza delle comunicazioni, si è rilevato come la tecnologia informatica sia adottata

anche per bonificare gli ambienti ove avvengono gli incontri (sia individuando microspie sia disturbando i segnali di trasmissione delle stesse). D'altra parte, le mafie hanno anche bisogno di acquisire informazioni e lo strumento informatico viene utilizzato per ottenere quelle di loro interesse, anche di tipo riservato, carpendo notizie utili sia per eludere le indagini sia per poter commettere reati. Anche se non di stretto rilievo per l'oggetto in trattazione, non si può non ricordare come nella rete siano presenti gruppi che inneggiano alla mafia o ne propagandano gli stili di vita e il potere intimidatorio.

Il ricorso al *web* può avvenire anche per il riciclaggio mediante attività apparentemente lecite. Si è già detto dell'utilizzo delle *criptovalute*, ma diffuso è anche il ricorso al commercio elettronico che consente di creare l'apparenza di transazioni lecite che, in realtà, hanno il solo scopo di fare entrare nel circuito legale denaro provento di illeciti: ad esempio, si possono simulare vendite mai avvenute da "negozi" *online* o effettuare dei pagamenti sproporzionati al valore del bene (si pensi alle aste *online*), il tutto solo per giustificare il transito e l'acquisizione di provviste di denaro in realtà di provenienza delittuosa. Rilevante è poi il ricorso alle ordinarie strutture economiche-finanziarie legali, con transazioni *online*, magari triangolate fra vari Paesi, in maniera da occultare la provenienza illecita delle somme e farne disperdere la tracciabilità. In tale contesto rilevante è l'utilizzo dei sistemi telematici per far approdare denaro "sporco" verso *paradisi fiscali*, per metterli al sicuro, o il transito dei proventi illeciti attraverso detti paradisi fiscali, al fine di occultare la provenienza del denaro prima di reimpiegarlo nell'economia legale dello Stato di origine dell'organizzazione mafiosa o in altro Stato.

In concreto, l'esperienza giudiziaria, italiana e internazionale, hanno evidenziato fra l'altro: *lease back* con triangolazioni fra società fittizie aventi sede legale in vari Stati; vendite di rilevanti complessi immobiliari mediante siti stranieri; clonazione del sistema informatico di una banca per effettuare operazioni con le quali somme illecite venivano artificiosamente confuse con fondi di provenienza pubblica destinati a società formalmente legali nella disponibilità delle mafie; diffusione di false informazioni al fine di alterare il prezzo di azioni quotate in borsa possedute da organizzazioni criminali.

Condotta tipica del *cybercrime* è la *frode informatica* che può avvenire in varie forme e con diverse tecniche. In primo luogo, può manifestarsi con l'accesso abusivo a sistemi informatici aziendali con lo scopo di ottenere gratuitamente i servizi erogati dalla società vittima. Inoltre, mediante vari modi è possibile ottenere i dati delle persone, delle carte di credito, dei conti correnti, così commettendo un illecito che spesso è solo un passaggio intermedio verso condotte criminali più ampie. In questi casi ci si trova al cospetto di *furto d'identità* altrui con lo scopo di appropriarsi delle risorse, delle informazioni o delle autorizzazioni della vittima. A tal fine si ricorre, fra l'altro, al c.d. *phishing*[36] e al *sim swap*[37].

In tal modo le mafie riescono a introitare un'enorme quantità di profitti illeciti, soprattutto se tali operazioni vengono poste in essere su larga scala o a danno di operatori economici di rilevanti dimensioni. Infatti, oltre ai furti seriali verso singoli individui, possono acquisire rilievo per le mafia le condotte di spionaggio e il furto di dati sensibili e di proprietà intellettuale in danno di imprese con lo scopo di ottenere informazioni riservate (si pensi alla proprietà intellettuale: *know-how,* logo, progetti di produzione, catalogo, segni distintivi di un'azienda) replicando poi i prodotti e commercializzandoli, via internet o in altre nazioni, senza che sia semplice individuare la contraffazione della merce e, soprattutto, gli autori. Ma può accadere che le aziende di mafia che operano sul mercato legale ricorrano al sabotaggio delle aziende concorrenti con finalità di

[36] R. ZULFIKAR, *Phishing Attacks and Countermeasures,* in P. STAVROULAKIS, M. STAMP, (eds.), *Handbook of Information and Communication Security*, Springer, Berlin-Heidelberg, 2010, p. 433.

[37] Con tale espressione si intende la clonazione della scheda telefonica ed il conseguente furto di tutti i dati. Il *sim swap* è, quindi, un'avanzata tipologia di frode informatica articolata in vari passaggi: individuata la vittima si procede alla acquisizione dei suo dati e delle credenziali di *home banking* tramite tecniche di *hacking* o mediante azioni di *phishing;* successivamente, si utilizzano documenti appositamente falsificati utilizzando i dati della vittima, si denuncia – in maniera fittizia – lo smarrimento del cellulare e, quindi, si ottiene da un gestore telefonico l'attivazione di una nuova *sim;* in tal modo si sostituisce *la sim card* della vittima, assumendone il controllo, e, attraverso lo stesso numero telefonico, si ottengono dalla banca le credenziali per operare sul conto corrente *online*, potendo, poi, agevolmente disporre bonifici e ricariche in proprio favore o a favore di prestanome compiacenti.

concorrenza sleale e illecita. Tali condotte mediante il *web* hanno sostituito, o si sono affiancate, alle tradizionali condotte delle mafie di vendita diretta di prodotti contraffatti (si pensi ai falsi in materia di abbigliamento o di prodotti musicali e cinematografici audiovisivi) o alle intimidazioni per estromettere concorrenti dal mercato.

Lo strumento informatico viene utilizzato anche per nuove forme di delitti mafiosi tradizionali. Un caso è quello dell'*estorsione informatica*, atto criminoso perpetrato attraverso l'installazione illegale di virus sul computer della vittima al fine di bloccarlo o di criptarne i dati, rendendone impossibile l'utilizzo, il tutto finalizzato a una richiesta illecita di pagamento per sbloccare il computer o il sistema vittima dell'aggressione.

Dunque, lo sviluppo della tecnologia informatica ha fornito alle mafie uno strumento e un *ambiente* nel quale porre in atto un suo crimine tipico che, in tal modo, può essere indirizzato anche in danno di soggetti che sono fisicamente lontani dai luoghi di operatività di "base" del sodalizio criminale. Inoltre, una richiesta estorsiva formulata in tal modo è certamente meno rischiosa di quella tradizionale (avvicinamento della vittima, attentati, ecc.) in quanto non si manifesta con le tradizionali modalità violente e avviene, oltretutto, in forma anonima, senza contatto fisico con la vittima e in forma a-territoriale.

Un altro settore di mutazione di forme di delitto tipiche delle mafie è quello del gioco d'azzardo che, come è noto, sovente ha rappresentato uno degli strumenti di arricchimento o riciclaggio. Infatti, lo stesso consente di giustificare la provenienza di cospicui capitali illeciti, o per effettuare frodi fiscali, con fittizie vincite a scommesse o a lotterie, attività spesso compiuta mediante l'acquisizione diretta o indiretta di attività economiche, quali casinò o sale scommesse. Con la diffusione di internet, negli ultimi anni sono proliferati moltissimi siti di gioco *online,* un settore che sin da subito ha suscitato l'interesse delle mafie non solo per le tradizionali ragioni di riciclaggio o per l'acquisizione del monopolio nel settore.

Invero, oltre a permettere di realizzare un maggior volume di giocate grazie alla velocità della connessione internet, i siti di scommesse *online* permettono alle mafie di frodare l'erario mediante svariati stratagemmi: il più diffuso è quel-

lo di costituire società di diritto straniero, allocando, altresì, all'estero i *server* dei siti di scommesse, costituendo, però, al contempo una rete fisica di agenzie di scommesse in Italia, fittiziamente qualificati come meri centri di trasmissione dati di tali società esteri, ma ottenendo direttamente il pagamento delle giocate consegnati direttamente al gestore dell' esercizio commerciale e, in seguito, trasferendo i profitti alla direzione amministrativa della società, allocata all'estero. In tal modo, pur essendosi il contratto di gioco o scommessa perfezionato in Italia, non vengono pagate le imposte dovute. Per di più, mediante la creazione di "conti gioco" intestati al titolare dell'agenzia o a soggetti compiacenti, si consente anche l'accesso al gioco *online* a soggetti non registrati, che restano anonimi, in violazione della normativa di settore che prevede la registrazione personale dei giocatori. In concreto, è stata accertata da un'indagine una circostanza inquietante, cioè che in tale settore si era realizzata una associazione fra soggetti appartenenti a varie organizzazioni mafiose, tanto da ritenere che si sia manifestata una pericolosa forma di *criminalità organizzata fluida* consistente o in una «organizzazione di scopo fra organizzazioni» o a una «associazione temporanea fra membri di varie mafie» in relazione a specifici affari.

Sono state più volte citate le *criptovalute* ed è stata evidenziata la loro diffusione. Circa la loro definizione le stesse sono «[…] rappresentazioni digitali di valore non emesse da una banca centrale o da un'autorità pubblica. Esse non sono necessariamente collegate a una valuta avente corso legale, ma sono utilizzate come mezzo di scambio o detenute a scopo di investimento e possono essere trasferite, archiviate e negoziate elettronicamente [...] non sono moneta legale e non devono essere confuse con la moneta elettronica»[38]. Il loro effetto è stato dirompente sul tradizionale sistema monetario in quanto il ricorso alle stesse consente una modalità di pagamento del tutto nuova sia rispetto a quelle tipiche, legali e tradizionali, sia a quelle con moneta elettronica[39]. Infatti, si tratta di

[38] *Cfr.* Banca d'Italia, Comunicazione del 30 gennaio 2015 – *Valute virtuali. Per un approfondimento sugli aspetti tecnico-informatici delle criptovalute.*

[39] La moneta elettronica è definita dall'art 1, comma 2 lettera *h-ter* della legge n. 385/1993 e ss.mm.ii.

un sistema di pagamento virtuale, non legato alle valute aventi corso legale, scambiate e utilizzate mediante un sistema autonomo e decentralizzato, non riconducibile a soggetti di intermediazione legale e, di fatto, sottratto al controllo delle istituzioni di settore. La peculiarità di tale mezzo di pagamento virtuale è quella di funzionare esclusivamente grazie ad una tecnologia *peer to peer*[40] tra i vari computer che adoperano il servizio, i quali, tutti, fungono da nodi della rete, validano le transazioni e "battono" la *criptomoneta*, così che non si ha la necessità di un'autorità centralizzata di emissione delle *criptovalute* e del relativo controllo. Prescindendo in questa sede dalle problematiche generali circa la liceità del sistema delle *criptovalute* e della responsabilità dei relativi operatori[41],

[40] Definizione che letteralmente significa "da punto a punto" e che nel linguaggio digitale significa anche "rete paritaria/paritetica"; con questa definizione si intende quindi un *sistema informatico decentralizzato* con un modello di architettura della rete in cui non vi sono gerarchie fra i nodi, senza *client* o *server* fissi e, dunque, con nodi *equivalenti* o *paritari* che operano contemporaneamente verso gli altri nodi terminali della rete. Con riferimento alle monete virtuali esistono, poi, specifici *software* che fungono da "portamonete elettronici" (*wallet)* e il controllo di ciascuna criptovaluta è decentralizzato e viene espletato mediante una tecnologia (generalmente una *blockchain)* che funge da registro delle transazioni finanziarie eseguite. In concreto, poi, ciascun utente è individuato in base uno pseudonimo e ogni individuo può essere titolare di un numero indeterminato di *account* riferibili alla propria persona. In tale ambito operano i c.d. *exchangers*, che convertono le *criptovalute* in monete tradizionali e viceversa.

[41] La questione maggiormente problematica è quella relativa all'inquadramento giuridico dell'attività degli *exchangers* e al loro possibile concorso nel reato di riciclaggio nel caso in cui attraverso di essi transitino capitali provento di attività delittuose. Sul punto, nel 2015 con l'*Avvertenza sull'utilizzo delle cosiddette valute virtuali,* la Banca d'Italia sollevava un dubbio circa l'attività degli *exchangers*: in particolare poneva la questione se quest'ultima potesse rientrasse nell'alveo delle attività tipizzate dal legislatore e riservate a determinate categorie di soggetti legittimati. Nello specifico, la Banca d'Italia sottolineava come «le attività di emissione di valuta virtuale, conversione di moneta legale in valute virtuali e viceversa e gestione dei relativi schemi operativi potrebbero invece concretizzare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati (artt. 130, 131 TUB per l'attività bancaria e l'attività di raccolta del risparmio; art. 131-*ter* TUB per la prestazione di servizi di pagamento; art. 166 TUF, per la prestazione di servizi di investimento)». In sostanza, il punto critico è dato dalla circostanza che le criptomonete sono mezzi di pagamento che, tuttavia, sono slegate dalle valute avente corso legale. In materia va però rilevato che il d.lgs. n. 90/2017 che ha ampiamento

tali caratteristiche rendono i vari sistemi estremamente funzionali sia al pagamento di transazioni illecite (si pensi al pagamento a distanza di forniture di droga) sia al riciclaggio[42], in quanto è complesso, se non impossibile, identificare la provenienza e la destinazione delle somme utilizzate.

modificato il d.lgs 231/2007, ha introdotto gli obblighi per gli *exchangers* (prestatori di servizi relativi all'uso di valuta virtuale) di iscriversi a pubblici registri, di effettuare operazioni di verifica sulla propria clientela e di vigilare sull'osservanza della normativa antiriciclaggio, attribuendo al Ministero dell'economia e delle finanze la titolarità dei controlli in materia. Sembrerebbe che, in base a tale novella legislativa, come l'attività degli *exchangers* di *criptovalute* sia stata riconosciuta dal legislatore e inquadrata nell'ambito delle attività di cambiavalute. Nondimeno, nel caso in cui una società svolga l'attività tipica di *exchange* senza adempiere agli obblighi di comunicazione, può essere sanzionata per esercizio abusivo dell'attività.

Dal punto di vista della responsabilità penale, inoltre, l'*exchanger* che non adempisse agli obblighi di verifica della propria clientela potrebbe, in seguito, rispondere del reato di concorso in riciclaggio o in autoriciclaggio, stante la concreta e colpevole agevolazione nella realizzazione del reato. Inoltre, una particolare contestazione di reato agli *exchangers* italiani si è verificata quando in una serie di richieste estorsive connesse all'inoculazione di *ransomware,* veniva un pagamento in *bitcoin.* Le vittime di tali estorsioni, per il pagamento del riscatto, si erano rivolte dunque agli *exchangers* per l'acquisto delle *criptovalute*. Tuttavia, tali società si sono poi ritrovate indagate, in concorso con gli *hackers*, per i reati di estorsione (art. 629 c.p.), danneggiamento di sistema informatico (art. 635-*bis* c.p.) e accesso abusivo al sistema informatico (art. 615-*ter* c.p.). Infine, per quanto concerne la configurabilità di reati tributari in capo agli *exchangers*, giova segnalare come sia la CGUE sia l'Agenzia delle Entrate abbiano più volte sancito che il profitto derivante dall'attività di cambiavalute virtuale rientrino tra le operazioni «relative a divise, banconote e monete con valore liberatorio'di cui all'articolo 135, paragrafo 1, lettera e), della direttiva 2006/112/CE», di guisa che concorrono alla formazione dell'imponibile ai fini IRES mentre risultano esenti ai fini IVA (*Corte di Giustizia UE, Sez. V, 22 ottobre 2015, Causa C-264/14, Skatteverket c. David Hedqvist,* con nota di S. CAPACCIOLI, in «Il Fisco», n. 44, 2015, pp. 4270-4277). Alla luce di ciò, l'*exchanger* che omettesse di dichiarare fedelmente e pienamente il profitto derivante dall'espletamento della propria attività professionale, sarebbe passibile di incriminazione, ai sensi del d.lgs. n. 74/2000, per dichiarazione fraudolenta, omessa dichiarazione e/o dichiarazione infedele (F. BONCOMPAGNI, R. LUVEV*, Criptovalute e profili di rischio penale nella attività degli exchanger*, in «Giurisprudenza Penale», n. 3, 2018, p. 6).

[42] Dal punto di vista giuridico, può ritenersi che la condotta di chi utilizzi la tecnologia *Bitcoin* per occultare proventi di natura illecita sia sussumibile nelle fattispecie di riciclaggio e autoriciclaggio di cui agli artt. 648-*bis* e 648-*ter*, comma 1 c.p., infatti le *criptovalute* rientrano nella nozione codicistica di "utilità", poiché alle stesse viene comunque attribuito un valore, anche se, per ora, limitatamente a chi ricorre, vario titolo, a tale forma di pagamento.

Proprio tale caratteristica ha ampliato il ricorso alle *criptovalute* da parte delle mafie, come dimostrato da varie indagini. Infatti, dal punto di vista del contrasto dei reati di riciclaggio connessi all'utilizzo di *criptovalute*, il principale fattore di criticità è costituito dalla «complicata identificabilità degli indagati; la complessa acquisizione di prove circa le movimentazioni di valuta virtuale e la riconducibilità a soggetti specifici»[43]. Tuttavia, mediante le tradizionali tecniche d'indagine è possibile individuare i conti correnti di partenza e di arrivo finale del denaro riciclato e risalire, in seguito, a tutti i passaggi della movimentazione illecita. Talvolta, inoltre, molteplici indirizzi adoperati per scambiare *criptovalute* afferiscono allo stesso *wallet* e alcuni di questi sono riconoscibili perché hanno la medesima etichetta virtuale, quindi è possibile risalire a dati personali e ricondurlo a una persona fisica; tuttavia, non sempre la persona individuata risulta essere la proprietaria effettiva del patrimonio virtuale anche se, spesso, sono meri prestanome, e, di conseguenza, per poter individuare compiutamente un'operazione di riciclaggio commessa mediante l'impiego di *criptovalute* è sempre possibile e necessaria una attività di investigazione "tradizionale".

Dal punto di vista repressivo, sono molteplici le questioni poste dalla relazione venutasi a creare tra le organizzazioni mafiose e le tecnologie informatiche.

In primo luogo si è osservato come sia necessario il coordinamento sovranazionale fra le indagini che riguardano il *cybercrime* e quelle relative alle mafie, ciò al fine di avere una visione complessiva delle connessioni fra i due fenomeni.

Altra problematica è quella derivante dalla transnazionalità delle condotte illecite e che investe la individuazione del luogo di commissione del reato, elemento che determina la competenza dell'autorità giudiziaria.

Ulteriore aspetto di rilievo riguarda, come già accennato, la possibilità di individuare il reale autore di una determinata condotta illecita. L'attività di inda-

[43] Direzione Nazionale Antimafia ed Antiterrorismo, *relazione* del luglio 2019, https://www.ilsole24ore.com/art/criptovalute-allarme-antimafia-paradiso-finanziario-virtuale-ACXWNXd (consultato il 30 gennaio 2022).

gine in questa materia non può che avvenire mediante complessi accertamenti tecnico/informatici il primo dei quali è l'individuazione dell'indirizzo IP dal quale avvengono le connessioni, attività per la quale è necessario acquisire i dati di accesso alla rete e che richiede sia la collaborazione degli operatori che forniscono la connettività sia la collaborazione giudiziaria internazionale in quanto, spesso, i dati sono contenuti in *server* allocati in più Stati. Ciò richiede regole sovranazionali comuni per permettere all'autorità giudiziaria di potere effettuare le indagini con tempestività ed efficacia.

Infine, la materia informatica, in costante evoluzione tecnologica, ha bisogno anche dell'individuazione di criteri internazionali e scientificamente validati al fine dell'uso nel processo penale affinché siano utilizzabili secondo le regole di quest'ultimo gli accertamenti effettuati sul materiale informatico e digitale[44].

8. Conclusioni

Le considerazioni svolte nel presente articolo consentono di approfondire il fenomeno del *cybercrime* e di comprendere come esso non costituisca un argomento settoriale limitato al solo ambito informatico, ma, per converso, sia una tematica posta in stretta interrelazione a svariati settori d'interesse, tra i più importanti dei quali, vi è certamente la pubblica sicurezza.

Difatti, come è noto, il citato concetto, pur essendosi evoluto nel corso del tempo, ha mantenuto un costante fondamento teorico rappresentato dallo scopo di presidiare l'ordinato e tranquillo esplicarsi della vita dei cittadini, icasticamente sintetizzato nel brocardo latino *ne cives ad arma ruant.*

Attualmente, nell'alveo della pubblica sicurezza vengono ricomprese, in ossequio all'insegnamento del giudice delle leggi, le attività degli apparati statali

[44] Si definisce *computer forensics* ("informatica forense") la scienza che si occupa della preservazione, identificazione e studio delle informazioni che sono contenute nei computer, con lo scopo di evidenziare l'esistenza di prove utili allo svolgimento dell'attività investigative, ed è una branca della *digital forensics*, che analizza i dati di tutti i dispositivi digitali.

attinenti «alla funzione inerente la prevenzione dei reati o al mantenimento dell'ordine pubblico»[45].

Al riguardo, giova precisare che per ordine pubblico debba intendersi, secondo i consolidati approdi della dottrina costituzionalistica, l'insieme dei «principi etici e politici, la cui osservanza ed attuazione sono ritenute indispensabili all'esistenza di tale ordinamento ed al conseguimento dei suoi fini essenziali» (ordine pubblico c.d. "ideale") e «il buon assetto o il regolare andamento del vivere civile, a cui corrispondono, nella collettività, l'opinione e il senso della tranquillità e della sicurezza» (ordine pubblico c.d. "materiale").

Ebbene, la cifra distintiva dei reati informatici è quella di essere connotati da una notevole invasività e lesività nei riguardi della sfera soggettiva e patrimoniale dei cittadini, anche in ragione dell'aspazialità delle tecnologie informatiche.

Nondimeno, come si è avuto modo di osservare in precedenza, il *cybercrime* è divenuto anche uno dei settori d'interesse dalle organizzazioni criminali, che sfruttano le opportunità offerte dalle nuove tecnologie all'uopo di incrementare i propri illeciti profitti. Inoltre, la rete internet viene, purtroppo, adoperata anche da sodalizi criminali di matrice terroristica a fini di propaganda, scambio di informazioni o pianificazione di attentati. Ancora, taluni attacchi *hacker* possono avere ad oggetto anche sistemi informatici di rilevanza nazionale, con il conseguente rischio di una loro distruzione o deterioramento.

Orbene, i suesposti fenomeni risultano essere certamente suscettibili di incrinare l'ordinato andamento della vita civile e la percezione della sicurezza in seno alla pubblica opinione, turbando, in tal modo l'ordine pubblico nella sua accezione materiale, con conseguenti ripercussioni sulla Pubblica Sicurezza.

Invero, alla luce di quanto sopra esposto, certamente ad oggi l'attività di contrasto al *cybercrime* rappresenta uno degli *asset* strategici degli Stati al fine di tutelare la pubblica sicurezza dei cittadini.

L'interrelazione esistente tra il crimine informatico e i concetti in scrutinio è evincibile, inoltre, dalla collocazione a opera del legislatore di taluni reati in-

[45] Corte cost., 24-27 marzo 1987, n. 77 e 23 giugno - 22 luglio 2010, n. 278.

formatici nei titoli del codice penale posti a presidio dell'ordine pubblico e della personalità dello Stato (es. art. 270-*quinquies*, comma 2 c.p., che prevede l'aggravante della commissione mediante strumenti informatici o telematici di condotte di addestramento ad attività con finalità di terrorismo anche internazionale o l'art. 420 c.p. che sanziona, tra l'altro, gli attentati ai sistemi informatici di pubblica utilità).

Allo stato, sicuramente segnali positivi in materia di contrasto al *cybercrime* provengono dalla sempre maggiore specializzazione degli organi inquirenti e dalla crescente attenzione posta al riguardo dal legislatore, testimoniata anche dall'istituzione dell'Agenzia nazionale per la *cybersecurity* e dall'inserimento della sicurezza cibernetica tra le missioni strategiche del Piano nazionale di ripresa e resilienza.

Tuttavia, in ragione della rapida evoluzione che connota le tecnologie digitali e della transnazionalità dei reati informatici, risultano necessarie l'implementazione del coordinamento internazionale tra le varie Autorità deputate al loro contrasto e un'assidua attenzione del legislatore ai fenomeni criminali in atto al fine di porre in essere una tempestiva ed efficace azione di contrasto alle nuove forme di *cybercrime* , anche per il tramite una costante opera di adeguamento della legislazione penale in materia.