UNIVERSITÀ DEGLI STUDI DI MILANO

Dipartimento di Studi internazionali, Giuridici e Storico-Politici

CORSO DI DOTTORATO IN STUDI SULLA CRIMINALITÀ ORGANIZZATA
XXXVIII° CICLO

Tesi di dottorato di ricerca

LA METAMORFOSI DEL CRIMINE ORGANIZZATO NELL'ERA DIGITALE

TUTOR:
Prof. Fabio Basile

CANDIDATA:
Pino Elisabetta
Matricola n. R13769

CO-TUTOR:
Prof. Giovanni Ziccardi

Anno accademico: 2024/2025

INDICE

SEZIONE II
LA MIGRAZIONE DELLA CRIMINALITÀ ORGANIZZATA "TRADIZIONALE" NEL CYBERSPACE: STRUTTURA, FINALITÀ E SFIDE GIURIDICHE

CAPITOLO II
L'inquadramento dell'indagine

CAPITOLO III
La criminalità organizzata "tradizionale" dal mondo fisico al *cyberspace*

CAPITOLO IV

La migrazione digitale delle mafie: problematiche giuridiche e strategie di contrasto

INTRODUZIONE

La presente ricerca si propone di analizzare il nuovo manifestarsi della criminalità organizzata che si fa spazio nel mondo digitale e recepisce le moderne tecnologie tra gli strumenti al suo servizio, con lo scopo ultimo di indagare le conseguenze e le risposte di una tale evoluzione sul piano normativo.

A più di vent'anni dalla Convenzione di Palermo, si assiste, contestualmente alla faticosa modernizzazione dei mezzi di contrasto alla criminalità, ad un'irrefrenabile progressione del fenomeno criminale associativo. Quest'ultimo resta al passo con il cambiamento sociale e prospera nelle sue attività con disinvoltura, approfittando della lenta adattabilità del sistema legislativo e, più in generale, dell'apparato repressivo statuale.

Come noto, infatti, le organizzazioni criminali, ben infiltrate nel tessuto sociale, si contraddistinguono per la capacità di mimetizzazione e di adattamento all'ambiente in cui sono radicate, non limitandosi soltanto a subire gli effetti del cambiamento sociale, ma riproducendone prontamente le patologie.

Diversamente da quanto avvenuto in passato, il proliferare delle organizzazioni criminali nell'era digitale costituisce l'esito, non già di un *deficit* sociale, bensì "di una ipertrofia delle opportunità; non del sottosviluppo, ma del sovrasviluppo"[1].

La criminalità organizzata, nella costante ricerca di "zone d'ombra", ha invero intravisto proprio nel mondo digitale un'opportunità per promuovere, ancor più inosservata, i propri affari illeciti e ha così integrato con celerità le moderne tecnologie nel suo *modus operandi*.

Lo spazio cibernetico o *cyberspace* diviene, così, una meta allettante per le organizzazioni criminali, attratte da maggiore protezione per i loro affari e da minori rischi per i loro membri.

I. Per affrontare in modo esaustivo l'evoluzione del crimine nella società digitale, appare dunque imprescindibile disporre di una conoscenza approfondita delle caratteristiche distintive del cyberspazio.

[1] RUGGIERO V., *Economie sporche. L'impresa criminale in Europa*, Bollati Boringhieri, Torino, 1996, p. 59.

Pertanto, la prima sezione e il primo capitolo del presente lavoro saranno dedicati, in primo luogo, all'analisi degli aspetti vantaggiosi del cyberspazio che attraggono le organizzazioni criminali e favoriscono il proliferarsi delle loro attività illegali: l'anarchia governativa dello spazio cibernetico; la pluridimensionalità spaziale della rete; la volatilità del dato digitale; l'immaterialità e l'a-territorialità dell'illecito virtuale; la commercializzazione delle tecniche del crimine.
In secondo luogo, all'interno di questa prima sezione si fornirà un quadro degli strumenti e delle piattaforme digitali a disposizione della criminalità, come il Deep web, il Dark web e il Dark Market, le criptovalute e le piattaforme di messaggistica criptata, con particolare riferimento alle recenti vicende di smantellamento delle piattaforme Encrochat, SkyEcc e Ghost.
A chiusura del capitolo, infine, si è ritenuto utile fornire un inquadramento dei *cybercrimes*, non circoscritto solo alla tipica classificazione offerta dalla Convenzione di Budapest, ma esteso altresì all'analisi di un'ulteriore categorizzazione, che distingue tra *cyber-enabled crimes* e *cyber-dependent crimes*, analisi, quest'ultima, funzionale ad una migliore comprensione dei successivi capitoli dedicati, tra l'altro, ad esaminare le attività delle differenti organizzazioni criminali operanti nel *cyberspace*.

II. Definito il nuovo contesto criminale, occorrerà inquadrare l'indagine volta a trattare, in maniera sistematica, le organizzazioni criminali che popolano il *cyberspace*.
Come illustrato in un secondo capitolo, di natura ancora introduttiva, la ricerca si concentrerà sull'analisi di due diversi gruppi criminali, distinti in relazione al ruolo della tecnologia e alle modalità di interazione tra dimensioni online e offline.
In particolare, la differenziazione tra due principali tipologie di gruppi criminali trova il proprio fattore scriminante nella tecnologia, il cui differente ruolo influenza in modo sostanziale l'organizzazione criminale, tanto sul fronte strutturale, relativo all'architettura interna ed operativa del gruppo, quanto sul fronte teleologico, attinente alle attività e agli scopi criminali.
A tal proposito, numerosi studi accademici e rapporti di organizzazioni internazionali hanno identificato tre principali tipologie di gruppi criminali che utilizzano la tecnologia in modi differenti.

La presente trattazione si avvarrà della distinzione operata da queste istituzioni internazionali, basandosi sui dati disponibili riguardanti i legami tra il crimine organizzato e il crimine informatico, il livello di coinvolgimento dei gruppi nelle attività online rispetto a quelle offline e la struttura interna delle associazioni criminali.
In particolare, si individuano tre gruppi principali: i gruppi di tipo I, che operano principalmente online e si dedicano esclusivamente ai crimini informatici; quelli tipo II, che svolgono attività sia online che offline, impegnandosi in crimini tradizionali e crimini informatici; infine, i gruppi di tipo III, che utilizzano le tecnologie dell'informazione e della comunicazione per facilitare crimini offline, senza però compiere reati direttamente legati al mondo digitale.
Di questi tre gruppi, che rappresentano diverse modalità con cui la tecnologia interagisce con le attività criminali, quelli di tipo I e quelli di tipo III, - dalle caratteristiche marcatamente più differenti - saranno oggetto di due distinte sezioni del presente lavoro di ricerca.
La sezione II, in particolare, si proporrà di esaminare, nei capitoli III e IV, le organizzazioni criminali "tradizionali" che migrano nel *cyberspace* (gruppi n. III), con lo scopo, rispettivamente, di esplorare come e se l'uso della tecnologia ha modificato la struttura di tali gruppi e influito nelle loro operazioni criminali, e di analizzare, d'altra parte, le conseguenze di tale evoluzione sul piano normativo.
Dall'altro lato, la sezione III sarà invece dedicata all'analisi della criminalità organizzata, prettamente di tipo cibernetico (gruppi di tipo I), e all'inquadramento giuridico di quest'ultima.

III. Pertanto, una volta chiarito e compreso il contesto di riferimento e inquadrata preliminarmente l'indagine, la seconda sezione del presente lavoro sarà dedicata, come già anticipato, dapprima (cap. III), alla criminalità organizzata "tradizionale" migrante nel cyberspace e all'analisi delle principali attività criminali che si servono della tecnologia; successivamente (cap. IV), all'inquadramento delle principali questioni giuridiche sorte a seguito di tale evoluzione digitale.
In proposito, rispetto al crimine organizzato "tradizionale", che impiega i servizi digitali come "facilitatori" del crimine, non sembrerebbe ravvisarsi alcuna radicale modificazione teleologica, restando intatti gli scopi e le attività illecite, legate comunque ad una base

offline. Si tratterebbe, piuttosto, di un semplice fenomeno migratorio del crimine organizzato "tradizionale" in un altro contesto criminale che gli impone una trasformazione del *modus operandi*.

Pertanto, sul piano giuridico, il percorso che si vuole intraprendere, con riferimento al modello della criminalità organizzata "tradizionale", mira allo svolgimento di un'indagine sull'impatto normativo dell'evoluzione digitale: si guarderà non solo agli effetti che passivamente "subisce" il sistema normativo, ma altresì alle eventuali reazioni dello stesso sistema come parte attiva.

Nel corso di quest'ultima indagine, pertanto, bisognerà valutare se gli strumenti normativi a disposizione possano considerarsi sufficienti al contrasto di una criminalità organizzata così avanzata. In particolare, occorrerà domandarsi se le misure normative attuali, previste in materia di diritto penale sostanziale e processuale dispongano di un grado di elasticità tale da potersi adattare al cambiamento delle nuove organizzazioni criminali.

Saranno, pertanto, analizzate, dapprima, le varie problematiche giuridiche sorte a seguito di tale "migrazione digitale" delle mafie e, in un secondo momento, verranno illustrate le prospettive di intervento e le strategie di contrasto a tali sfide giuridiche.

In primo luogo, verrà esaminato il tema delle comunicazioni criptate, considerate una delle principali sfide per l'ordinamento penale contemporaneo, sia per le difficoltà investigative che pongono, sia per le delicate questioni di compatibilità con i diritti fondamentali. A tal fine, l'analisi si svilupperà attraverso un *excursus* che prende in considerazione le posizioni critiche maturate dalla dottrina e dalla giurisprudenza antecedenti l'intervento delle Sezioni Unite, proseguendo con la prospettiva europea delineata dalla Corte di Giustizia, fino a giungere ai contributi forniti dalle Sezioni Unite, i quali, pur fornendo elementi risolutivi, lasciano aperti profili interpretativi di particolare rilievo.

Successivamente, l'indagine giuridica si focalizzerà sul fenomeno delle criptovalute e sulle modalità di riciclaggio digitale, con una ricognizione delle principali implicazioni che tali strumenti comportano sul piano della criminalità economico-finanziaria. In tale contesto, vengono approfondite le dinamiche di de-individualizzazione dell'azione criminosa, la delocalizzazione geografica e giuridica dei comportamenti illeciti e la dematerializzazione dell'oggetto del reato, fattori che accentuano l'opacità delle condotte e pongono sfide regolatorie e investigative non indifferenti. Completano l'analisi i

mercati illegali del dark web, dove la tecnologia e la struttura decentralizzata degli spazi digitali rendono particolarmente ardua l'azione delle forze dell'ordine e mettono in evidenza significativi vuoti normativi ancora non colmati.
Nella seconda parte della ricerca, l'attenzione si sposterà sulle prospettive di intervento e sulle strategie di contrasto alla criminalità digitale, con un'analisi delle scelte normative di armonizzazione sovranazionale della disciplina probatoria e della circolazione dei dati digitali, nonché delle potenziali riforme volte a regolamentare in maniera più efficace e coerente le comunicazioni criptate. Verranno altresì esaminate le nuove tecniche investigative digitali, le criticità derivanti dalla progressiva obsolescenza delle categorie probatorie tradizionali, le iniziative volte a definire un quadro regolatorio organico dei *crypto-asset* e le prospettive di riforma per una sistematizzazione penalistica delle criptoattività.
Il percorso di indagine si concluderà con un approfondimento sui più recenti strumenti investigativi e sulle tecniche innovative impiegabili nel contrasto ai cripto-reati, evidenziando come la trasformazione tecnologica abbia imposto una revisione complessiva dei paradigmi di indagine e di tutela penale.

IV. Guardando invece al secondo percorso di indagine, la criminalità organizzata nativamente cibernetica sarà dettagliatamente analizzata nella sezione III, nella quale il capitolo V sarà principalmente dedicato alle caratteristiche strutturali dei gruppi cibernetici (gruppi di tipo I e II) e all'analisi delle principali attività criminali da questi attuate.
Inoltre, considerata la novità del *cyber-organised crime* e la sua lontananza dalla struttura e dal *modus operandi* tipico delle tradizionali organizzazioni criminali, nel capitolo VI, di tipo prettamente giuridico, verrà adottato un differente approccio rispetto a quello della sezione precedente.
L'indagine farà infatti un passo indietro, essendo ancora alquanto controverso l'inquadramento giuridico di questo fenomeno nella categoria della criminalità organizzata. Ciò in quanto, a differenza del modello di criminalità precedentemente analizzato, la tecnologia, oltre ad essere strumento per la commissione dei crimini, è altresì parte intrinseca dell'attività del gruppo criminale e ne influenza i connotati teleologici e strutturali.

Come si è anticipato, infatti, gli strumenti digitali vengono impiegati per la prevalente commissione di crimini cibernetici, conseguendone, pertanto, una divergenza nei "reati fine" tipici del tradizionale crimine organizzato. D'altro canto, poi, dalla più alta presenza della componente tecnologica deriva una notevole semplificazione nell'organizzazione del gruppo criminale.

Per queste ragioni, da vari studi sulla criminalità organizzata cibernetica emerge la maggioritaria considerazione che l'attribuzione dell'etichetta di "*organised crime*" non sia empiricamente giustificata, ma che sia, piuttosto, conferita al solo fine di creare sensazionalismo o, ancora, allo scopo di perseguire delle politiche securitarie di contrasto alla criminalità organizzata.

La suddetta questione definitoria andrà comunque affrontata attraverso lo studio dei casi più noti di *cyber-organised crime*. Pertanto, risulterà preliminarmente necessario procedere a un'analisi dell'istituto dell'associazione per delinquere, di cui all'art. 416 c.p., concentrandosi sui suoi requisiti essenziali e sulle modalità con cui dottrina e giurisprudenza ne hanno definito i confini applicativi. Solo disponendo di questo quadro di riferimento sarà possibile valutare come la giurisprudenza abbia giuridicamente inquadrato i principali gruppi criminali digitali, esaminando le soluzioni interpretative adottate e le eventuali problematiche sorte nell'inquadramento di tali organizzazioni all'interno della fattispecie prevista dal codice penale. Nell'ambito dei casi concreti bisognerà, infatti, ricercare gli elementi costitutivi richiesti dal reato associativo di cui all'art. 416 c.p. (in specie, lo stabile vincolo associativo, il programma indeterminato di delitti e la struttura organizzativa) ed altresì analizzare l'elasticità giurisprudenziale nell'adattamento di tali elementi a forme associative morfologicamente eterogenee.

Verranno così analizzati, attraverso l'esame di casi concreti, i profili associativi che emergono nelle diverse tipologie di comunità criminali digitali.

In primo luogo, si prenderanno in considerazione le comunità online dedite allo scambio di materiale pedopornografico, nelle quali la giurisprudenza ha dovuto interrogarsi sulla sussistenza di un vincolo stabile tra soggetti spesso geograficamente distanti e collegati esclusivamente tramite piattaforme virtuali.

In secondo luogo, sarà approfondito il fenomeno degli hacktivisti, con particolare attenzione al caso emblematico di Anonymous, che solleva questioni complesse in ordine all'individuazione di una struttura organizzativa e alla definizione di ruoli all'interno di

un gruppo caratterizzato da un'estrema fluidità e dall'assenza di gerarchie formalizzate. A ciò si aggiungerà l'analisi delle comunità virtuali ibride dedite alle truffe online, nelle quali si riscontrano modelli associativi a metà strada tra forme di collaborazione occasionale e vere e proprie organizzazioni criminali, con il conseguente problema di stabilire la soglia oltre la quale la condotta diventa penalmente rilevante ai sensi dell'art. 416 c.p.

L'obiettivo sarà quello di mettere in luce come la giurisprudenza, nel confrontarsi con tali realtà, abbia progressivamente adattato i criteri tradizionali di accertamento dell'associazione criminosa – pensati per fenomeni mafiosi o comunque radicati nel territorio – a contesti radicalmente nuovi, caratterizzati dall'anonimato, dalla decentralizzazione e dall'assenza di legami fisici tra i partecipi.

SEZIONE I
IL NUOVO CONTESTO CRIMINALE: IL *CYBERSPACE*

CAPITOLO I
Il quadro della ricerca:
lo spazio cibernetico e le nuove prospettive del crimine

SOMMARIO **1.** Il *cyberspace*: nuova meta per il crimine organizzato. – **2**. I vantaggi del *cyberspace* per le organizzazioni criminali. – **3.** Strumenti e piattaforme digitali a disposizione della criminalità. – **3.1.** Deep Web, Dark Web e Dark Market. – **3.2.** Criptovalute: Bitcoin, Monero e altre monete digitali al servizio del crimine organizzato. – **3.3.** Piattaforme di messaggistica criptata tra legalità e illegalità. – **3.3.1.** Le piattaforme di messaggistica "sicura": WhatsApp, Telegram e Signal tra privacy e potenziale abuso da parte dei criminali. – **3.3.2.** La crittografia al servizio dei criminali: dalla nascita allo smantellamento di Encrochat, SkyEcc e Ghost. – **3.3.2.1.** Encrochat. – **3.3.2.2.** SkyEcc – **3.3.2.3.** Ghost. – **4.** Il *cyberspace* nuovo terreno di reati: i *cybercrimes*. – **4.1.** La categorizzazione dei *cybercrimes* nella Convenzione di Budapest e nella nuova Convenzione ONU sul *cybercrime***.** – **4.2.** I crimini cyber dipendenti e i crimini facilitati dal cyber.

1. Il *cyberspace*: nuova meta per il crimine organizzato

Nella nostra "società digitale" o "*digital society*", quale insieme delle trasformazioni sociali, culturali ed economiche derivanti dall'adozione diffusa delle tecnologie, le tecnologie dell'informazione e della comunicazione (ICT) svolgono un ruolo fondamentale nel modo in cui le persone interagiscono, lavorano, apprendono e accedono alle informazioni[2].

La digitalizzazione ha senza dubbio influito sulla comunicazione sociale in termini di velocità ed estensione: la costante connessione tra le persone, garantita dall'utilizzo di internet, rende infatti la comunicazione istantanea, e soprattutto globale.

[2] Cfr. CASTELLS M., *The Internet galaxy: Reflections on the Internet, business and society*, Oxford University Press, Oxford, 2001; LUPTON D., *Digital sociology*, Routledge, London, 2014.

A ciò si aggiunga, poi, la semplicità e l'immediatezza nell'accesso all'informazione e alla conoscenza, oltre che l'espansione delle transazioni economiche e la nascita di nuovi modelli di business derivante dal commercio elettronico e dall'impiego di piattaforme digitali[3].

La società digitale ha certamente avuto un impatto non indifferente anche sul mondo criminale. Il crimine si modifica, strutturalmente e funzionalmente: cambiano il *modus operandi*, le interazioni fra gli attori criminali, le relazioni autore-vittima[4].

In particolare, il panorama informativo, fortemente digitalizzato, ha aperto la strada a nuove forme di criminalità organizzata. Quest'ultima, nella costante ricerca di "zone d'ombra", ha invero intravisto proprio nel mondo digitale un'opportunità per promuovere, ancor più inosservata, i propri affari illeciti e ha così integrato con celerità le moderne tecnologie nel suo *modus operandi*[5].

Tali manifestazioni criminali, per quanto continuino a presentare elementi di continuità e di connessione con le attività illecite del passato, si caratterizzano al contempo per una significativa discontinuità. Se, infatti, da un lato, le reti criminali si abilitano alla tecnologia, dall'altro lato, invece, è proprio la stessa tecnologia ad avere consentito lo sviluppo di nuove reti criminali più complesse e digitalizzate[6].

Per affrontare in modo esaustivo lo studio e l'analisi dell'evoluzione del crimine nella società digitale, appare dunque imprescindibile un'indagine sul nuovo contesto criminale rappresentato dal cyberspazio, meglio noto con il termine anglosassone *cyberspace*. In particolare, una comprensione approfondita delle caratteristiche distintive del cyberspazio appare dunque fondamentale per delineare i tratti salienti delle forme di criminalità contemporanea.

Fin dalla metà degli anni '90 il cyberspazio è stato oggetto di studio di numerosi esperti che hanno tentato di definirne la natura e le caratteristiche.

---

[3] Cfr. STRATTON G., POWELL A., CAMERON R., *Crime and justice in digital society: Towards a 'digital criminology'*, in *International Journal for Crime Justice Social Democracy*, 6, 2, 2017, pp. 17–33; GRANIERI G., *La società digitale*, Editori Laterza, 2006; BETTINELLI E., *Società digitale/società della conoscenza: per una ulteriore analisi, tra progresso e crisi*, in *Studi di Sociologia*, 3, 2022, pp. 493-508.

[4] Cfr. DI NICOLA A., *Towards digital organized crime and digital sociology of organized crime*, in *Trends in Organized Crime*, 2022, p. 4.

[5] Cfr. MARTINU, O., MCEWEN, G., *Crime in the age of technology*, in E*uropean law enforcement research Bulletin*, (4 sce), Cepol, 2018, p. 24.

[6] In proposito v. DEMETIS D., *Organised crime The Cyber dimension*, in *A research agenda for organized crime*, a cura di Barry Rider, 2023.

Lo spazio cibernetico è uno spazio virtuale ed intangibile, non è un dominio puramente naturale come tutti gli altri, ma una realtà artificiale ed ibrida alla cui formazione concorrono sia elementi naturali che virtuali. Il cyberspazio può essere infatti concepito come uno spazio definito a partire da una base naturale, rappresentata dallo spettro elettromagnetico, ma la cui configurazione è intrinsecamente influenzata dall'intervento umano. Sono infatti le tecnologie sviluppate dall'uomo a determinare non solo la struttura di questo ambiente, ma anche le sue caratteristiche peculiari e le problematiche ad esso associate[7].

Sarebbe dunque errato concepire tale spazio come una realtà fittizia, alternativa a quella fisica, dal momento che nient'altro è che un'espansione e un prodotto del mondo fisico stesso[8].

Da questa prospettiva, il cyberspazio si presenta anzitutto come uno spazio integrato, frutto dell'interazione tra diverse tecnologie dell'informazione. Inoltre, si configura come uno spazio aperto, facilmente accessibile a chiunque, grazie a costi relativamente contenuti in termini di competenze e risorse necessarie per interagire attraverso le tecnologie ICT[9].

2. I vantaggi del *cyberspace* per le organizzazioni criminali

L'accessibilità e l'integrazione dello spazio cibernetico costituiscono, tuttavia, un'arma a doppio taglio, dal momento che, non solo incentivano la partecipazione di individui e aziende, ma rappresentano, come anticipato, un ambiente fertile per il proliferare di attività illecite e, dunque, una meta allettante per le organizzazioni criminali. Queste ultime, infatti, approfittando di barriere d'ingresso basse e facilmente accessibili e della possibilità di operare in modo anonimo, trovano nel mondo virtuale un terreno

[7] Cfr. KUEL T. D., *From Cyberspace to Cyberpower: Defining the Problem*, in *Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Cyberpower and National Security*, in *National Defence University Press*, 2009, pp. 28 e ss. ne fornisce la seguente definizione "*a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdipendent and interconnected networks using information – communication technologies*"; LIBICKI M. C., *Cyberdeterrence and Cyberwarfare*, Santa Monica, 2009, pp. 11-37.

[8] Sul punto, PICARELLA L., *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, Roma, Donzelli Editore, 2025.

[9] Cfr. MIRTI M., *Struttura e caratteri del Cyberspace*, in *Opinio Iuris Law and Politics review*, 2020.

ideale per espandere i propri affari. La combinazione di opportunità e protezione diventa così un fattore chiave nella crescita delle operazioni criminali[10].

Per tali ragioni, pare opportuno e fondamentale, ai fini della presente ricerca, vagliare i benefici che le organizzazioni criminali possono trarre dal trasferimento, o dalla diretta fondazione, delle loro attività illecite nel mondo virtuale.

Prima tra tutti, l'*"anarchia" governativa* dello spazio cibernetico, appetibile agli scopi criminali in quanto *terra nullius*, priva di regole e di controllo[11]. Le organizzazioni criminali operano, pertanto, senza timore di sanzioni immediate o di interventi da parte delle autorità; in più, la mancanza di coordinamento internazionale e l'eterogeneità normativa tra diversi paesi rendono difficile l'immediata individuazione della legge applicabile, consentendo ai criminali di sfruttare le debolezze del sistema e di muoversi liberamente tra giurisdizioni.

Si pensi, in secondo luogo, alla *pluridimensionalità spaziale della rete*, che offre una complessità pluridimensionale che rende difficile l'identificazione degli attori criminali[12]. L'anonimato, garantito, ad esempio, da tecnologie come VPN e criptovalute, di cui si dirà più avanti, complica ulteriormente le indagini, poiché non solo ostacola l'identificazione dei soggetti criminali, ma rende anche arduo il rintracciamento di profitti illeciti, poiché i fondi possono essere trasferiti rapidamente tra diverse piattaforme e con differenti valute, rendendo il processo di rilevamento estremamente complesso[13].

Le organizzazioni criminali possono altresì trarre vantaggio dalla *volatilità del dato digitale*, connotato che, a sua volta, ne agevola l'occultamento, la distruzione, l'alterazione. Si pensi, ad esempio, alle tecniche di *data wiping* (cancellazione dei dati) e

---

[10] Sulle opportunità del *cyberspace*, v. GRABOSKY P., *The Internet, Technology, And Organized Crime,* in *Springer Science*, 2007, p. 156; KOOPS B., *The Internet and its Opportunities for Cybercrime,* in *Tilburg Law School Legal Studies Research Paper Series*, 9, 2011, p. 740; LAVORGNA A., *Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics,* in *Trends in Organised Crime*, 17, 4, 2014, p. 250; BRENNER S. W., *Organized Cybercrime? How Cyberspace may affect the structure of criminal relationships,* in *North Carolina Journal of Law & Technology*, 4, 1, 2002, p. 39; MINNAAR A., *Organised Crime And The 'New More Sophisticated' Criminals Within The Cybercrime Environment: How 'Organised' Are They In The Traditional Sense?,* in *Acta Criminologica: Southern African Journal of Criminology,* 29, 2, 2016, p. 126.

[11] Cfr. ANSALONE G., *Cyberspazio e nuove sfide*, in *GNOSIS – Rivista italiana di intelligence*, 3, 2012, p. 41.

[12] Cfr. SABELLA P.M., *Il fenomeno del cybercrime nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali*, in *Informatica e diritto*, XXVI, 1-2, 2017, p. 148.

[13] Sul *money laundering*, v. KRUISBERGENA E.W., LEUKFELDT E.R., KLEEMANSC E.R, ROKSD R.A., *Money talks money laundering choices of organized crime offenders in a digital age*, in *Journal of Crime and Justice*, 42, 5, 2019, p. 574.

di crittografia, che consentono ai criminali di proteggere le loro comunicazioni e di eliminare tracce di attività illecite. In aggiunta, la diffusione di strumenti di *hacking* e *malware* rende ancora più accessibile la capacità di alterare o cancellare informazioni[14].

Anche l*'immaterialità e* l*'a-territorialità dell'illecito virtuale* contribuiscono ad ostacolare la definizione del *tempus* e del *locus commissi delicti*[15] e ad intralciare lo svolgimento dell'attività cautelare ed investigativa e l'individuazione delle relative autorità competenti[16]. Infatti, dal momento che i reati possono essere commessi da chiunque e ovunque nel mondo, e dal momento che non esiste un "luogo di reato" tradizionale, le autorità devono affrontare sfide significative nella definizione della giurisdizione competente. Al contempo, l'incertezza sulla legge applicabile e la difficoltà nel determinare il "dove" e il "quando" del crimine rendono complessa l'interazione tra le varie autorità legali. Questo caos normativo offre, di conseguenza, alle organizzazioni criminali un vantaggio strategico non indifferente.

Infine, le organizzazioni criminali traggono un indubbio beneficio dalla *commercializzazione delle tecniche del crimine online*, vale a dire la possibilità che queste tecniche, una volta sviluppate dagli esperti, possano essere condivise e cedute; a ciò consegue la facile replicabilità dei reati e la semplificazione delle modalità operative del crimine organizzato che potrà comodamente limitarsi ad acquistare un servizio criminale, senza doversi impegnare direttamente nella progettazione del crimine[17]. La facilità di accesso e la disponibilità di tecniche criminali online, da tutorial di hackeraggio a servizi di "*crime as a service*"[18], democratizzano l'accesso al crimine, consentendo a chiunque abbia accesso a Internet di acquisire strumenti per compiere reati, senza l'esigenza di

---

[14] Cfr. Consiglio d'Europa, *Convenzione sulla criminalità informatica*, STE n.185, 2001, in *www.coe.int*; MINNAAR A., *Organised Crime And The 'New More Sophisticated' Criminals Within The Cybercrime Environment: How 'Organised' Are They In The Traditional Sense?,* cit., p. 126; sulle conseguenze processuali delle attività illecite su web, LUPÀRIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (l. 18 Marzo 2008, n. 48). I profili processuali*, in *Dir. pen. proc.*, 6, 2008, pp. 717 ss.

[15] In argomento, v. SABELLA P.M., *Il fenomeno del cybercrime nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali*, cit., p. 148; CAMPLANI F., *Locus commissi delicti, norme di collegamento e reati informatici a soggetto passivo indeterminato*, in *Archivio Penale*, 2. 2020.

[16] Cfr. SABELLA P.M., op. ult. cit.; CAMPLANI F., op. ult. cit.

[17] Sulla commercializzazione delle tecniche criminali nel *cyberspace,* v. Europol's European Cybercrime Centre, Trend Micro Research, Unicri,, *Malicious Uses and Abuses of Artificial Intelligence*, 2020, in *https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence#downloads*; sulla facile replicabilità dei crimini nel *cyberspace*, v. CALDWELL M., ANDREWS J. T. A., TANAY T., GRIFN L. D., *AI-enabled future crime*, in *Crime Science*, 2020.

[18] Cfr. Europol, *Cyber-Attacks: The Apex Of Crime-As-A-Service*, IOCTA 2023.

competenze tecniche avanzate. Questo non solo abbassa la barriera per l'ingresso per le nuove organizzazioni criminali, ma rende anche più facile per i gruppi esistenti espandere le loro operazioni[19]. L'acquisto di servizi criminali consente, inoltre, di esternalizzare attività ad alto rischio, come l'hacking o il riciclaggio di denaro, a professionisti del crimine, aumentando la loro efficienza e riducendo il rischio personale. Tramite questo modello commerciale innovativo, le organizzazioni criminali si concentrano, dunque, su strategie di alto livello, lasciando i dettagli operativi a esperti esterni[20].

La tecnologia agisce in questo senso come una "forza moltiplicatrice": persino chi non dispone di adeguate risorse può avervi accesso ed abusarne[21]. Secondo questa prospettiva, dunque, l'utilizzo di tecnologie sofisticate interrompe la diretta proporzionalità tra la dimensione del gruppo criminale e l'offesa arrecata, rendendo potenzialmente pericolosi persino gruppi di ridotte dimensioni[22].

3. Strumenti e piattaforme digitali a disposizione della criminalità

Al fine di favorire una lettura più chiara dei capitoli a seguire, si rende necessaria un'analisi del funzionamento delle principali piattaforme e dei principali strumenti utilizzati dalla criminalità organizzata.

3.1. Deep web, Dark Web e Dark Market.

Tra le principali piattaforme digitali che hanno favorito la prosperazione delle organizzazioni criminali nel *cyberspace* figura indubbiamente il Dark Web, realtà profondamente diversa dal web di fruizione comune.

In proposito, prima di illustrarne le peculiarità, pare opportuno evidenziare in questa sede come il Surface Web (o Web visibile/indicizzato), al quale accediamo quotidianamente tramite i motori di ricerca più noti - come Google e Bing – rappresenti soltanto una parte limitata del contenuto complessivamente disponibile online. Tutto ciò che non è indicizzato dai motori di ricerca si colloca invece nel Deep Web, dove la ricerca

[19] Cfr. PICARELLA L., *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, cit.
[20] Cfr. DEMETIS D., *Organised crime The Cyber dimension*, cit.
[21] Sul punto, v. YAR M., *Cybercrime and society*, London, Sage, 2006, p. 12.
[22] Cfr. MC GUIRE M., *Organised crime in the digital age*, London, John Grieve Center for policy and security and Bae, 2012.

dell'informazione è resa estremamente più complessa dalla mancata indicizzazione dei contenuti[23].

Nell'ambito di questo "web sommerso" si colloca proprio il Dark Web, dove sono collocati contenuti e siti intenzionalmente nascosti e criptati. Non a caso, al Dark Web è possibile accedere solo con software specializzati di crittografia che mascherano l'indirizzo IP dell'utente, rendendo ardua la sua identificazione.

All'apparenza, dunque, i mercati darknet o cryptomarket si presentano esteriormente come piattaforme di commercio elettronico, non dissimili da eBay o Amazon; la differenza sostanziale risiede, tuttavia, nell'affidamento a tecnologie di crittografia e anonimizzazione che li rendono impermeabili a controlli esterni.

Per tali ragioni, il Dark Web si configura come un vero e proprio mercato illecito, che fornisce servizi ai criminali e si sviluppa grazie alla sua natura senza confini e all'anonimato. È altresì sede di "forum di discussione", tramite cui è permesso ai criminali comunicare, condividere informazioni e pianificare le proprie attività illegali[24]. Oltre a fungere da vetrina per l'offerta e la compravendita di beni e servizi illegali – dalle sostanze stupefacenti alle armi, dagli organi alle valute contraffatte – offre altresì la possibilità di "affittare" esperti informatici per eseguire attività illegali, come il riciclaggio di denaro tramite servizi automatizzati di mixing di criptovalute[25].

Il primo mercato darknet ad acquisire notorietà fu Silk Road[26], attivo da gennaio 2011 e sequestrato dall'FBI nel mese di ottobre 2013. Alla sua chiusura seguì subito Silk Road 2.0, aprendo la strada ad una proliferazione di darkmarket, con una stima di oltre 100 mercati emersi fino ad oggi[27].

---

[23] In proposito v. DEMETIS D., *Organised crime The Cyber dimension*, cit., pp. 3 ss.; anche ALEXANDROU A., *Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security*, *Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices*, CRC Press, 2022, pp. 76 ss.

[24] Cfr. MARTINU, O., MCEWEN, G., *Crime in the age of technology*, cit., p. 4; Europol, *Serious and Organised crime threat assessment, A Corrupting Influence: The Infiltration And Undermining Of Europe's Economy And Society By Organised Crime*, 2021, in *https://www.europol.europa.eu/publications-events/main-reports/socta-report*, pp. 22 ss; BERTOLA F., *Drug Trafficking on Darkmarkets: How Cryptomarkets are changing drug global trade and the role of organized crime,* in *American Journal of Qualitative Research*, 4, 2, 2020, pp. 27-34.

[25] Cfr. CHAWKI M., *The Dark Web and the future of illicit drug markets*, in *Journal of Transportation Security*, 2022.

[26] *Ibidem*; KRISHNAN A., *Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organization*s, in *Journal of Strategic Security*, 13, 1, 2020, pp. 41-58.

[27] Sul punto sempre CHAWKI M., *The Dark Web and the future of illicit drug markets*, cit.; a questo proposito, anche European Commission, Europol*, Drugs and the darknet: Perspectives for enforcement, research and policy,* Publications Office of the European Union*, 2017.*

Al centro delle attività illegali del darkmarket si colloca certamente il commercio di droghe illecite[28]. I cryptomarket offrono infatti al criminale una nuova modalità per trafficare la droga poiché, contrariamente ai modelli iniziali di distribuzione gestiti per via centralizzata e gerarchica da gruppi di criminalità organizzata, forniscono un nuovo canale, prevalentemente a distribuzione diretta, per il flusso di droga tra diverse località; ciò implica che non saranno più coinvolti trafficanti di droga, mediatori, grossisti, rivenditori di strada o altri intermediari, ma che le droghe verranno semplicemente inviate online direttamente dai produttori ai consumatori, senza la necessità di contatti personali o interazioni tra le parti[29]. A ciò si aggiunge che i darkmarket offrono la possibilità ai trafficanti di droga di estendere la loro base di clienti al di fuori della loro area fisica controllata, diminuendo la concorrenza locale con altri trafficanti, tipica invece dei mercati fisici[30].

In tema invece di rapporto tra venditore e acquirente, i venditori di droga operanti online sono in grado di interagire con clienti sconosciuti, grazie alla fiducia offerta dai meccanismi di anonimato integrati nel marketplace[31], ma anche dai feedback lasciati dai clienti precedenti. Gli stessi venditori, inoltre, possono pubblicizzare apertamente i loro prodotti in vendita a qualsiasi utente del marketplace, migliorando anche la loro "reputazione" online tramite feedback e recensioni lasciate dai precedenti compratori[32].

L'esistenza di tali reti di distribuzione più dirette, intercorrenti tra consumatori e produttori di droga, potrebbe all'apparenza limitare significativamente il coinvolgimento dei narcotrafficanti, della criminalità organizzata e delle bande di strada nella distribuzione delle droghe. Tuttavia, secondo un recente rapporto dell'Europol su "Come le droghe illegali sostengono la criminalità organizzata nell'UE", sui darkmarket "*sebbene si valuti che la maggior parte dei venditori siano criminali solitari, che trattano piccole*

[28] United Nations Office on Drugs and Crime, *Use Of The Dark Web And Social Media For Drug Supply*, in World Drug report, 2023, pp. 223-234.
[29] In proposito v. MARTIN J., *Lost on the Silk Road: Online drug distribution and the 'cryptomarket'*, in *Criminology and Criminal Justice*, 14, 2013, pp. 351–367.
[30] Sul punto v. MORSELLI, C., TURCOTTE, M., TENTI, V, *The mobility of criminal groups*, in *Global Crime*, *12*, 2011, pp. 165–188.
[31] Cfr. BARRATT M.J., *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*, UK Palgrave pivot, 2014.
[32] Cfr. ALDRIDGE, J., DÈCARY-HÈTU, D.,*Cryptomarkets and the future of illicit drug markets. In the internet and drug markets* (pp. 23–30), EMCDDA, Publication Office of the European Union, 2016, pp. 23-30.

quantità, è stato segnalato che molti dei 'venditori di punta' sono probabilmente gruppi di criminalità organizzata che guadagnano profitti significativi"[33].

A questo proposito, non può infatti ignorarsi – tematica che ci riserva di approfondire in altra sede – che le mafie spesso operano in qualità di "fornitori" di droga, fungendo da collegamento tra i mercati internazionali di droga e i venditori locali e operando su diverse catene di approvvigionamento con una pluralità di rivenditori, anche nel darkweb[34].

3.2. Criptovalute: Bitcoin, Monero e altre monete digitali a servizio del crimine organizzato

Le criptovalute, monete digitali basate su tecnologie crittografiche, hanno rapidamente guadagnato popolarità dal loro esordio con il Bitcoin, prima criptovaluta rilasciata nel 2008, e basata su un sistema decentralizzato. In tale modello, per la validazione delle transazioni, l'intervento di un ente centrale o di un istituto di credito viene sostituito con un sistema *peer-to-peer*, basato su una prova crittografica, invece che sulla fiducia interpersonale, consentendo a due parti di negoziare direttamente tra loro senza la necessità di un intermediario[35].

Tre tratti distintivi rendono le criptovalute particolarmente appetibili tanto per gli utenti legittimi, quanto per soggetti criminali: anonimato, decentralizzazione e irreversibilità delle transazioni.

Dal momento che le transazioni tramite criptovalute non sono convalidate da un unico intermediario ma dagli stessi utenti, va sottolineato che tutte le operazioni effettuate nella rete Bitcoin vengono registrate su un "libro contabile", noto come *distributed ledger*, accessibile a ciascun utente tramite il proprio computer. Tale libro è composto da una serie di blocchi concatenati di transazioni (blockchain) che vengono poi condivisi all'interno della rete. Sebbene, grazie a questo sistema di registrazione, le transazioni Bitcoin siano pubbliche, e dunque visibili e accessibili a chiunque in qualsiasi momento, ciò non implica tuttavia una piena trasparenza riguardo alle identità dei soggetti coinvolti, che restano anonimi. In altre parole, le operazioni Bitcoin sono tracciabili, ma ciò non

[33] Europol, *How Illegal Drugs Sustain Organised Crime in the EU*, 2017.
[34] Cfr. BERTOLA F., *Drug Trafficking on Darkmarkets: How Cryptomarkets are Changing Drug Global Trade and the Role of Organized Crime,* cit.
[35] Cfr. NAKAMOTO S., *Bitcoin: A peer-to-peer electronic cash system*, 2008.

consente di identificare con certezza le persone o entità che le effettuano. Infatti, seguendo la catena delle transazioni, ciò che emerge non è un nome, ma una stringa alfanumerica complessa, difficile da risolvere e praticamente impossibile da ricondurre direttamente a una persona fisica o giuridica[36].

Inoltre, accanto a criptovalute teoricamente tracciabili come Bitcoin, ne esistono altre, come Monero o Zcash, progettate per garantire un maggiore anonimato, mascherando l'identità degli utenti e i dettagli delle transazioni. Questo rende alle autorità difficile, se non impossibile, seguire il flusso di denaro tra i partecipanti, consentendo a chi compie attività illecite di operare senza il rischio di essere facilmente identificato[37].

In secondo luogo, a differenza delle valute tradizionali, le criptovalute non sono emesse da una banca centrale o da un ente governativo, ma si basano su un sistema decentralizzato di nodi di rete, che consente alle transazioni di essere convalidate senza la necessità di un intermediario centralizzato, come una banca. La decentralizzazione impedisce altresì che le criptovalute siano soggette ai controlli e alle regolamentazioni tradizionali, consentendo ai criminali di eludere le normative bancarie e fiscali[38]. Si tratta, pertanto, di un sistema "*open source*", connotato dall'operare di soggetti indipendenti che operano e cooperano in via autonoma, senza il controllo centralizzato e monopolistico di un ente[39].

Questo "processo di disintermediazione" è uno dei profili che rende le criptovalute particolarmente appetibili per il crimine organizzato. Mentre, infatti, in un sistema tradizionale di riciclaggio, il denaro viene trasferito da una persona o da un'organizzazione a un'altra attraverso banche o altri istituti finanziati, obbligati a

---

[36] Cfr. POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, in *Diritto penale contemporaneo*, 2, 2019, pp. 164 ss.

[37] Cfr. ALEXANDROU A., *Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices*, cit., pp. 76 ss; DEMETIS D., *Organised crime The Cyber dimension*, cit.

[38] In proposito v. POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, cit., p. 161 ss.; KRISHNAN A., *Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations*, cit., pp. 41-58; ALBRECHT C. ET AL., *The use of cryptocurrencies in the money laundering process*, in *Journal of Money Laundering Control*, 22, 2, 2019, p. 214.; CAMPBELL-VERDUYN, *Bitcoin and beyond: cryptocurrencies, blockchains and global governance*, Routledge, 2018, p. 74. In argomento, si veda la definizione di "dematerializzazione" fornita da CONSULICH F., *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali, in Diritto penale e processo,* 2, 2022, p. 153 come "*collocazione delle transazioni in un ecosistema in cui i servizi (dai prestiti, ai pagamenti fino agli investimenti) vengono forniti senza la supervisione e regolazione di un'autorità pubblica*".

[39] Cfr. PASSERELLI N., *Bitcoin e antiriciclaggio*, in *Gnosis, Rivista italiana di intelligence*, 2016.

rispettare rigidamente le normative contro il riciclaggio di denaro e sul finanziamento del terrorismo, con le criptovalute, invece, questi passaggi intermediari vengono eliminati, e le transazioni avvengono direttamente tra il venditore e l'acquirente, senza la supervisione di istituzioni finanziarie o agenzie governative[40].

Grazie a queste caratteristiche, che rendono il sistema vulnerabile all'abuso e ne impediscono il monitoraggio, le criptovalute sono diventate uno strumento fondamentale per il *darknet* e, in particolare, per le operazioni di riciclaggio di denaro[41]. Come detto, il mercato *darknet* è il luogo dove la maggior parte delle attività illegali legate alle criptovalute si svolge con venditori e acquirenti che operano in totale anonimato, scambiando beni e servizi illeciti come droghe, armi e dati rubati. In questo contesto, le criptovalute fungono, dunque, da strumento privilegiato per il riciclaggio di denaro sporco, poiché gli utenti possono utilizzare i *mixers*[42] (software che mescolano le transazioni per renderle più difficili da tracciare) o le monete anonime per ripulire i proventi di attività criminali. Ad esempio, come si dirà nel dettaglio nel prosieguo del presente lavoro, attraverso un processo chiamato "*smurfing*", i criminali suddividono grosse somme di denaro in piccole transazioni per mascherarne l'origine illecita e trasferirle attraverso il network di criptovalute senza attirare l'attenzione delle autorità[43].

3.3.Piattaforme di messaggistica criptata tra legalità e illegalità

Nell'ambito dell'ecosistema del cyberspazio, anche le piattaforme di messaggistica criptata hanno acquisito un'importanza crescente per le attività criminali.

La crittografia *end-to-end* che caratterizza tali piattaforme digitali e che implica che solo il mittente e il destinatario, che dispongono delle chiavi necessarie, sono in grado di leggerne i contenuti - rappresenta infatti un'arma a doppio taglio: se da un lato offre maggiore sicurezza e privacy agli utenti legittimi, dall'altro lato, fornisce alle

---

[40] Cfr. POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, cit., p. 161 ss.
[41] Cfr. DI LERNIA A., *Crowdfounding @ ICOs: esigenze di prevenzione del rischio di commissione di reati nell'era della digital economy,* in *DPC*, 2, 2019, p. 106.
[42] Sul punto v. DEMETIS D., *Organised crime The Cyber dimension*, cit., p. 8.
[43] Cfr. Europol, *Serious and Organised crime threat assessment, A Corrupting Influence: The Infiltration And Undermining Of Europe's Economy And Society By Organised Crime*, cit., p. 29; DELL'OSSO A., *Riciclaggio di proventi illeciti e Sistema penale*, in *Itinerari di diritto penale*, collana diretta Dolcini E., Fiandaca G., Musco E., Padovani T., Palazzo F., Sgubbi F., Giappichelli Editore, Torino, 2017, p. 36 ss.

organizzazioni criminali uno strumento efficace per evitare l'intercettazione delle loro comunicazioni da parte delle forze dell'ordine[44].

In questa sede, si propone una panoramica sulla storia e sul funzionamento delle principali piattaforme di messaggistica criptata, analizzando in che modo si sono evolute nel tempo, quali tecnologie utilizzano per garantire la sicurezza delle comunicazioni e come si distinguono in termini di funzionalità e protezione. In seguito, ci si riserva di dedicare un'apposita trattazione all'impiego specifico di tali strumenti da parte della criminalità organizzata, con un focus particolare sull'abuso delle tecnologie di cifratura da parte di gruppi illeciti come strumento facilitatore delle attività criminose.

3.3.1. Le piattaforme di messaggistica "sicura": WhatsApp, Telegram e Signal tra privacy e potenziale abuso da parte dei criminali

La tecnologia VoIP (Voice over IP) ha favorito la nascita di numerose applicazioni di messaggistica e chiamate vocali, come Skype, WhatsApp, Signal, e altre. Queste piattaforme, basate sulla rete internet, hanno abbattuto i limiti geografici e i costi associati alle comunicazioni tradizionali. La trasmissione dei dati avveniva, in origine, tramite il protocollo TCP/IP[45] per inviare e ricevere dati sotto forma di pacchetti, utilizzando il protocollo HTTP[46]. Tuttavia, in assenza di cifratura, queste comunicazioni restavano intercettabili. Ragion per cui, per ovviare a questa vulnerabilità a garanzia della privacy, è stato introdotto il protocollo HTTPS[47], che garantisce invece la cifratura delle comunicazioni, rendendo più complessa l'intercettazione dei dati[48].

---

[44] Cfr. PUJIA P., *L'acquisizione della messaggistica criptata conservata su server straniero tra classificazioni concettuali e divergenze giurisprudenziali*, in *Archivio Penale*, 2024, 2, p. 3.

[45] Il protocollo TCP/IP (*Transmission Control Protocol / Internet Protocol*) è un insieme di regole utilizzato per la trasmissione di dati su reti, come Internet. TCP gestisce la trasmissione affidabile dei dati, suddividendoli in pacchetti e garantendo che arrivino correttamente al destinatario, mentre IP si occupa dell'indirizzamento e del routing dei pacchetti tra dispositivi. Insieme, questi protocolli permettono la comunicazione tra computer e dispositivi su reti locali e globali.

[46] *Hypertext Transfer Protocol* è un protocollo di comunicazione che consente al browser e al server web di scambiarsi informazioni su Internet.

[47] *Hypertext Transfer Protocol Secure*. Contrariamente al precedente protocollo, con HTTPS il sito utilizza la versione sicura di http dal momento che si escludono rischi di intercettazioni e furti di credenziali. Inoltre, un'altra differenza chiave tra i due protocolli risiede nella possibilità per il proprietario con un proxy HTTPS di impiegare una chiave privata per verificare di esserne il legittimo proprietario, impedendo l'accesso al sito ad utenti non autorizzati.

[48] Cfr, RAMPIONI M., *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, in *Giurisprudenza penale*, 10, 2023, p. 4; CURTOTTI D., RIZZI V., NOCERINO W., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e*

È opportuno precisare che le piattaforme di messaggistica criptata possono comunque essere rilevate: vale a dire che le forze dell'ordine o altre agenzie possono identificare l'esistenza di una comunicazione che avviene attraverso questi servizi, non potendo, però, facilmente intercettarne nel loro contenuto, almeno non senza l'accesso diretto ai dispositivi o alle chiavi di cifratura.

Detto altrimenti, le forze dell'ordine, o altre entità, possono comunque rilevare il traffico criptato, ossia possono notare che esiste una comunicazione che passa attraverso un determinato server, una determinata applicazione o una determinata rete. Ad esempio, i metadati di una comunicazione (come l'indirizzo IP di origine e destinazione, l'ora, la durata e il volume del traffico) possono essere monitorati senza che sia noto il contenuto dei messaggi. E benché ciò consenta di identificare che una comunicazione è avvenuta, non è tuttavia possibile rilevare cosa è stato detto o inviato.

La cifratura rende quindi i messaggi illeggibili a chiunque non possieda le chiavi di decifrazione; anche se il traffico è intercettato, i dati risultano dunque incomprensibili.

È bene ora passare in rassegna le principali piattaforme di messaggistica criptata, con lo scopo di illustrarne brevemente le caratteristiche e le differenze quanto al funzionamento e alle garanzie di anonimato.

WhatsApp è stata l'app di messaggistica che ha reso la crittografia *end-to-end* una caratteristica standard per la maggior parte delle piattaforme di messaggistica moderne. Fondata nel 2009 da Jan Koum e Brian Acton, WhatsApp ha rapidamente guadagnato popolarità grazie alla sua semplicità e alla possibilità di inviare messaggi gratuitamente via Internet. La piattaforma ha introdotto nel 2016, in collaborazione con Open System Whispers, la crittografia *end-to-end* [49], tramite la quale si garantiva la cifratura dei messaggi sul dispositivo del mittente con possibile decriptazione solo sul dispositivo del destinatario. Tuttavia, l'autenticazione dell'utente tramite numero di telefono costituisce un possibile punto debole, consentendo di legale le comunicazioni direttamente a un'identità personale verificabile tramite SIM card. Inoltre, WhatsApp consente agli utenti di fare backup delle chat su cloud (Google Drive o iCloud), ma questi backup non

prova penale, in *Sistema penale*, 6, 2023, pp. 173 ss; BASSOLI E., *I crimini informatici, il dark web e le web room*, Pacini giuridica, 2021, p. 131.

[49] Cfr. SANTONS M. ET AL., *Affordance is power: contradictions between communicational and technical dimensions of Whatsapp's end-to-end encryption*, in *Social media and Society*, 2018; AHMED W. ET AL., *Whatsapp network Forensics: discovering the IP addresses of suspects, in International Conference of new technologies*, 2021.

sono cifrati *end-to-end*, il che significa che se qualcuno ottiene l'accesso al cloud, potrebbe leggere i messaggi. Questo è uno dei principali limiti in termini di privacy rispetto ad altre piattaforme, come Signal, di cui dopo si illustrerà il funzionamento[50].

Telegram, app di messaggistica tra le più note ed utilizzate, fondata nel 2013 dai fratelli Nikolai e Pavel Durov, non utilizza, contrariamente a Whatsapp, la crittografia *end-to-end* per le chat normali, bensì una crittografia *server-client*[51], il che implica che i messaggi risultano cifrati nella fase di trasmissione tra i singoli dispositivi e i server di Telegram, potendo tuttavia essere letti sui server stessi. Ciò in quanto Telegram ha la capacità di decrittografare i messaggi in transito e archiviarli sui suoi server, rendendo questa piattaforma meno sicura di WhatsApp in termini di privacy. Al contempo, però, Telegram offre una funzionalità, attivabile solo manualmente, chiamata "chat segrete", che utilizza la crittografia *end-to-end*, garantendo che solo il mittente e il destinatario possano leggere i messaggi. Tra le varie opzioni in termini di sicurezza e privacy, Telegram consente inoltre agli utenti di impostare la distruzione automatica dei messaggi nelle chat segrete, con un timer che elimina i messaggi dopo un periodo di tempo predefinito[52].

Signal è infine un'applicazione non profit di messaggistica criptata, fondata nel 2010 da Brian Acton (co-fondatore di WhatsApp) e Moxie Marlinspike. Tale piattaforma si serve del Signal Protocol (lo stesso adottato da WhatsApp per la crittografia *end-to-end*) per garantire che tutte le comunicazioni siano sicure e private. Tuttavia, contrariamente a WhatsApp, Signal è open-source[53], ovvero riduce al minimo la raccolta di metadati e non associa l'account a sistemi di backup esterni.

---

[50] In proposito, v. MUSIANI F., *La crittografia nei sistemi di messaggistica sicura: le libertà digitali tra sviluppo tecnologico e regolazione*, in *Rivista di Digital Politics*, 3, 2022, pp.423-442; SIMIOL E. ET AL., *A security analysis comparison between Signal, WhatsApp and Telegram,* in *Cryptology ePrint Archive*, 2023.

[51] *Ibidem*; SEELAM N., PALISETTI V., *Comparative research of WhatsApp and Telegram by using heuristic principles*, Faculty of Computing, Sweden, 2022, p. 7.

[52] Cfr. LAIBY T., SUBRAMANYA B., *A Comprehensive Overview of Telegram Services - A Case Study*, in *International Journal of Case Studies in Business, IT, and Education*, 6, 1, 2022.

[53] Cfr. ROSLER P. ET AL., *More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema*, in *EuroS&P*, 2018, p. 6; SIMIOL E. ET AL., *A security analysis comparison between Signal, WhatsApp and Telegram,* cit.

3.3.2. La crittografia al servizio dei criminali: dalla nascita allo smantellamento di Encrochat, SkyEcc e Ghost

Alcune piattaforme di messaggistica criptata sono nate e si sono diffuse come soluzioni alternative rivolte principalmente a gruppi criminali. Queste piattaforme, infatti, non solo offrivano la crittografia *end-to-end*, ma implementavano anche misure di sicurezza aggiuntive, come dispositivi hardware modificati, per rendere più difficile l'intercettazione delle comunicazioni.

Per anni, strumenti di comunicazione criptata, noti come *criptofonini*, hanno rappresentato uno dei principali canali di comunicazione della criminalità organizzata. Le operazioni condotte dalle forze di polizia europee contro reti come Encrochat e SkyEcc rappresentano casi di studio emblematici, in quanto mostrano l'elevato livello di sofisticazione tecnologica raggiunto da tali piattaforme.

Maggiori dettagli sulle operazioni di polizia aventi ad oggetto tali strumenti di comunicazione criptata verranno forniti nel prosieguo del presente lavoro, in cui si descriveranno più approfonditamente non solo le modalità di acquisizione dei dati da parte delle autorità internazionali, ma anche le successive questioni, su cui si è espressa giurisprudenza nazionale ed internazionale, relative alla legittimità dell'utilizzo dei dati intercettati.

3.3.2.1. Encrochat

EncroChat è stata una delle piattaforme maggiormente utilizzate dal crimine organizzato, in particolare per il traffico di droga e per altre attività illecite. Fondata nel 2016, EncroChat si è distinta per l'utilizzo di smartphone modificati, i già menzionati "criptofonini", dotati di un software progettato a garantire comunicazioni sicure.

Segnatamente, i dispositivi utilizzati per la comunicazione sicura sono in genere telefoni standard, come dispositivi Android o anche Blackberry, il cui software viene modificato con l'installazione di un sistema operativo che disabilita diverse funzionalità per ridurre i rischi di intercettazione e localizzazione, come il GPS, i servizi Google, il Bluetooth, la fotocamera e la porta USB (che resta attiva solo per la ricarica). Le chiamate vocali restano attive, ma avvengono esclusivamente tramite VoIP, mentre la messaggistica è consentita solo tramite applicazioni crittografate. Entrambi i tipi di

comunicazioni – chiamate e messaggi – sono crittografati con diversi livelli di sicurezza e sono generalmente progettati per funzionare in modalità *peer-to-peer*, senza che le comunicazioni vengano archiviate sui server[54]. Gli utenti possono anche scegliere se fare il backup dei propri dati (come i contatti) e, in caso affermativo, decidere dove memorizzarli, mantenendosi comunque un sistema di cifratura anche sui dati oggetto di backup[55]. I dispositivi dispongono, inoltre, di funzionalità particolari come la cancellazione automatica dei messaggi e la protezione tramite password di emergenza ("*kill switch*")[56].

Per tali ragioni di sicurezza e privacy, gran parte degli utenti abbonati ad Encrochat impiegavano i criptofonini per lo svolgimento di attività illegali, come il traffico di droga, il riciclaggio di denaro o traffico di armi.

L'indagine digitale sulla rete di comunicazione criminale criptata Encrochat ha rappresentato una delle prime in Europa condotte così in ampia scala, frutto della cooperazione coordinata tra la squadra investigativa congiunta (JIT) franco-olandese, Europol, Eurojust e la National Crime Agency (NCA) britannica.

La NCA aveva individuato le operazioni illegali di EncroChat già dal 2016, rilevando che le comunicazioni che transitavano sulla rete erano state utilizzate principalmente per coordinare il traffico di droga, riciclare denaro e pianificare eliminazioni di rivali nel crimine[57]. A livello globale, sono stati stimati circa 60.000 utenti del servizio, di cui 10.000 nel Regno Unito[58].

---

[54] Cfr. STOYKOVA, R., *Encrochat: The hacker with a warrant and fair trials?*, in *Forensic Science International: Digital Investigation*, 46, 2023.
[55] *Ibidem*.
[56] Sul punto v. MIRANDA M. L., *L'utilizzabilità delle chat criptate acquisite mediante ordine europeo di indagine*, in *Quotidiano Legale*, 4, 2024, p. 4; CURTOTTI D. ET AL., *Piattaforme criptate e prova penale*, cit., p. 177.
[57] Cfr. RAGAZZI S., SPIEZIA F., *Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano*, in *Sistema penale*, 2, 2024, p. 205.
[58] Cfr. National Crime Agency*, NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation*, 2020, https://www.nationalcrimeagency.gov.uk/news/operation-venetic; Europol/Eurojust press release, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, 2 luglio 2020; GUAGLIARDI G., *Utilizzo nel processo penale di messaggi criptati ottenuti tramite una operazione di hacking massiva all'estero e acquisiti in Italia tramite Ordine Europeo di Indagine. Il fine giustifica i mezzi?,* in *Giurisprudenza penale*, 2024, 6, p. 5; STOYKOVA R., *Encrochat: The hacker with a warrant and fair trials?*, cit.

Solo verso la fine del 2019, le autorità francesi hanno ottenuto l'autorizzazione per avviare le indagini[59], dando il via ad una serie di operazioni congiunte, quali "Operation Venetic" nel Regno Unito, "Operation Emma 95" in Francia e "Operation Lemont" nei Paesi Bassi[60].

A partire dalla fine di marzo 2020, le polizie europee hanno avviato un programma di sorveglianza massiva delle comunicazioni attraverso EncroChat che ha consentito di raccogliere informazioni vitali per prevenire crimini e procedere con gli arresti. In particolare, la polizia francese è riuscita a localizzare i server di Encrochat e, ottenuto l'accesso, li ha utilizzati per installare un *trojan* mascherato da aggiornamento di sicurezza sui telefoni degli utenti, consentendo l'intercettazione in tempo reale dei messaggi criptati. Sebbene il metodo esatto di decifrazione non sia stato chiarito, si ipotizza che il malware abbia acquisito le chiavi di decrittazione o intercettato comunicazioni già decriptate[61].

Nel giugno 2020, l'operazione, nota come "Operazione Venetic", ha rivelato al pubblico la decodifica di milioni di messaggi provenienti da migliaia di utenti in tutta Europa[62]. I risultati sono stati significativi: nel Regno Unito 746 arresti con il sequestro di 54 milioni di sterline, 77 armi da fuoco e oltre due tonnellate di droga[63]. In Francia, invece, "Operation Emma 95" ha condotto a più di 100 arresti, alla chiusura di 19 laboratori di droghe sintetiche e al sequestro di oltre 20 milioni di euro, oltre a 9,2 tonnellate di droga, armi e beni di lusso. Infine, l'"Operazione Lemont" nei Paesi Bassi

---

[59] In proposito v. RAGAZZI S., SPIEZIA F., *Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italianocit.*; Europol/Eurojust press release, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, cit.; OERLEMANS J.J., VAN TOOR D., *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in E*uropean journal of crime, criminal law and criminal justice*, 30, 2022, pp. 309–328.

[60] Cfr. RAGAZZI S., SPIEZIA F., *Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano*, cit., p. 206; GUAGLIARDI G., *Utilizzo nel processo penale di messaggi criptati ottenuti tramite una operazione di hacking massiva all'estero e acquisiti in Italia tramite Ordine Europeo di Indagine. Il fine giustifica i mezzi?,* cit., p. 5; STOYKOVA R., *EncroChat: The hacker with a warrant and fair trials?,* cit..

[61] Cfr. STOYKOVA R., *EncroChat: The hacker with a warrant and fair trials?,* in *Forensic Science International: Digital Investigation*, 46, 2023.

[62] Cfr. Europol/Eurojust press release, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, cit.; GUAGLIARDI G., *Utilizzo nel processo penale di messaggi criptati ottenuti tramite una operazione di hacking massiva all'estero e acquisiti in Italia tramite Ordine Europeo di Indagine. Il fine giustifica i mezzi?,* cit., p. 5.

[63] Cfr. HARINAM V., BARAK A., *Law Enforcement Strategies for Disrupting Cryptomarkets*, Springer, 2024, p. 53.

ha contribuito al sequestro di oltre 9 tonnellate di stupefacenti e alla confisca di 25 automobili, armi, orologi di valore e denaro[64].

3.3.2.2. SkyEcc

Un destino analogo ha interessato SkyEcc, altro fornitore di criptofonini largamente impiegato nel narcotraffico internazionale.

Come EncroChat, SkyEcc forniva dispositivi crittografati con software personalizzato per garantire la sicurezza delle comunicazioni. I telefoni SkyEcc erano dotati di crittografia avanzata e includevano misure di sicurezza come l'auto-distruzione dei messaggi e l'assenza di dati identificativi legati alle SIM card[65].

Anche con SkyEcc, il 9 marzo 2021 il panorama è cambiato, quando le forze di polizia di Belgio, Paesi Bassi e Francia hanno annunciato di aver decifrato i messaggi scambiati tramite la piattaforma.

Già dal 2015 le forze dell'ordine olandesi e francesi erano a conoscenza dell'uso a scopi criminali dei telefoni SkyEcc; nel 2018, le autorità belghe hanno avviato indagini mirate, scoprendo che i server si trovavano presso il provider di hosting OVH a Roubaix, in Francia. [66].

Così, nel dicembre 2018, ordini di indagine europei hanno permesso alle autorità francesi e belghe di acquisire l'immagine dei server per verificarne la configurazione tecnica, avviando formalmente l'indagine nel febbraio 2019, con l'autorizzazione, altresì di intercettare e trascrivere le comunicazioni che passavano attraverso i server[67].

Nel giugno e luglio 2019, le forze dell'ordine francesi hanno intercettato e condiviso con le altre autorità i dati intercettati su due server di OVH, identificando gli oggetti delle chiamate di gruppo e gli Sky ID degli utenti.

L'1 novembre 2019, le forze dell'ordine di Paesi Bassi, Belgio e Francia hanno istituito un "Team di Investigazione Congiunto" (JIT) per raccogliere prove sulle attività criminali

---

[64] Cfr. Europol/Eurojust press release, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, cit.
[65] Cfr. PUJIA P., *L'acquisizione della messaggistica criptata conservata su server straniero tra classificazioni concettuali e divergenze giurisprudenziali*, cit., p. 3.
[66] Cfr. OERLEMANS J., ROYER S., *The future of data-driven investigations in light of the Sky ECC operation*, in *New Journal pf European Criminal law*, 14, 4, 2023.
[67] *Ibidem*.

di Sky Global e dei suoi utenti, condividendo risorse e conoscenze tecniche. L'accordo prevedeva la condivisione dei dati intercettati dai server OVH in Francia per smantellare SkyEcc e determinare se fosse utilizzato per facilitare attività criminali[68].

L'intercettazione dei dati è stata autorizzata fino al 9 Marzo 2021, quando l'operazione è stata resa pubblica, portando a numerosi arresti e intercettazioni: interettati 1 miliardo di messaggi intercettati, con 500 milioni decrittati nel primo mese, fornendo alle forze dell'ordine prove cruciali per future indagini[69].

Nel momento in cui è stato violato, si stima che SkyEcc avesse più di 170.000 utenti a livello globale, con circa 70.000 in Europa e tra i 12.000 e i 15.000 in Italia, con oltre 80 milioni di messaggi intercettati e scambiati tra gli utenti[70].

In particolare, nel 2023, la cosiddetta "*Operazione Eureka",* condotta da Europol ed Eurojust in stretta cooperazione con 10 Stati europei, ha segnato un passaggio cruciale nella lotta alla criminalità organizzata, culminando con l'arresto di 132 soggetti legati a potenti clan della ndrangheta operanti nella provincia di Reggio Calabria[71].

L'attività di infiltrazione all'interno della piattaforma si è rivelata determinante per l'individuazione e la cattura di Rocco Morabito, storico boss della ndrangheta e per anni secondo latitante più ricercato d'Italia. Grazie alla penetrazione nella piattaforma, gli investigatori sono riusciti a monitorare in tempo pressoché reale gli spostamenti del capo mafioso e dei suoi sodali[72].

Le informazioni acquisite hanno altresì consentito di assicurare alla giustizia altri esponenti di rilievo delle organizzazioni criminali internazionali, tra cui Vincenzo Pasquino, ritenuto il braccio destro del boss calabrese[73].

---

[68] *Ibidem*.
[69] *Ibidem*.
[70] *Ibidem*.
[71] Cfr. LAVORGNA A SERGI A., *Intergenerational and technological changes in mafia- type groups: a transcultural research agenda to study the 'ndrangheta and its mobility*, in *SN Social Sciences*, 2024, p. 192.
[72] In proposito, è stata oggetto di consultazione l'ordinanza di applicazione cautelare personale nei confronti, tra gli altri, di Rocco Morabito, del Gip del Tribunale di Reggio Calabria, p.p. n. 4837/2022 r.g.n.r. d.d.a. e l'ordinanza di applicazione di misure cautelari custodiali in carcere nei confronti, tra gli altri, sempre di Rocco Morabito, del GIP del Tribunale di Genova, p.p. 6267/2021 r.g.n.r.
[73] Cfr. sempre l'ordinanza di applicazione di misure cautelari custodiali in carcere nei confronti, tra gli altri, sempre di Rocco Morabito, del GIP del Tribunale di Genova, p.p. 6267/2021 r.g.n.r.; anche la stampa riferisce in proposito, v. https://lavialibera.it/it-schede-1199-l_ultima_chat_dei_narcos

Non meno rilevante è stato, infine, il contributo offerto dalla piattaforma allo svelamento delle articolate attività dell'arco piccante Raffaele imperiale, permettendo di ricostruire con chiarezza i suoi affari illeciti a livello internazionale[74].

3.3.2.3. Ghost

Ghost rappresenta l'ultima piattaforma di messaggistica criptata che ha guadagnato attenzione delle autorità per il suo utilizzo da parte di gruppi criminali, in particolare per il traffico di droga e altre attività illecite.

Come SkyEcc e EncroChat, Ghost permette di inviare messaggi e chiamate tramite dispositivi sicuri, con crittografia *end-to-end*.

La piattaforma, creata nel 2016 da un 32enne australiano di origini coreane, aveva acquisito notorietà dopo la chiusura di altre piattaforme simili, grazie alle sue avanzate misure di sicurezza: non era necessario fornire alcun dato personale durante l'acquisto, offriva tre livelli di crittografia e consentiva di eliminare tutti i messaggi tramite un codice apposito[75]. Non sorprende, dunque, come tale piattaforma ben si prestasse ad attività illegali di vario tipo, tra cui il traffico di droga su larga scala, il riciclaggio di denaro e altre operazioni criminali[76].

Secondo quanto riportato da Europol, la piattaforma veniva utilizzata da migliaia di persone in tutto il mondo, con circa mille messaggi scambiati ogni giorno[77]. Pur rimanendo di dimensioni inferiori rispetto ai network di Encrochat o SkyEcc, la piattaforma veniva comunque considerata altamente rilevante, stante anche quanto osservato dal dirigente di Europol, secondo cui il panorama delle comunicazioni criptate è oggi più frammentato e popolato da reti minori che, tuttavia, talvolta si rivelano ospitare i criminali più influenti[78].

---

[74] Sul punto, ordinanza di custodia cautelare nei confronti, tra gli altri, di Raffaele Imperiale, del Gip del Tribunale di Napoli, p.p. n. 32678/16 r.g.n.r.
[75] Cfr, Europol, *Global Coalition Takes Down New Criminal Communication Platform*, 18 settembre 2024.
[76] Cfr. Europol, *Global Coalition Takes Down New Criminal Communication Platform*, 18 settembre 2024.
[77] *Ibidem*.
[78] Europol press conference, 18 settembre 2024; sul punto, si consultino anche altri fonti di stampa, "Europol provides detail on Ghost encrypted comms platform takedown" in https://www.computerweekly.com/news/366611232/Europol-provides-detail-on-Ghost-encrypted-comms-platform-takedown.

Di recente, anche quest'ultima piattaforma è stata "bucata" dalle forze dell'ordine tramite un'operazione internazionale che ha visto la cooperazione delle autorità di nove paesi, cooperazione resasi necessaria a causa della differente localizzazione tra i server, collocati in Francia ed in Islanda, e le attività finanziarie illecite, che invece si svolgevano negli Stati Uniti.

Nel marzo 2022 l'Europol ha istituito una task force operativa (Otf), coinvolgendo autorità di polizia di Australia, Canada, Francia, Irlanda, Islanda, Italia, Paesi Bassi, Svezia e Stati Uniti, sotto la supervisione giuridica dei paesi del Joint investigation team (Jit), istituita dall'Eurojust[79].

L'azione della task force si è rivelata duplice: da un lato, ha permesso di mappare l'infrastruttura tecnica globale della piattaforma e di colpire i suoi nodi più sensibili, identificando fornitori e utenti chiave[80]; dall'altro lato, l'Australian Federal Police (AFP) è stata strategicamente in grado di intercettare migliaia di messaggi su dispositivi australiani, intervenendo sugli aggiornamenti software che l'amministratore di sistema distribuiva regolarmente agli utenti, aggiornamenti apparentemente innocui, ma modificati in modo da infettare i dispositivi e consentire l'intercettazione di migliaia di messaggi[81].

L'operazione, conclusasi nel settembre 2024 con lo smantellamento della piattaforma, ha portato a un totale di 51 arresti: 38 in Australia, 11 in Irlanda, uno in Canada e uno in Italia. In Italia, in particolare, il 13 settembre scorso è stato arrestato, grazie a questa operazione di polizia, Giovanni Parlangeli, latitante della Sacra Corona Unita[82].

4. Il *cyberspace* nuovo terreno di reati: i *cybercrimes*

Da ultimo, questo capitolo introduttivo non può prescindere da un breve inquadramento dei *cybercrimes*, non circoscritto alla tradizionale classificazione offerta dalla Convenzione di Budapest, ma esteso ad un'ulteriore categorizzazione, di tipo duale, che distingue tra *cyber-enabled crimes* e *cyber-dependent crimes*. Ciò in quanto, sulla

[79] Europol, *Global Coalition Takes Down New Criminal Communication Platform*, cit..
[80] *Ibidem.*
[81] AFP press release, "*AFP Operation Kraken charges alleged head of global organised crime app*", 18 settembre 2024, https://www.afp.gov.au/news-centre/media-release/afp-operation-kraken-charges-alleged-head-global-organised-crime-app.
[82] Cfr. Europol, *Global Coalition Takes Down New Criminal Communication Platform*, cit..

definizione dei *cybercrimes*, con cui genericamente si intende ricomprendere quei comportamenti criminali commessi in tutto o in parte online, appare più opportuno fare riferimento ad alcuni tentativi definitori basati sulle categorizzazioni del fenomeno, potendo le singole definizioni risultare alquanto riduttive e poco esplicative[83].

In particolare, la distinzione tra *cyber-enabled crimes* e *cyber-dependent crimes* si rivelerà essenziale per comprendere appieno le modalità con cui diverse organizzazioni criminali operano nel contesto digitale, tematica oggetto di approfondimento nel capitolo successivo.

4.1. La categorizzazione dei cybercrimes nella Convenzione di Budapest e nella nuova Convenzione ONU sul cybercrime

Il principale sistema di classificazione dei crimini informatici è fornito dalla famosa Convenzione sulla Criminalità Informatica del Consiglio d'Europa (CoE), firmata a Budapest nel 2001. La Convenzione di Budapest, integrata nel tempo da protocolli aggiuntivi, rappresenta, infatti, un punto di riferimento cruciale per la lotta internazionale contro i crimini informatici. È il primo trattato internazionale giuridicamente vincolante che stabilisce una base per la cooperazione tra i paesi nella prevenzione e nel contrasto della criminalità informatica, nonché nella protezione dei dati e della privacy[84].

La sezione è suddivisa in cinque titoli[85].

Il titolo I comprende il nucleo centrale dei reati informatici, ossia i reati contro la riservatezza, l'integrità e la disponibilità dei dati e dei sistemi informatici, rappresentando questi ultimi le minacce basiche a cui sono esposti i sistemi di elaborazione elettronica dei dati e di comunicazione. Vengono trattati, in particolare, sia l'accesso illegale che la manipolazione o interferenza illecita di sistemi, programmi o dati.

---

[83] Cfr. PAYNE R., *Defining cybercrime*, in *The Palgrave handbook of international cybercrime and cyberdeviance*, (a cura di) T. Holt – A. Bossler, Palgrave Macmillan, Cham, 2020.

[84] Sui profili relativi alla ratifica della Convenzione, v. PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale,* in *Dir. pen. proc.*, 6, 2008.

[85] Sul punto, PICOTTI L., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo,* in *Dir. Internet,* 2008, pp. 437-448; DOBRIINOIU M., *Proposals for a broader approach of misuse of devices and programs' provision in combating cyber-dependent and cyber-enabled crimes*, in *Lex et Scientia International Journal*, XXXI, 1, 2024; Consiglio d'Europa, *Explanatory Report to the Convention on Cybercrime*, ets n. 185.

Nel titolo II, invece, vengono descritti altri tipi di "reati informatici", che rivestono un ruolo maggiore nella pratica, giacché i sistemi informatici e di telecomunicazione, a differenza del caso precedente, vengono utilizzati come mezzo per attaccare determinati interessi giuridici che, nella maggior parte dei casi, sono già protetti dal diritto penale contro attacchi che utilizzano mezzi tradizionali. Si tratta, in altre parole, di crimini che utilizzano i sistemi informatici per commettere reati legati ad attività tradizionali, come la frode e la falsificazione, ma con l'ausilio della tecnologia, reati che sono stati aggiunti seguendo le indicazioni contenute nelle linee guida della Raccomandazione n. R (89) 9 del Consiglio d'Europa.

Il titolo III riguarda i "reati legati ai contenuti", come la produzione e distribuzione illecita di pornografia minorile tramite l'uso di sistemi informatici, considerata una delle modalità operative più pericolose degli ultimi tempi. Sebbene il comitato che ha redatto la Convenzione abbia discusso sulla possibilità di includere altri reati legati ai contenuti, come la distribuzione di propaganda razzista tramite sistemi informatici, non è stato tuttavia in grado di raggiungere un consenso sulla criminalizzazione di tale condotta, scegliendo di rinviare la questione al Comitato europeo sui problemi criminali (CDPC) per redigere un protocollo aggiuntivo alla presente Convenzione.

Il titolo IV stabilisce i "reati legati alle violazioni del diritto d'autore e dei diritti connessi". Questo è stato incluso nella Convenzione perché le violazioni del diritto d'autore rappresentano una delle forme più diffuse di crimine informatico di allarme internazionale.

Infine, il titolo V include disposizioni aggiuntive sul tentativo, assistenza e favoreggiamento, sanzioni e misure, e, in conformità con i recenti strumenti internazionali, sulla responsabilità degli enti[86].

È opportuno chiarire, da ultimo, che le disposizioni della Convenzione non si applicano solo ai reati in essa definiti, che si possono denominare "cibernetici in senso proprio", ma anche a tutti i reati commessi mediante un sistema informatico, nonché a qualsiasi altro reato di cui si debbano o possano raccogliere "prove in forma elettronica" (art. 14, paragrafo 2 ed art. 23). Questi reati possono definirsi cibernetici "in senso

[86] *Ibidem*.

improprio" dato che sono potenzialmente comprensivi di qualsivoglia fattispecie delittuosa, anche non realizzata nel *cyberspace*[87].

Sempre in tema di criminalizzazione di *cybercrimes*, non può non farsi menzione della recente Convenzione ONU sul *cybercrime*, il cui testo definitivo è stato adottato dall'Assemblea Generale il 24 dicembre 2024 e sarà aperto alla firma dal 25 ottobre 2025 fino a dicembre 2026, divenendo vincolante solo con il raggiungimento della quarantesima ratifica.

Rispetto alla Convenzione di Budapest, sotto il profilo della criminalizzazione, la nuova Convenzione introduce un rilevante ampliamento delle condotte punibili, inserendo nel proprio catalogo normativo diverse fattispecie che testimoniano una maggiore sensibilità verso le minacce digitali emergenti[88]. Tra le innovazioni più significative rientrano, oltre all'adescamento online di minori, anche la diffusione non autorizzata di immagini intime e il riciclaggio dei proventi derivanti da reati informatici, segnando un chiaro allargamento del perimetro di tutela penale.

Di particolare interesse risulta la disciplina contenuta nell'articolo 15 della Convenzione ONU che, rispetto all'articolo 9 della Convenzione di Budapest – incentrato esclusivamente sulla detenzione e diffusione di materiale pedopornografico – amplia la sfera incriminatrice sino a ricomprendere condotte preparatorie all'abuso sessuale, come la sollecitazione, il grooming e l'organizzazione di incontri a fini illeciti. Tale scelta normativa segna un passaggio rilevante, poiché evidenzia la volontà di anticipare la soglia di tutela, colpendo anche quei comportamenti che, pur non generando nell'immediato un danno concreto, costituiscono il presupposto logico e funzionale della successiva attività criminale[89].

---

[87] Cfr. PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Diritto dell'internet*, 2, 2005, p. 197.

[88] Sull'analisi comparata delle due Convenzioni cfr. KAZAKOVA A., TELEANU S., KOVAC B., HAMZA F., *Comparative analysis: The Budapest Convention vs the UN Convention Against Cybercrime*, in *Digital Watch Observatory*, 2024; TROPINA T., "*This is not a human rights convention!": The perils of overlooking human rights in the UN cybercrime treaty*, in *Journal of Cyber Policy*, 9, 2, 2024; si consulti anche ICT Security Magazine redazione, "*La nuova Convenzione ONU contro il Cybercrime: un passo storico nella lotta alla criminalità informatica*", 20 maggio 2025.

[89] Per una analisi della struttura e dei capitoli che compongono la Convenzione cfr. anche UNODC website, "Chapters of the Convention".

Parallelamente, l'esclusione delle violazioni in materia di proprietà intellettuale e diritto d'autore – espressamente previste, invece, nella Convenzione di Budapest – mette in luce una differente scala di priorità nella protezione dei beni giuridici.

L'approccio seguito in sede ONU sembra infatti orientato a selezionare un insieme più essenziale e condivisibile di fattispecie penalmente rilevanti, rinunciando, almeno in questa fase, a includere reati che avrebbero potuto ostacolare il raggiungimento di un consenso multilaterale ampio e stabile.

4.2. I crimini cyber dipendenti e i crimini facilitati dal cyber

Come si anticipava, per comprendere a pieno il ruolo della tecnologia nelle dinamiche criminali contemporanee, è opportuno chiarire sin d'ora un'ulteriore importante distinzione tra crimini "cyber dipendenti" (*cyber dependent crimes*) e crimini "facilitati dal cyber" (*cyber facilitated crimes or cyber enabled crimes*). Nonostante entrambi i tipi di reato coinvolgano l'uso di tecnologie informatiche, la loro connessione con la tecnologia è sostanzialmente diversa.

Secondo la definizione della National Cybersecurity Strategy, i crimini "cyber dipendenti" sono crimini che possono essere commessi solo tramite l'uso di dispositivi di tecnologie dell'informazione e della comunicazione (ICT), in cui i dispositivi sono sia lo strumento per commettere il crimine, sia il bersaglio del crimine stesso (ad esempio, sviluppare e diffondere malware per scopi finanziari, hacking per furti, danneggiamenti, alterazioni o distruzione di dati e/o reti o attività)[90].

Pertanto, come ci suggerisce la stessa definizione, esistono fintantoché esiste la tecnologia, non potendo essere commessi senza l'uso di computer, reti informatiche o altre tecnologie di comunicazione. Ne sono esempi attacchi come il *ransomware*, dove il crimine è interamente dipendente dall'uso di software dannoso che può infettare dispositivi informatici, o il *phishing*, in cui i criminali utilizzano internet per ingannare le vittime e ottenere dati sensibili. In questi crimini, la tecnologia è parte intrinseca, elemento costitutivo del crimine tanto che, se viene meno, viene meno anche il reato[91].

---

[90] Cfr. Parlamento europeo, *Understanding cybercrime*, in *European Parliament Research Service*, 2024; CROSS S., HIRRLE S., LIM M.A., *Cybercrime Strategy Guidebook,* Interpol, 2021.

[91] Cfr. KRANENBARG M., *Cyber-Dependent Crime Versus Traditional Crime*, in *Kranenbarg, and Leukfeldt, Cybercrime in context: The human factor in victimization, offending, and policing, Crime and*

I tipi di criminali coinvolti nei crimini cyber dipendenti vanno da gruppi criminali strutturati ad autori solitari[92]. Persino potenziali trasgressori, senza alcuna competenza specifica in materia informatica, possono commettere attacchi informatici facendo affidamento su strumenti e servizi disponibili tramite un modello di business illecito, previamente anticipato in questo capitolo, e denominato "*crime-as-a-service*".

Il "*crime-as-a-service*" consente ai criminali di acquistare e vendere servizi e strumenti legati alla criminalità, senza la necessità di avere competenze tecniche avanzate, fornendo quindi un facile accesso agli strumenti e ai servizi della criminalità informatica a piccoli e grandi attori criminali, o a qualsiasi altra parte anche non mossa da scopi illeciti. I servizi e gli strumenti utilizzati per commettere crimini informatici, come *malware*, *ransomware*, attacchi *DDoS*, e le istruzioni per realizzare diversi tipi di attacchi, vengono venduti online, frequentemente nel *dark web*.

Una sua declinazione specifica è rappresentata dal *ransomware-as-a-service*, sistema che permette agli sviluppatori di ransomware e ai criminali che ne fanno uso di condividere i profitti derivanti dalle attività illecite. Segnatamente, gli sviluppatori mettono a disposizione competenze tecniche e supporto come fornitori di servizi, mentre gli affiliati, spesso principianti nel crimine informatico, si occupano di individuare e infettare obiettivi vulnerabili[93]. Questo modello ha conseguentemente abbassato la barriera all'ingresso nel mondo del crimine informatico, permettendo anche a chi non ha competenze tecniche di diventare un criminale informatico.

Lo sviluppo e la distribuzione di *malware* continuano a essere la pietra angolare della criminalità informatica: si tratta di un programma informatico che utilizza codice dannoso per danneggiare, infiltrarsi, rubare dati o compromettere il funzionamento di computer, dispositivi o reti. Gli attacchi di *malware* mirano infatti a rubare dati e commettere furto d'identità, causare interruzioni dei servizi e supportare attività di spionaggio[94].

Una delle sue varianti più insidiose è il *ransomware*, in grado di paralizzare completamente l'accesso a componenti principali della rete o crittografare i dati presenti

---

Justice in Digital Society, 1, 2021, pp. 195-216; MCGUIRE M., DOWLING S., *Cybercrime: A Review of the Evidence: Summary of Kedy Findings and Implications*, Home Office, London, UK, 2013.

[92] In proposito, v. MAIMON D., LOUDERBCK E.R., *Cyber-Dependent Crimes: An Interdisciplinary Review*, in *Annual Review of Criminology*, 2019; Cfr. MARTINU, O., MCEWEN, G., *Crime in the age of technology*, in E*uropean law enforcement research Bulletin*, cit., p. 4.

[93] *Ibidem*; Europol, *Cyber-Attacks: The Apex Of Crime-As-A-Service*, IOCTA 2023.

[94] In proposito v. MCGUIRE M., DOWLING S., *Cybercrime: A Review of the Evidence: Summary of Kedy Findings and Implications*, cit., pp.1–35; Europol, *Cyber-Attacks: The Apex Of Crime-As-A-Service*, cit.

su un device rendendoli inaccessibili all'utente. Dopo aver effettuato la cifratura, viene chiesto alla vittima il pagamento di un riscatto per ottenere il ripristino di quei dati criptati che, in caso di rifiuto, l'utente non avrà più possibilità di recuperare[95].

Altrettanto diffusi sono gli attacchi DDoS (acronimo di *Distributed Denial of Service*, ovvero "interruzione distribuita del servizio"), che rappresentano una minaccia informatica significativamente diversa rispetto ai *ransomware*. Questi attacchi consistono nell'invio massivo di richieste di accesso false verso sistemi informatici, data center o reti di distribuzione, con l'obiettivo di sovraccaricarli; quando poi il sistema bersaglio non è in grado di gestire l'enorme quantità di richieste, subisce un blocco parziale o totale e, esaurendo la larghezza di banda disponibile, impedisce a chiunque cerchi di accedere al sistema di farlo, con conseguente "negazione dell'accesso" per gli utenti legittimi[96].

Al contrario dei crimini "cyber-dipendenti", nei crimini "facilitati dal cyber" la tecnologia non è parte intrinseca del crimine, ma ne è strumento agevolatore, in grado di facilitarne ed ampliarne su scala maggiore la commissione. La National Cybersecurity Strategy li definisce: "crimini tradizionali che possono essere ampliati in scala o portata mediante l'uso di computer, reti informatiche o altre forme di ICT"[97]. Si tratta, pertanto, di crimini, come il furto d'identità, la frode o il traffico di sostanze stupefacenti, preesistenti allo sviluppo della tecnologia, che potrebbero teoricamente essere commessi anche senza l'ausilio della tecnologia, ma che da quest'ultima sono certamente potenziati.

I crimini *cyber-enabled* riflettono la metamorfosi dei reati convenzionali attraverso l'integrazione tecnologica[98], e sono dunque il risultato dell'integrazione di crimini tradizionali e tecnologia[99]. A differenza della categoria di crimini di cui si è appena trattato, che si basa esclusivamente sulle ICT, questa seconda categoria racchiude crimini

[95] *Ibidem*.
[96] *Ibidem*; in proposito v. anche MAIMON D., LOUDERBCK E.R., *Cyber-Dependent Crimes: An Interdisciplinary Review*, cit.
[97] Cfr. Parlamento europeo, *Understanding cybercrime*, in *European Parliament Research Service*, 2024; CROSS S., HIRRLE S., LIM M.A., *Cybercrime Strategy Guidebook,* Interpol, 2021; FURNELL S., EMM D., PAPADAKI M., *The challenge of measuring cyber- dependent crimes*, in *Computer fraud and Security*, 2015.
[98] Cfr. MCGUIRE M., DOWLING S., *Cybercrime: A Review of the Evidence: Summary of Kedy Findings and Implications*, cit.; Parlamento europeo, *Understanding cybercrim*e, cit.
[99] Cfr. WALL, D. S., *Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'*, in Jewkes, Y. and Yar, M. (Ed.s) *Handbook of Internet Crime*, 2010, pp. 88-103.

che possono essere commessi anche senza l'uso della tecnologia, ma che quest'ultima ha trasformato in termini di scala e forma [100].

Come anticipato, le organizzazioni criminali ricorrono sempre più ad Internet per facilitare le loro attività e massimizzare i loro profitti nel minor tempo possibile. L'uso crescente della tecnologia per facilitare crimini come furto, frode e persino crimini di tipo terroristico aggiunge una nuova dimensione, che potremmo definire "digitale", a queste attività criminali tradizionali. Le forze dell'ordine riscontrano difficoltà nello svolgimento delle indagini sulla criminalità informatica, non avendo sempre accesso a informazioni in tempo reale sulle minacce che potrebbero avere un impatto grave sulla sicurezza dei cittadini e delle infrastrutture[101].

A titolo esemplificativo, è opportuno rinviare alla esaustiva elencazione dei *cyber enabled crimes* del United Kingdom Home Office[102]. In particolare, nell'ambito della criminalità informatica di tipo economico, si evidenziano indubbiamente la truffa, i crimini contro la proprietà intellettuale, pirateria, contraffazione e falsificazione, e la compravendita online di merce illegale; in secondo luogo, vengono individuati nell'ambito della categoria "*malicious and offensive communications*", tutti quei reati commessi attraverso la comunicazione digitale, come il cyberbullismo/trolling o il mobbing virtuale; da ultimo, rientrano, tra i *cyber-enabled crimes*, reati che colpiscono uno specifico target di individui, principalmente donne, come la divulgazione di immagini sessuali private senza consenso (anche "revenge porn"), il cyberstalking e le molestie, nonché, i reati sessuali contro i minori[103], la cui diffusione è sempre in maggiore crescita[104].

Inoltre, la distinzione tra *cyber-dependent crimes* e *cyber-enabled crimes* ha rappresentato uno dei principali nodi di discussione nel processo negoziale che ha condotto all'approvazione della già menzionata Convenzione ONU sul *cybercrime*.

Sin dalla sua formazione, il comitato *ad hoc* incaricato della stesura della Convenzione si è trovato ad agire in un contesto fortemente polarizzato, caratterizzato da tensioni

---

[100] Cfr. CROSS S., HIRRLE S., LIM M.A., *Cybercrime Strategy Guidebook,* Interpol, 2021, p. 10; LEVI M., ET AL.., *The Implications of Economic Cybercrime for Policing*", Cardiff University, 2015, http://orca.cf.ac.uk/88156/1/Economic-Cybercrime-FullReport.pdf.
[101] Cfr. Interpol, *Cybercrime*, in Future oriented policing projects, in www.interpol.int
[102] Cfr. Crown prosecution service, *Cybercrime - prosecution guidance*, in *Legal Guidance Cyber*, online crime, updated 15 Jul 2024.
[103] *Ibidem.*
[104] Cfr, Parlamento europeo, *Understanding cybercrime, by Colin Murphy*, 2024.

geopolitiche, contrasti sul piano normativo e concettuale, nonché da una marcata disomogeneità tra i sistemi giuridici di riferimento.

Per quanto riguarda le scelte di criminalizzazione, ad esempio, alcuni Stati promotori, come la Federazione Russa e la Repubblica Popolare Cinese, sostenevano un impianto regolativo più ampio e vincolante; in contrapposizione, i Paesi occidentali, in particolare gli Stati membri dell'Unione Europea e gli Stati Uniti, esprimevano significative riserve, temendo che una definizione troppo estesa delle condotte punibili potesse incidere negativamente sulle libertà fondamentali.

Dalle relazioni presentate dai vari Stati durante le prime sessioni negoziali[105] emergeva, infatti, una linea di frattura già evidente in merito all'ambito materiale, alla struttura e agli obiettivi della Convenzione. L'Unione Europea e i suoi membri, da un lato, propendevano per un approccio più limitato, centrato esclusivamente sugli "*high-tech crimes*" o "*cyber-dependent crimes*", ossia quei reati che non avrebbero ragione di esistere senza il ricorso alle tecnologie digitali[106]. La Cina, invece, spingeva per una visione più inclusiva, che comprendesse anche i "*cyber-enabled crimes*", vale a dire i reati tradizionali resi possibili o agevolati dalla tecnologia, come frodi, pornografia o terrorismo[107].

L'attuale secondo capitolo del testo definitivo della Convenzione ha ad oggetto proprio la "Criminalizzazione" e pone le basi per una "armonizzazione legale"[108], individuando con precisione una gamma articolata di reati che gli Stati hanno l'obbligo di introdurre nei propri ordinamenti penali. Si tratta, alla fine, di reati informatici, sia "*cyber-dependent*", ovvero dipendenti dalle tecnologie, sia "*cyber-enabled*", ovvero agevolati dalle stesse.

---

[105]Cfr. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

[106] Cfr. Ad Hoc Committee, Unione Europea, *Contribution from the European Union and its member states, Preparation for the first session of the United Nations Ad Hoc Committee to elaborate a Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, disponibile inhttps://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/EU_Position_for_AHC_first_session.pdf.

[107] Cfr. Ad Hoc Committee, Cina, *China's Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes*, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf

[108] Parole usate da Glen Prichard Capo della Sezione Cybercrime e Riciclaggio di Denaro dell'Ufficio delle Nazioni Unite contro la Droga e il Crimine (UNODC) durante l'intervento alla 13° Cybercrime Conference, cfr. "*La nuova Convenzione ONU contro il Cybercrime: un passo storico nella lotta alla criminalità informatica*", in ICT Security Magazine, 20 maggio 2025.

Rispetto a quest'ultima categoria, degna di nota è l'introduzione di nuove condotte, mai incluse prima in trattati internazionali, come la diffusione non consensuale di immagini intime o l'adescamento online di minori.

SEZIONE II

LA MIGRAZIONE DELLA CRIMINALITÀ ORGANIZZATA "TRADIZIONALE" NEL CYBERSPACE: STRUTTURA, FINALITÀ E SFIDE GIURIDICHE

CAPITOLO II

L'inquadramento dell'indagine

SOMMARIO: **1.** Premessa definitoria – 2**.** Definizione della struttura dell'indagine: i gruppi criminali oggetto della ricerca.

1. Premessa definitoria

Il presente capitolo si propone di esplorare in maniera sistematica le organizzazioni criminali che popolano il *cyberspace*.

L'analisi delle diverse tipologie di gruppi criminali trova il proprio fattore scriminante nella tecnologia, il cui differente ruolo influenza in modo sostanziale l'organizzazione criminale, tanto sul fronte strutturale, relativo all'architettura interna ed operativa del gruppo, quanto sul fronte teleologico, attinente alle attività e agli scopi criminali.

Prima di addentrarsi nell'analisi delle diverse organizzazioni, risulta fondamentale una premessa definitoria circa l'oggetto di questa indagine: il crimine organizzato.

La definizione di crimine organizzato, infatti, non solo stabilisce i confini teorici di questa ricerca, ma offre altresì gli strumenti concettuali necessari per inquadrare le manifestazioni moderne di criminalità, comprese quelle che operano nel cyberspazio.

Secondo la ricostruzione sistematica di Von Lampe[109], il concetto di crimine organizzato è ampiamente dibattuto e definito in diversi settori e da parte di diverse categorie di soggetti: studiosi, forze dell'ordine, giornalisti e politici.

---

[109] Cfr. VON LAMPE K., *A Systematic Overview of Definitions of Organized Crime*, in *Organized Crime: Analyzing illegal activities, criminal structures, and extra-legal governance*, Sage Publications, 2016, pp. 27-30.

Lo studioso evidenzia tre principali visioni della natura del crimine organizzato: una che si concentra sull'attività criminale, una sulla struttura delle organizzazioni criminali e una sulla governance illegale.

Mentre nel primo caso, il crimine organizzato è visto come un tipo di attività criminale sofisticata, continua e razionale, nel secondo, si sottolinea l'importanza delle organizzazioni criminali, come gruppi che si dotano di specifiche strutture formali; infine, nel terzo caso, il crimine organizzato è legato al potere illegittimo che i criminali esercitano nella società, sia attraverso il controllo del crimine che attraverso l'influenza sulla politica[110].

Altrettante divergenze definitorie emergono in relazione alle caratteristiche delle organizzazioni criminali, come la dimensione e la struttura. Alcune definizioni non richiedono criteri strutturali specifici, mentre altre enfatizzano organizzazioni formali e gerarchiche. Inoltre, si ravvisano opinioni discordanti circa l'importanza della violenza e della corruzione come tratti distintivi del crimine organizzato, nonché sugli scopi delle organizzazioni criminali, in base ai quali alcune definizioni pongono l'accento sul guadagno materiale, escludendo gli obiettivi politici, mentre altre individuano nel potere politico proprio lo scopo criminale[111].

Ad ogni modo, evidenzia Lampe, la mancanza di un consenso definitorio riflette la complessità della realtà sociale e politica. È infatti innegabile che le definizioni sul crimine organizzato siano influenzate da considerazioni pratiche e politiche, come la protezione delle élite sociali e la gestione di crimini di natura politica, oltre che dalla percezione collettiva del fenomeno; tutti fattori, questi ultimi, che indubbiamente contribuiscono a rendere il concetto di crimine organizzato relativo e contestabile[112].

La stessa Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale[113] non fornisce una definizione di crimine organizzato.

---

[110] *Ibidem.*
[111] *Ibidem.*
[112] *Ibidem*.
[113] La Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale è stata adottata il 15 novembre 2000 a Palermo durante la Sessantacinquesima sessione dell'Assemblea generale delle Nazioni Unite. È stata ratificata da oltre 190 Stati membri delle Nazioni Unite. Al centro della Convenzione viene posta la lotta alla criminalità organizzata di carattere transnazionale, con particolare attenzione a fenomeni illeciti quali il traffico di esseri umani, la tratta di migranti, il traffico di stupefacenti, il riciclaggio di denaro, la corruzione e altre forme di crimine organizzato internazionale. Obiettivo della Convenzione è rafforzare la cooperazione internazionale tra gli Stati membri, promuovendo un approccio condiviso e integrato nella prevenzione, nella repressione e nella penalizzazione di tali crimini, istituendo un quadro giuridico che favorisce il coordinamento tra le autorità di polizia, i sistemi giuridici e le agenzie governative.

Tuttavia, la mancanza di una definizione unitaria e universale non deriva solo dall'assenza di un accordo tra gli Stati membri, ma pare, piuttosto, una scelta consapevole dei negoziatori della Convenzione. L'elaborazione di una specifica definizione avrebbe presupposto, infatti, uno specifico riferimento alle attività illecite svolte dai gruppi criminali organizzati e avrebbe rischiato, considerata la loro capacità di rapido adattamento alle trasformazioni sociali, di divenire obsoleta in breve tempo[114].

Piuttosto che il crimine, la Convenzione definisce, invece, l'attore coinvolto nella sua commissione: in particolare, un "gruppo criminale organizzato", ai sensi dell'articolo 2(a) della Convenzione, è un "*un gruppo strutturato di tre o più persone, esistente per un periodo di tempo e che agisce di concerto con l'intento di commettere uno o più crimini gravi o reati stabiliti in conformità con questa Convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o altro beneficio materiale*".

Si tratta, senza dubbio, di una definizione ampia, adattabile a gruppi criminali eterogenei, persino a gruppi poco affiliati senza ruoli formalmente definiti per i propri membri o con strutture particolarmente sviluppate[115].

Analogamente, quando si parla di crimine organizzato informatico si intende fare generico riferimento alle attività del crimine organizzato nel cyberspazio.

Ne deriva, pertanto, che l'inquadramento di certi crimini di tipo informatico nel crimine organizzato o l'identificazione di un legame tra gli stessi ed il crimine organizzato dipende dalle definizioni operative del "crimine organizzato" stesso.

Non vi è, difatti, tuttora unanime consenso sulla definizione di crimine organizzato informatico[116], giacché, inevitabilmente, le stime sulla proporzione di crimini informatici riconducibili al crimine organizzato sono strettamente condizionate dalle definizioni di

---

[114] Cfr. United Nations Office on Drugs and Crime, *Conceptualizing organized crime and defining the actors involved*, in E4J mod. 13 "*Cyber organized crime*", 2019; CARNEVALE S., FORLATI S., GIOLO O., *The Notion of Organised Crime: Why Definitions Matter*, in *Redefining Organised Crime: A Challenge for the European Union?*, Oxford, Hart Publishing, 2017.

[115] Sull'ampiezza della definizione della Convenzione di Palermo, vedi MICHELINI G., *La Convenzione Di Palermo/2. Il ruolo dell'italia nella redazione del testo finale*, in *Cross*, 5, 2, 2019, p. 24; United Nation Office on Drug and Crime, *Definition in the Organized Crime Convention,* mod. 1, https://sherloc.unodc.org/cld/en/education/tertiary/organized-crime/module-1/key-issues/definition-in-convention.html; LAVORGNA A., SERGI A., *Types of organised crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies*, in *International Journal of law, crime and Justice*, 2014, 42, pp. 16-32.

[116] Cfr. United Nation Office on Drug and Crime, *Comprehensive Study on cybercrime*, Draft, 2013, p. 45; BROADHURST R., GRABOSKY P., ALAZAB M., CHON S., *Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime*, in *International Journal of Cyber Criminology*, 2014, 8, 1, pp. 1-20; MARAS M., *Cybercriminology*, Oxford University Press, 2016.

"crimine informatico" e "crimine organizzato" adottate dai singoli Stati[117], nonché, come si dirà più approfonditamente in apposita sezione dedicata al tema (v. sez. III), dalla complessità di adattare alcune delle caratteristiche tradizionali del crimine organizzato al cyberspazio.

Si pensi, ad esempio, a tipiche caratteristiche del crimine organizzato, quali l'uso della violenza o il controllo sul territorio, che si rivelano difficili da applicare al contesto del crimine informatico. Inoltre, aspetti legati alla gestione e al coordinamento delle organizzazioni criminali, come la fiducia reciproca e l'implementazione di regole condivise, possono incontrare notevoli difficoltà in ambienti virtuali, come forum online o chat room, dove la struttura e la dinamica interpersonale sono radicalmente diverse rispetto ai contesti fisici[118].

Pertanto, nel prosieguo, si spiegheranno le ragioni per cui, in alcuni casi, risulti particolarmente complesso inquadrare il crimine informatico all'interno di tale definizione tradizionale, data la natura fluida e in continua evoluzione delle attività criminali legate alle tecnologie. Inoltre, in sede di inquadramento giuridico-normativo dei gruppi organizzati di tipo informatico (v. sez. III, cap. VI), sarà altresì esaminato come la giurisprudenza, pur in presenza di queste difficoltà, sia riuscita a individuare le caratteristiche distintive di tale fenomeno e a proporre un inquadramento normativo adeguato, consentendo così di affrontare efficacemente le nuove sfide poste dal crimine organizzato di tipo informatico.

2. Definizione della struttura dell'indagine: i gruppi criminali oggetto della ricerca

Prima di esplorare la classificazione delle varie organizzazioni criminali, è bene chiarire come le diverse forme di criminalità siano influenzate dal ruolo della tecnologia e dalle diverse modalità di interazione tra le dimensioni online e offline.

[117] Cfr. United Nation Office on Drug and Crime, *Comprehensive Study on cybercrime*, cit., p. 45.
[118] *Ibidem*; BAE Systems Detica and London Metropolitan University, *Organised Crime in the Digital Age*, *Norton Cybercrime Report 2011,* 2012.

Secondo questa prospettiva, risulta esplicativa la "teoria dello spettro della criminalità digitale" elaborata da Di Nicola, il quale propone un approccio elastico ed ampio per leggere l'eterogeneità del fenomeno della criminalità che si rapporta al mondo digitale[119].

In particolare, secondo questa teoria, i crimini moderni possono essere visti come un insieme di comportamenti che si trovano su uno spettro che unisce comportamenti online e offline. Da un lato, ci sono crimini completamente digitali, che avvengono nel mondo virtuale e che non esisterebbero senza l'uso delle tecnologie digitali. Dall'altro lato, ci sono crimini puramente fisici, che non hanno nulla a che fare con il mondo digitale. Le interazioni tra esseri umani e macchine e l'impiego di strumenti digitali variano in base a dove si trovano su questo spettro; gli stessi concetti di spazio e tempo cambiano a seconda di dove si colloca il crimine lungo questo *continuum*: vale a dire, più il crimine è virtuale, meno lo spazio ha significato, e più il tempo può diventare veloce e condensato[120].

Tra i due estremi ci sono diverse modalità di adattamento, ovvero vari modi in cui i gruppi criminali organizzati usano il digitale nelle loro attività. In questo contesto, quando parliamo di crimini organizzati digitali, dunque, non intendiamo solo i crimini informatici, ma più in generale tutti i crimini organizzati che si sviluppano nella società digitale, in base a questa continua evoluzione[121].

La metodologia che verrà adottata in questo lavoro per analizzare ed esaminare le diverse organizzazioni criminali si baserà, dunque, su un approccio alla materia elastico e flessibile, che sia in grado di tener conto dell'eterogeneità del fenomeno della criminalità organizzata nel contesto digitale, in relazione al ruolo variabile della tecnologia e all'interazione tra le dimensioni online e offline.

In proposito, da vari studi accademici[122] e report di organizzazioni internazionali, come le Nazioni Unite (UNODC)[123], sono state individuate tre tipologie generali di gruppi criminali che si servono della tecnologia in modi diversi.

---

[119] Cfr. DI NICOLA A., *Towards digital organized crime and digital sociology of organized crim*e, cit.
[120] *Ibidem*.
[121] *Ivi*, p. 13.
[122] Cfr. HUTCHINGS A., *Crime from the keyboard: organized cybercrime, co-offending, initiation and knowledge transmission*, in *Crime, Law and Social Change*, 62, 1, 2014, pp. 1–20; BROADHURST R., GRABOSKY P., ALAZAB M., CHON S., *Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime*, cit., pp.1-20; OLSON P., *We Are Anonymous: Inside the Hacker World of LulzSec*, in *Anonymous, and the Global Cyber Insurgency*, London: Little, Brown, 2012.
[123] Cfr. United Nation Office on Drug and Crime, *Comprehensive Study on cybercrime*, cit., p. 46; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, II ed., 2022.

Si vuole, per la trattazione che qui rileva, far riferimento alla distinzione operata dalle istituzioni internazionali sulla base dei dati disponibili riguardo ai legami tra il crimine organizzato e crimine informatico, ai gradi di coinvolgimento dei gruppi in attività online (rispetto a quelle offline) e alla struttura delle associazioni all'interno del gruppo.

In particolare, sono stati identificati tre tipi generali di gruppi: gruppi che operano principalmente online e commettono crimini informatici (tipo I); quelli che operano sia offline che online e si impegnano in crimini offline e informatici (tipo II); e quelli che utilizzano solo le tecnologie dell'informazione e della comunicazione per facilitare crimini offline (tipo III).

Quest'ultima tripartizione si ramifica ulteriormente, come evidenziato dal report di McGuire "*Organised crime in the digital age*"[124].

Infatti, i gruppi di tipo I, che operano principalmente online, possono essere ulteriormente suddivisi in "*swarms*", ossia gruppi più elastici e meno strutturati che operano principalmente online senza una leadership definita, e "*hubs*", ovvero gruppi operanti sempre online, ma con una catena di comando più strutturata.

Al contempo, anche i gruppi di tipo II, operativi sia online che offline, possono essere ulteriormente separati in "*clustered hybrids*", nonché gruppi di dimensioni ridotte, dalla struttura simile agli "*hubs*" che si focalizzano su attività specifiche, sia offline che online (es. carding forums e skimmers), e, dall'altra parte, in "*extended hybrids*", che pur operando sempre tra il mondo fisico e quello digitale, presentano una struttura più decentralizzata con componenti impegnati in attività criminali più disparate, come le frodi o il trading online.

Infine, i gruppi di tipo III, operativi solo offline, che possono costituire delle "*hierarchies*", ossia gruppi criminali organizzati tradizionali che facilitano le loro attività offline tramite l'uso delle tecnologie dell'informazione e della comunicazione (es. la criminalità mafiosa che si serve del gioco d'azzardo online per facilitare le proprie attività di riciclaggio), e degli "*aggregates"*, gruppi di natura transitoria, meno organizzati, che utilizzano le tecnologie per motivi limitati per facilitare le loro attività offline.

Tralasciando al momento i gruppi ibridi, a cui verrà riservata una trattazione separata, la ricerca si concentrerà, principalmente, sui modelli n. 1 e n. 3 che, per facilità espositiva,

---

[124] Cfr. BAE Systems Detica and London Metropolitan University, *Organised Crime in the Digital Age*, *Norton Cybercrime Report 2011,* 2012.

definiremo, rispettivamente, "*cyber-organised crime*" e gruppi criminali organizzati *"tradizionali*".

CAPITOLO III

La criminalità organizzata "tradizionale" dal mondo fisico al *cyberspace*

SOMMARIO **1.** Le organizzazioni criminali "tradizionali" che migrano nel *cyberspac*e – **2** Il ruolo della tecnologia e la sua influenza sulla struttura dei gruppi criminali "tradizionali" – **3.** Il ruolo della tecnologia nelle attività criminali del crimine organizzato "tradizionale" – **3.1.** La tecnologia nelle attività di narcotraffico – **3.2.** La tecnologia nelle attività di riciclaggio – **3.2.1.** Il supporto dei "*professional enablers*" alle attività di riciclaggio – **3.2.2.** Dal riciclaggio tradizionale al *cyber-laundering* – **3.2.2.1.** Recenti casi di *cyber-laundering* tra le organizzazioni criminali – **3.2.2.2.** Metodi di *cyber-laundering*: il riciclaggio tramite aste online e piattaforme d'azzardo online – **3.2.2.3.** Il riciclaggio tramite *money mules*.

1. Le organizzazioni criminali "tradizionali" che migrano nel *cyberspace*

La prima parte dell'analisi delle organizzazioni criminali operanti nel *cyberspace* sarà dedicata all'esame di quei gruppi, tradizionalmente attivi offline, che hanno scelto di trasferire una parte significativa delle proprie attività nello spazio digitale.

Tali entità, pur mantenendo radici consolidate in contesti fisici, si avvalgono delle potenzialità offerte dal *cyberspace* per ampliare la propria influenza e le proprie modalità operative.

Al fine di distinguere queste organizzazioni dalle altre che verranno trattate nel prosieguo dell'analisi, esse verranno designate come "tradizionali" o "convenzionali", poiché continuano a preservare strutture e pratiche consolidate, originariamente sviluppate in contesti non digitalizzati.

La comprensione delle modalità operative di questi gruppi criminali organizzati nell'era digitale deve dunque tener conto di un aspetto fondamentale: sebbene si parli spesso di un "crimine senza confini", vi sono prove sempre più concrete che questo tipo di criminalità mantenga una dimensione locale ben definita, radicandosi nel contesto offline e mantenendo forti legami con le strutture tradizionali. Tuttavia, sebbene le analisi disponibili suggeriscano che le attività dei criminali coinvolti in questo tipo di criminalità dipendano in maniera significativa dalle risorse e dalle dinamiche del mondo offline,

l'espansione di Internet ha senza dubbio creato nuove opportunità per queste organizzazioni criminali, abbattendo l'ostacolo dei confini fisici e giuridici per lo sviluppo delle loro iniziative criminali[125].

Pertanto, è indubbio che esistano ancora organizzazioni criminali monolitiche, gerarchiche e formalmente strutturate, ma la loro configurazione sta subendo un processo di crescente diversificazione. Allo stesso modo, anche le attività in cui tali organizzazioni sono coinvolte si stanno moltiplicando e ramificando[126].

Prima di intraprendere un'analisi approfondita delle modifiche strutturali, delle attività e degli strumenti maggiormente utilizzati da queste organizzazioni criminali nel *cyberspace*, è fondamentale partire dal ruolo che riveste la tecnologia: la comprensione di come le tecnologie digitali abbiano trasformato il panorama criminale è, infatti, la premessa necessaria per esplorare i cambiamenti nelle dinamiche operative e nelle risorse impiegate da tali gruppi.

2. Il ruolo della tecnologia e la sua influenza sulla struttura dei gruppi criminali "tradizionali"

La tecnologia, pur giocando un ruolo fondamentale, non è intrinsecamente parte della criminalità, ma costituisce semplicemente un facilitatore del crimine. Vale a dire che non è la tecnologia in sé a determinare la natura criminale delle attività, quanto piuttosto il modo in cui viene utilizzata per amplificare, velocizzare e rendere più sofisticate le azioni illecite. In questo senso, essa diventa uno strumento che permette ai gruppi criminali di operare in modo più efficiente e in contesti più ampi, pur non essendo parte protagonista di questo tipo di criminalità[127].

Se in passato la commissione di crimini complessi richiedeva l'esistenza di un'organizzazione criminale strutturata, in cui il coordinamento e la divisione del lavoro erano essenziali per garantire il successo delle operazioni illecite, con l'avanzamento delle

---

[125] Cfr KRUISBERGEN E.W., LEUKFELDT E.R., KLEEMANS E.R., ROKS R., *Money talks money laundering choices of organized crime offenders in a digital age,* cit., p. 574.
[126] Cfr. GRABOSKY P., *The Internet, Technology and Organised crime*, in *Asian criminology*, 2, 2007, pp. 146-161; WANG P., SU M., WANG J.*, Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer- to-peer lending market in China,* in *Brit. Journal Criminology*, 61, 2021, pp. 303-324.
[127] Cfr. LAVORGNA A., *Organised crime goes online: realities and challenges,* in *Journal of Money Laundering Control,* 18, 2, 2015, pp. 153-168.

tecnologie dell'informazione e della comunicazione, molti dei tradizionali strati organizzativi delle reti criminali risultano più superflui[128].

Questo porta a un paradosso: più i criminali acquisiscono competenze tecnologiche, più l'originaria strutturazione organizzativa ed operativa della criminalità organizzata tradizionale appare superflua, evolvendo verso una forma più fluida e decentralizzata.

La struttura gerarchica e stabile che caratterizzava le organizzazioni criminali convenzionali cede quindi il passo ad una criminalità più dinamica, dispersa e adattabile, in cui i confini tra i membri e le funzioni sono sempre più sfumati. In questo modo, la tecnologia non solo facilita l'operato criminale, ma provoca una trasformazione profonda nella stessa natura della criminalità organizzata[129].

Tramite la tecnologia, infatti, la criminalità si trasforma, divenendo sempre più fluida e iperconnessa. "Fluida" poiché la criminalità organizzata, tradizionalmente caratterizzata da gruppi stabili e strutturati, si fa ora più dispersa e dinamica grazie alle potenzialità offerte dalle tecnologie digitali, lasciando spazio alla nascita di nuove formazioni meno rigidamente definite. "Iperconnessa" fa riferimento, invece, alla capacità di questi gruppi di unirsi temporaneamente per commettere crimini, trarne profitto, disperdersi rapidamente e riconfigurarsi in nuove alleanze, creando una rete criminale che si adatta ed evolve in continuazione, in funzione delle specifiche "specializzazioni" richieste da ogni singolo crimine. In questo contesto, la criminalità diventa non solo più pervasiva, ma anche più pericolosa, grazie alla sua capacità di operare in modo rapido e capillare[130].

D'altro canto, si intende definire la tecnologia come un mero "facilitatore del crimine", poiché non elimina il radicamento che queste organizzazioni hanno nelle dinamiche sociali e territoriali che caratterizzano il mondo fisico.

Si pensi al bisogno di un fondamento solido di legami offline.

Infatti, nonostante il trasferimento delle operazioni nel *cyberspace*, la criminalità organizzata tradizionale conserva ancora una forte connessione con il mondo offline, e i contatti sociali fuori dalla rete continuano a svolgere un ruolo fondamentale per la stabilità

---

[128] Cfr. LAVORGNA A., *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?, 2016,* in *Narratives on organised crime in Europe. Criminals, corrupters and policy*, a cura di Van Duyne P., Scheinost M., Antonopoulos G. A., Harvey J., Von Lampe K, The Hague, Wolf Legal Publisher, 2016, p. 209.

[129] Sul punto si veda KOOPS B., *The Internet and its Opportunities for Cybercrime,* cit.; WALL D., *Cybercrime. The Transformation of Crime in the Information Age,* Cambridge Polity press, 2007.

[130] Cfr. DEMETIS D., *Organised crime The Cyber dimension*, in *A research agenda for organized crime*, cit.

di queste reti criminali. Questi legami garantiscono una forma di sicurezza sociale, che permette ai membri di operare con maggiore fiducia e di superare le potenziali insidie e incertezze date dall'interazione con ambienti digitali. In molti casi, i membri di queste reti criminali si conoscono già attraverso legami sociali, familiari o professionali consolidati nel contesto offline. Questi legami, che si radicano in background locali o in esperienze comuni, costituiscono, dunque, una base solida di fiducia e cooperazione che facilita l'ingresso di nuovi membri nelle organizzazioni criminali, anche quando queste si adattano al contesto digitale[131].

Quanto alla struttura, le reti criminali tradizionali tendono a presentare e preservare le caratteristiche tipiche delle reti *small-world* e *scale-free*.

In particolare, a livello interno, si parla di reti *small-world* con riferimento a quelle reti criminali strutturate in modo tale che, nonostante la loro complessità e dimensione, i membri siano generalmente ben connessi tra loro con poche "distanze" tra i vari nodi. Questo rende la rete particolarmente coesa, in quanto i membri possono facilmente raggiungersi tra loro attraverso pochi passaggi, garantendo così una comunicazione e un coordinamento più efficaci.

D'altro canto, sul fronte esterno, le reti *scale-free* sono caratterizzate dalla presenza di alcuni nodi con un numero molto elevato di connessioni, contrariamente dalla maggior parte dei membri che compongono la rete, i quali, invece, non dispongono dei medesimi legami[132].

Nella criminalità organizzata, ad esempio, figure centrali come i leader possiedono molteplici contatti e un elevato potere di influenza, mentre altri membri della rete possono avere un ruolo più marginale. Questa struttura conferisce alla rete criminale una certa resilienza, poiché, non dipendendo da singoli componenti, rimane relativamente resistente alla rimozione casuale di membri, come nel caso di arresti o perdite non pianificate. Tuttavia, la vulnerabilità della rete emerge quando vengono mirati membri

---

[131] Cfr. KRUISBERGEN E.W., LEUKFELDT E.R., KLEEMANS E.R., ROKS R., *Money talks money laundering choices of organized crime offenders in a digital age,* cit., p. 577*;* LEUKFELDT, E. R., KLEEMANS E.R., STOL W.P., *Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks*, in *British Journal of Criminology*, 57, 3, 2017, pp. 16 ss.; LEUKFELDT, E. R., LAVORGNA A., KLEEMANS E. R., *Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, in *European Journal on Criminal Policy and Research*, , 23, 3, 2017, pp. 292 ss.

[132] Sul punto v. KALM K., *Illicit Network Structures in Cyberspace*, *5th International Conference on Cyber Conflict*, 2013, p. 10.

chiave: l'eliminazione o l'arresto di un elemento centrale, come un leader o un collegamento cruciale, può indebolire gravemente la rete, compromettendo la sua stabilità e la capacità di operare efficacemente[133].

Si consideri, inoltre, il legame con il territorio.

Le organizzazioni criminali "tradizionali", in particolare quelle di tipo mafioso, sono strettamente connesse al territorio, e molte delle loro attività illecite, come l'estorsione, richiedono una presenza fisica, che costituisce una caratteristica distintiva. Questo accade perché il contesto sociale, economico e culturale in cui queste attività si radicano non sempre si presta facilmente all'utilizzo di Internet, e sembra che tale struttura continui a funzionare in modo sufficientemente efficace da non spingere queste organizzazioni a modificare il loro tradizionale legame con il territorio[134].

In generale, poi, la criminalità organizzata "tradizionale" si contraddistingue per l'uso della violenza, che serve a tutelare il proprio monopolio su territori e risorse illegali. La violenza, dunque, non è una misura difensiva, ma un mezzo per consolidare il controllo[135].

Infine, occorre considerare che, pur potendo diventare più fluida e dinamica grazie all'uso di strumenti tecnologici, la criminalità organizzata tradizionale continua a preservare una struttura formale e gerarchicamente organizzata. Si caratterizza per una serie di regole interne che disciplinano tanto le dinamiche sociali del gruppo quanto la gerarchia delle posizioni al suo interno, garantendo ordine, coesione e rispetto delle funzioni attribuite a ciascun membro[136].

È bene precisare, poi, che la distribuzione del potere nelle reti criminali tradizionali e il loro adattamento alla tecnologia può variare anche in base alla loro struttura storica. Vale a dire, che se, a titolo esemplificativo, un gruppo segue una gerarchia rigida e centralizzata, la distribuzione del potere sarà più stabile e meno libera. Al contrario, se la

---

[133] *Ibidem*.

[134] Cfr. LAVORGNA A., SERGI A., *Types of organised crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies*, cit., pp. 16-32.

[135] In proposito, cfr. TROPINA T., *The Evolving Structure of Online Criminality*, in *eucrim*, 4, 2012, p. 158; LEUKFELDT, E. R., LAVORGNA A., KLEEMANS E. R., *Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., pp. 292 ss.*;* con riferimento al rapporto tra violenza e il c.d. "loan sharking", si veda WANG P., SU M., WANG J.*, Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer- to-peer lending market in China,* in *Brit. Journal Criminology*, 61, 2021, p. 303.

[136] Cfr. TROPINA T., *The Evolving Structure of Online Criminality*, cit., p. 158; PATALANO V., *L'associazione per delinquere*, Jovene, Napoli, 1971, p. 151.

rete è organizzata in modo più orizzontale, senza una gerarchia fissa, si noterà una distribuzione del potere più aperta, dove alcuni membri avranno più influenza[137].

3. Il ruolo della tecnologia nelle attività criminali del crimine organizzato "tradizionale"

Nonostante i gruppi criminali tradizionali mantengano caratteristiche storiche come la struttura gerarchica e l'uso della violenza, l'avanzamento tecnologico ha inevitabilmente influenzato il loro *modus operandi*. Sebbene continuino a concentrarsi su attività illecite consolidate, come il traffico di droga e l'estorsione, la tecnologia offre loro strumenti per operare in modo più efficiente.

Per analizzare come la tecnologia influenzi le attività dei gruppi criminali tradizionali, è utile fare riferimento al cosiddetto "test di trasformazione" di Wall[138].

Secondo Wall, l'aspetto distintivo del crimine informatico è la sua fusione con le tecnologie digitali e la rete. Se un crimine non scompare in assenza di queste tecnologie, allora non può essere considerato un vero crimine informatico. Applicando questo "test di trasformazione", dunque, si apre la possibilità che, oltre ai crimini informatici veri e propri, esistano anche una serie di crimini cosiddetti ibridi.

Rispetto alla scala di categorizzazione dei *cybercrimes* in base alla dipendenza dal fattore "tecnologia", già vista nel primo capitolo di questo lavoro di ricerca, Wall ritiene che all'opposto dei *cyber-dependent crimes,* di cui si è detto, vi sia un'ulteriore categoria di crimini, diversi dai *cyber-enabled crimes*: i "*cyber-assisted crimes*".

Questi ultimi, sebbene si servano di internet sul lato organizzativo, sono quei crimini che si verificherebbero comunque anche senza lo stesso. In questo contesto, pertanto, internet non è necessario per commettere il crimine in sé, ma rappresenta una semplice forma di "assistenza" che rende il crimine più efficiente, informato o meno rischioso, fornendo risorse e conoscenze che altrimenti potrebbero non essere facilmente accessibili.

---

[137] Cfr. KALM K., *Illicit Network Structures in Cyberspace*, *5th International Conference on Cyber Conflict*, cit., p. 6.

[138] Cfr. WALL, D.S., *Cybercrime: The transformation of crime in the information age*, cit.; WALL D.S., *Towards a conceptualisation of cloud (Cyber) crime*, in *Tryfonas, T, (ed.) Lecture Notes in Computer Science. International Conference on Human Aspects of Information Security, Privacy, and Trust,* 2017, pp. 529-538.

In termini essenziali, l'esempio di un assassino che cerca su internet "come uccidere qualcuno" o "come sbarazzarsi del corpo" è un caso di *cyber-assisted crime,* perché internet viene utilizzato come strumento per ottenere informazioni che potrebbero aiutare a commettere il crimine. In altre parole, l'omicidio rimane un crimine che potrebbe essere commesso anche senza l'uso di internet, ma l'assassino sfrutta la rete per raccogliere dettagli, suggerimenti o metodi che potrebbero facilitare l'esecuzione del reato.

All'estremo opposto, ci sono i "*cyber-dependent crimes*", di cui si è già ampiamente detto (v. cap. I, sez. I), che nascono direttamente dall'uso di internet, come gli attacchi DDoS, lo spam, la pirateria, ecc. Se internet venisse rimosso, questi crimini semplicemente cesserebbero di esistere.

Tra i crimini assistiti dal cyber e quelli dipendenti dal cyber, troviamo invece una categoria di crimini ibridi, anch'essi già menzionati nella fase introduttiva di questo lavoro (v. cap. I, sez. I), e definiti "abilitati dal cyber" o "*cyber-enabled crimes"*. Questi includono la maggior parte dei crimini aventi ad oggetto una condotta fraudolenta e ingannevole e sono crimini già previsti dalla legge che, grazie a internet, acquisiscono una portata globale. Se si rimuovesse internet, quindi, questi crimini continuerebbero a verificarsi, ma a livello molto più localizzato, perdendo così la dimensione globale, informativa e distribuita che invece li caratterizza nel contesto "*cyber*"[139].

Di conseguenza, con il termine "criminalità organizzata cyber-abilitata" ci si può riferire, ad esempio, a frodi informatiche, crimini legati all'identità digitale, come estorsioni online e *ransomware*, abuso e sfruttamento sessuale online; crimini che sono sempre più commessi da vari gruppi organizzati[140].

Invece, parleremo di organizzazioni criminali "*assistite dal cyber*" per riferirci a quei gruppi che utilizzano le tecnologie per facilitare operazioni criminali già esistenti o per trasferire parte delle loro attività tradizionali nel mondo online[141].

Spesso, tali gruppi criminali si impegnano in attività criminali complesse che, dal punto di vista della giustizia penale, si presentano come "catene" di crimini

---

[139] *Ibidem*.

[140] Sul punto v. UNODC, *Digest of cyber organized crime*, United Nations, Vienna, 2021; Europol, *Serious and Organised crime threat assessment, A Corrupting Influence: The Infiltration And Undermining Of Europe's Economy And Society By Organised Crime*, 2021, in *https://www.europol.europa.eu/publications-events/main-reports/socta-report*, pp. 22 ss.

[141] Sui *cyber-assisted crimes* v. WALL, D.S., *Towards a conceptualisation of cloud (Cyber) crime*, cit., pp. 529-538.

interdipendenti, il cui svolgimento è solo facilitato dall'uso di tecnologie digitali come computer, reti informatiche e altre forme di ICT. In questi casi, la tecnologia non è essenziale per il crimine in sé, ma svolge un ruolo secondario, anche se importante, nel rendere più efficiente l'organizzazione e l'esecuzione dell'attività illecita.

Si tratta dunque di crimini definiti come "*tradizionali*" da Wall, ma "*assistiti dalla tecnologia*", dove quest'ultima viene usata come mezzo di comunicazione o per supportare l'organizzazione e le operazioni già esistenti nel contesto offline[142].

È interessante allora tentare di comprendere in cosa si concretizzi questa "assistenza" o "facilitazione" del crimine da parte della tecnologia.

Su questo tema non può non menzionarsi l'approfondimento operato da Lavorgna, che ha esaminato come Internet venga utilizzato per commettere crimini di transito e come la rete abbia modificato i comportamenti e i processi criminali, riorganizzando le relazioni tra fornitori, intermediari e acquirenti. Lavorgna ha identificato cinque principali tipi di opportunità che Internet offre ai gruppi criminali coinvolti in attività illecite tradizionali. In questi casi, la rete: facilita la comunicazione non solo tra criminali, ma anche tra loro e i potenziali clienti tramite l'uso di e-mail, Skype e altre forme di messaggistica istantanea (opportunità comunicative); migliora l'efficienza dei mercati criminali consentendo aggiustamenti rapidi e facili del commercio in risposta ai cambiamenti nella domanda (opportunità manageriali); agevola l'organizzazione interna dei gruppi commerciali (opportunità organizzative); consente l'espansione delle relazioni tra criminali creando nuove relazioni commerciali (opportunità relazionali); serve anche come risorsa per comprendere le esigenze dei clienti potenziali e promuovere i prodotti contraffatti in modo più efficace (opportunità promozionali)[143].

Inoltre, le nuove tecnologie, incluse quelle legate al deep web e alla darknet, possono essere utilizzate in diverse fasi delle operazioni criminali.

In primo luogo, durante le fasi preparatorie, i membri delle organizzazioni possono comunicare in modo sicuro tramite piattaforme di messaggistica protette da crittografia *end-to-end*, come Signal e le altre già trattate, o attraverso il Voice over IP (VoIP). Inoltre,

---

[142] Sul punto sempre WALL D.S.*, Digital realism and the governance of spam as cybercrime*, in *European Journal on Criminal Policy and Research*, 10, 4, 2005, pp. 309–335; WALL D.S., *The Internet as a Conduit for Criminals*, in Pattavina A. (ed*) Information technology and the criminal justice system*. Sage, Thousand Oaks, 2015, pp. 77–98.
[143] Cfr. LAVORGNA A., *Organised crime goes online: realities and challenges*, cit., pp. 153–168.

si avvalgono del deep web per acquistare strumenti illeciti, come armi, e sfruttano sistemi di geo-localizzazione satellitare e di sorveglianza a distanza tramite WiFi per monitorare e controllare il territorio[144].

Una volta che i reati vengono commessi, poi, la tecnologia continua a svolgere un ruolo fondamentale. Nel caso del traffico di sostanze stupefacenti, ad esempio, i criminali possono utilizzare il *deep web* per la distribuzione delle droghe attraverso il *black market*. Oppure attività come il riciclaggio di denaro sporco, le frodi tramite carte di credito, e il commercio di prodotti contraffatti e preziosi vengono svolte poi in ambienti sicuri e anonimi come i Tor *black markets*[145].

Fatte queste considerazioni generali sull'interazione tra tecnologia e attività criminali, è ora necessario esaminare in dettaglio come Internet abbia trasformato alcune delle principali aree del crimine.

3.1. La tecnologia nelle attività di narcotraffico

Le droghe continuano a rappresentare una delle principali fonti di finanziamento per i gruppi criminali organizzati, ma i modelli di business nel traffico illecito stanno subendo profondi cambiamenti. L'avvento di nuove tecnologie e l'emergere di reti virtuali, come la Darknet – un ambiente criptato e anonimo – hanno trasformato il panorama del commercio di sostanze stupefacenti e modificato il profilo degli attori coinvolti.

In particolare, le ricerche indicano che i gruppi criminali che operano in contesti digitali tendono a essere caratterizzati da legami più deboli e ad adottare strutture organizzative orizzontali, in contrapposizione alle tradizionali gerarchie verticali[146].

Sul punto, è utile richiamare un report dell'EMCDDA[147] che, per quanto non sia di recente pubblicazione, ha il merito di aver, per la prima volta, distinto tra le diverse funzioni che Internet svolge nel traffico di droga[148].

---

[144] Cfr. FLOR R., LUPARIA L., *Criminalità organizzata e criminalità informatica ("cyber-organized-crime")*, in *Diritto penale contemporaneo*, 2019.
[145] *Ibidem*.
[146] Cfr United Nations Office on Drugs and Crime, European Monitoring Centre for drugs and drug addiction, *Organized Crime Markets. Drug Trafficking*, in Organized Crime, Module 3 E4J, 2018..
[147] European Monitoring Centre for drugs and drug addiction.
[148] Cfr. EMCDDA, *EU drug markets report: a strategic analysis*, European Monitoring Center for Drugs and Drug Addiction, Publications office of the European Union, Luxembourg, 2013.

Il rapporto evidenzia come Internet venga sfruttato per ottenere risorse, in particolare informazioni su come produrre droghe. Ci sono addirittura delle aree apposite nel deep web dedicate al traffico di sostanze, come Silk Road, una piattaforma globale utilizzata per la vendita di cannabis, oppiacei e droghe sintetiche, che sfrutta l'anonimato per ostacolare i tentativi di sorveglianza. Le reti sociali tra corrieri di fiducia vengono utilizzate anche per reclutare nuovi membri. Inoltre, gli acquirenti possono esaminare la qualità delle sostanze, dando così la possibilità ai venditori di costruire una reputazione online. Si segnala poi che Internet permette l'uso di sistemi di pagamento alternativi, come carte prepagate e criptovalute, oltre che la possibilità per i venditori di operare in modalità "*stealth*", ovvero nascondersi dietro ulteriori livelli di sicurezza e gestire le transazioni solo con una clientela selezionata[149].

Negli ultimi anni, l'impiego di piattaforme online per la commercializzazione di droghe sintetiche è aumentato e si è evoluto, fornendo ai criminali uno strumento efficace per promuovere i loro prodotti e raggiungere una vasta clientela, nonché per celare in modo più sofisticato le loro attività illecite. Queste piattaforme hanno anche contribuito a rendere più professionale il mercato della droga, attraverso la pubblicità dei prodotti con descrizioni precise, immagini, informazioni sulla disponibilità, offerte e sconti, nonché la creazione di una reputazione online tra i consumatori[150].

Il "modello di distribuzione diretta" rappresenta uno degli strumenti principali attraverso cui la vendita di droga online massimizza i profitti e accelera i processi operativi. Questo modello, che caratterizza i criptomercati, consente ai venditori di eliminare o quantomeno ridurre significativamente la necessità di intermediari tradizionali come grossisti, broker, trafficanti e venditori ambulanti. In sostanza, la distribuzione delle sostanze stupefacenti avviene direttamente attraverso il sistema postale o tramite corrieri privati, che partecipano in maniera indiretta alla distribuzione, senza però avere una conoscenza diretta dell'attività illecita in corso[151]. La rimozione di

---

[149] *Ibidem*.

[150] Per una chiara schematizzazione delle piattaforme digitali v. United Nations, *UN Toolkit on synthetic drugs*, disponibile al seguente indirizzo: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/onlinetrafficking/onlinesalesplatforms.html; Cfr. CHILDS A., BERNOT A., *The platformisation of illicit drug markets: How datafication, technological affordances, and platform-mediated labour practices shape illicit drug markets*, in *Crime, Media, Culture, an International journal,* 21, 2, 2024, p. 4.

[151] Cfr. MORELATO, M., BROSÉUS, J., DE GRAZIA, A., TAHTOUH, M., ESSEIVA, P., ROUX, C., 2018. *Forensic drug intelligence and the rise of cryptomarkets. Part II: Combination of data from the physical and virtual markets,* in *Forensic Sci. Int*., 288, pp. 201-210, https://doi.org/10. 1016/j.forsciint.2018.05.002; BERTOLA

tali intermediari, che tradizionalmente aumentano i costi e rallentano i tempi di consegna, consente dunque ai venditori di massimizzare i propri guadagni e di operare in un contesto più rapido e flessibile.

Il vantaggio principale di questo modello è la semplificazione e l'accelerazione delle operazioni. I venditori, infatti, non sono più vincolati a strutture di distribuzione rigide e complesse, tipiche dei mercati tradizionali, ma possono raggiungere direttamente i loro acquirenti, abbattendo le barriere logistiche e facilitando la gestione delle transazioni. Questa forma di distribuzione diretta, infatti, non solo riduce i costi legati al passaggio di mano delle merci attraverso vari attori intermediari, ma consente anche una gestione più agile e sicura della transazione, specialmente grazie all'uso di sistemi di pagamento avanzati come le criptovalute e i sistemi di deposito a garanzia. Quest'ultimo, in particolare, contribuisce ad aumentare la fiducia tra venditori e acquirenti, poiché il pagamento viene effettuato solo dopo che la merce è stata ricevuta, proteggendo entrambe le parti da truffe e da interventi da parte delle forze dell'ordine[152].

Nella stessa logica si inseriscono cosiddette "opportunità comunicative": in tutte le fasi del traffico di droga, la comunicazione tra i trafficanti e tra questi e i potenziali acquirenti è semplificata da strumenti come e-mail, Skype e forum[153].

Inoltre, il modello di distribuzione diretta ha reso più accessibile l'ingresso nel mercato della droga, abbattendo molte delle barriere all'ingresso tipiche dei traffici tradizionali. La struttura dei mercati darknet ha messo a disposizione degli utenti non solo una vasta base di clienti preesistente, ma anche risorse pratiche, come guide ai venditori e forum di discussione, che offrono supporto a chi desidera entrare nel commercio illecito[154].

Il secondo vantaggio derivante dalla vendita di droga online, che contribuisce ulteriormente alla massimizzazione dei profitti e all'efficienza operativa, risiede nella libertà territoriale che i criptomercati offrono ai venditori, contrastando con il tradizionale modello di "spaccio", che è invece intrinsecamente limitato e territoriale.

F., *Drug Trafficking on Darkmarkets. How Cryptomarkets are Changing Drug Global Trade and the Role of Organized Crime*, cit., p. 28.

[152] Cfr. KABRA S., GORI S., *Drug trafficking on cryptomarkets and the role of organized crime groups,* in *Journal of economic criminology*, 2, 2023, p. 2; LAVORGNA A., *Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics*, cit., pp. 267-268.

[153] Cfr. LAVORGNA A., op. ult. cit., pp. 250-270.

[154] Cfr. KABRA S., GORI S., *Drug trafficking on cryptomarkets and the role of organized crime groups,* cit., p. 2; BERTOLA F., *Drug Trafficking on Darkmarkets. How Cryptomarkets are Changing Drug Global Trade and the Role of Organized Crime*, cit., p. 28.

Infatti, nel contesto tradizionale, il commercio di droga avviene all'interno di aree geografiche prestabilite, gestite da gruppi criminali che si spartiscono il territorio. Generalmente, ogni gruppo è vincolato a una zona specifica, e qualsiasi tentativo di vendere oltre i confini stabiliti provoca conflitti, alimentando la competitività e la guerra tra gli stessi per il controllo del mercato locale. La territorialità, in questo caso, non solo limita l'espansione del traffico di droga, ma implica anche il rischio di violenze, scontri diretti e danni economici per diversi gruppi criminali, che sono costretti a mantenere il commercio all'interno dei limiti del loro dominio geografico[155].

Al contrario, i criptomercati eliminano questa rigidità territoriale, offrendo ai venditori la possibilità di operare senza alcuna restrizione fisica. La piattaforma online permette a un venditore, indipendentemente dalla sua posizione nel mondo, di accedere a una clientela globale e di distribuire droga a livello internazionale. L'abbattimento delle barriere geografiche consente dunque di ampliare significativamente il raggio d'azione delle attività illecite, poiché un venditore non è più vincolato alle dinamiche locali o alle leggi dei singoli Stati. Infatti, grazie alla natura anonima e criptata del dark web, le transazioni possono avvenire senza il rischio di interferenze dirette da parte delle autorità locali o della concorrenza territoriale[156].

Al contempo, il traffico di droga nel cyberspazio consente una minimizzazione dei rischi legati alle operazioni tradizionali delle organizzazioni criminali.

Grazie alla possibilità di operare in modo anonimo, i sodalizi criminali riescono ad abbattere significativamente il rischio di arresti o la violenza perpetrata da altre organizzazioni criminali. L'accesso ai criptomercati avviene con un semplice clic, senza confini territoriali che possano limitare la distribuzione della sostanza, ed è possibile condurre ogni fase dell'approvvigionamento e della vendita da dietro uno schermo, eliminando completamente l'elemento della vulnerabilità fisica[157]. In proposito, Lavorgna si riferisce anche alle cosiddette "opportunità di contromisure", poiché Internet permette

[155] Cfr. KABRA S., GORI S., *Drug trafficking on cryptomarkets and the role of organized crime groups,* cit., pp. 2-3; LAVORGNA A., *Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics*, cit., pp. 267-268.
[156] *Ibidem.*
[157] *Ibidem*; v. BERTOLA F., *Drug Trafficking on Darkmarkets. How Cryptomarkets are Changing Drug Global Trade and the Role of Organized Crime*, cit., p. 28.

di mascherare il traffico, gestendo in modo discreto le interazioni con i clienti e riducendo i rischi di infiltrazione delle forze dell'ordine[158].

Proseguendo, le opportunità tecniche si rivelano altrettanto decisive, in quanto consentono di organizzare trasporti e alloggi tramite servizi online, riducendo così il contatto fisico e l'esposizione ai rischi. Ciò facilita, a sua volta, anche le opportunità manageriali, che permettono una gestione più efficace del traffico in tutte le sue fasi, dalle prime preparazioni alla distribuzione finale. In particolare, nel caso delle droghe tradizionali, queste opportunità permettono di controllare mercati offline anche a distanza, mentre per le droghe sintetiche, la gestione avviene in base al feedback online dei consumatori, permettendo di adattare la produzione alle richieste del mercato[159].

Le opportunità organizzative derivanti dall'uso di Internet, inoltre, semplificano alcune fasi della rete criminale, eliminando, come si è detto, gli intermediari locali e favorendo l'ingresso di nuovi soggetti, come nel caso di acquisti da grossisti online.

L'uso della rete amplia anche le opportunità relazionali, poiché consente di espandere le reti criminali e di creare contatti tra colleghi e nuovi acquirenti. Per esempio, nel traffico di droghe tradizionali, Internet viene utilizzato anche per reclutare nuovi corrieri. In parallelo, Internet offre anche opportunità promozionali, consentendo la pubblicizzazione di disponibilità e prezzi, sia online che in eventi fisici, con un impatto diretto sulle fasi centrali e finali del traffico[160].

Infine, le opportunità persuasive legate alla rete sono fondamentali, specialmente nel traffico di droghe sintetiche, dove vengono utilizzate per rassicurare i clienti riguardo l'anonimato e la segretezza delle transazioni, influenzando così le fasi finali del traffico. Allo stesso modo, le opportunità di marketing e fidelizzazione permettono di rafforzare il legame con i clienti abituali, per esempio attraverso sconti per gli acquirenti frequenti di droghe sintetiche[161].

Un esempio emblematico di questa tendenza è rappresentato dal criptomercato "Cartel de Sinalao" (CDS), direttamente associato al celebre cartello di Sinaloa e ai suoi leader, Los Chapitos. Oltre al traffico di stupefacenti, il CDS offre una vasta gamma di servizi

---

[158] Cfr. sempre LAVORGNA A., *Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics,* cit., pp. 250-270.
[159] *Ibidem*.
[160] *Ibidem*.
[161] *Ibidem*.

illeciti, tra cui software e malware, noleggio di strumenti per attività criminali, contraffazione, tratta di esseri umani, riciclaggio di denaro e altri servizi legati a crimini di diversa natura. Questa espansione nel cyberspazio consente al cartello di operare in maniera più sicura, anonima e senza confini geografici, riducendo sensibilmente i rischi associati alle operazioni di traffico di droga tradizionali[162].

Altro esempio significativo di come la tecnologia, in particolare le comunicazioni criptate, siano diventate fondamentali per il traffico di droga delle organizzazioni criminali può essere tratto dall'Operazione Eureka, condotta nel 2023 da Europol ed Eurojust in collaborazione con dieci Stati membri dell'UE.

Le indagini hanno rivelato come l'uso di comunicazioni criptate fosse essenziale per le attività internazionali di traffico di droga svolte da gruppi criminali, in particolare da clan della 'ndrangheta, sia in paesi con grandi diaspore calabresi che in altri contesti. Questi gruppi, noti per la loro struttura e potenza, utilizzavano tecnologie avanzate per coordinare le loro operazioni su scala globale, riducendo così il rischio di intercettazioni e aumentando l'efficienza delle loro reti di distribuzione[163].

Dalle intercettazioni effettuate nell'Operazione Eureka è emerso chiaramente un approccio imprenditoriale nei confronti della tecnologia, dove l'adozione di strumenti avanzati come i criptotelefoni diventa parte integrata e necessaria per il successo e la continuità delle attività illecite.

In particolare, dalle intercettazioni del membro di un clan criminale ‘ndranghetista, che interloquiva con un associato in Germania, è emerso chiaramente come questi dispositivi fossero diventati strumenti funzionali per la gestione delle attività di traffico di droga. Nel corso della conversazione si sottolineava come i telefoni fossero stati impiegati per portare avanti il lavoro, in particolare per la movimentazione della droga e riconosceva altresì come l’utilizzo della piattaforma SkyEcc, da loro testata avrebbe rappresentato, un’opportunità per i loro affari[164].

---

[162] Cfr. KABRA S., GORI S., *Drug trafficking on cryptomarkets and the role of organized crime groups,* cit., pp. 2-3.

[163] Cfr. LAVORGNA A. SERGI A., *Intergenerational and technological changes in mafia- type groups: a transcultural research agenda to study the ‘ndrangheta and its mobility*, cit., p. 3.

[164] Tribunale di Reggio Calabria Proc. n. 3886/2022 r.g.n.r., DDA Proc. n. 2520/2022 Reg. G. L P. DDA/2022 R. O. C. C. 44/2022 R. O. C. C. 4/202S R. O. C. C., p. 2139. Si fa riferimento alle intercettazioni di Giorgi, membro di un clan ‘ndranghetista. Di seguito l’estratto della conversazione: “*Bro’, listen to me, not just because I sell the Sky phones, but figure it out, with what phones have we carried out the job? How did we move all the stuff until this morning? All those who came to pick up, did you do that? All of them with Sky...so what does that mean? I say that Sky has been tested and I only see business”.*

3.2. La tecnologia nelle attività di riciclaggio

Un'altra attività criminale in cui le organizzazioni mafiose tradizionali sono da sempre coinvolte, e che l'avvento della tecnologia ha indubbiamente facilitato, è il riciclaggio di denaro. Attraverso questa pratica, i criminali riescono a pulire i fondi derivanti dalle loro attività illecite, trasferendoli tramite una rete di transazioni apparentemente legittime che permettono di inserirli nel sistema economico ufficiale.

Per comprendere come la tecnologia abbia rivoluzionato il riciclaggio di denaro, appare essenziale fare una premessa sulle tre fasi fondamentali che caratterizzano questo processo.

Il momento iniziale dell'operazione si definisce "*placement"*, in quanto consiste nel "collocamento" all'interno del sistema finanziario delle risorse ottenute dalla commissione del reato presupposto del riciclaggio, attraverso la conversione dei fondi illeciti in importi più piccoli, più gestibili, trasportabili e meno sospetti, con lo scopo di conferirvi un'apparenza di legittimità.

Obiettivo principale di questa prima fase è, dunque, quello di allontanare i fondi dalla loro originaria fonte illecita, mettendo così le basi per intraprendere ulteriori stratificazioni dei proventi illeciti che ne mascherino la natura criminosa. Infatti, l'importanza di questa fase si individua nel momento in cui il denaro contante viene convertito in moneta scritturale, un tipo di valore che, per sua natura, è destinato a diventare parte dei saldi attivi detenuti presso gli intermediari finanziari[165].

Tra le tecniche più note di collocamento si annovera lo "*smurfing*", consistente nell'esecuzione di versamenti frazionati attraverso il deposito del denaro di provenienza illecita in più conti aperti presso il medesimo istituto bancario oppure presso banche diverse, tramite l'impiego di numerosi corrieri, noti anche come *smurfs*[166].

"Bro', ascoltami, non solo perché vendo i telefoni Sky, ma capisci, con che telefoni abbiamo fatto il lavoro? Come abbiamo spostato tutta la roba fino a stamattina? Tutti quelli che sono venuti a prendere, l'hai fatto? Tutti con Sky... quindi cosa significa questo? Dico che Sky è stato testato e vedo solo affari".

[165] Cfr. DELL'OSSO ALAIN, *Riciclaggio di proventi illeciti e sistema penale, Itinerari di diritto penale*, cit., p. 35.

[166] Sul punto, v. CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, in *Principles and Practice of Blockchain*, a cura di Daimi K., Dionysiou I., El Madhoun N., 2022, p. 276; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., pp. 97-98.

Passando alla seconda fase tipica del riciclaggio, conosciuta come "*layering*" o stratificazione, si fa riferimento a un movimento più dinamico dei capitali, attraverso il compimento di differenti operazioni come bonifici bancari, trasferimenti, prestiti e pagamenti, con lo scopo di rendere quasi impossibile tracciare l'origine illecita del denaro e, infine, farlo sembrare legittimo[167].

Il successo delle operazioni di *layering* è spesso garantito se le transazioni, sia fisiche che elettroniche, attraversano i confini nazionali o più strutture aziendali. Più strati vengono aggiunti, più complesso diventa lo schema e più difficile risulta per le autorità rintracciare e indagare. Questo continuo spostamento interrompe il legame diretto con la fonte originaria dei proventi – il crimine da cui provengono i fondi.

Non a caso, la tecnica di *layering* più semplice ed efficace è quella di trasferire fondi tramite bonifico elettronico verso giurisdizioni bancarie offshore prima di reindirizzare i fondi verso un'altra località o entità aziendale. In alternativa, piuttosto che coinvolgere istituzioni finanziarie, si può procedere con la creazione di più società di comodo transnazionali, come attività di import-export, agenzie di viaggio e imprese di servizi finanziari[168].

La terza e ultima fase del processo di riciclaggio è conosciuta come "*integration*" o "investimento", e implica la reintegrazione del capitale illecito nel sistema economico legale, con l'intento di farlo sembrare parte di altre risorse legittime presenti sul mercato.

Le origini illecite del denaro diventano così irrintracciabili e i fondi possono essere utilizzati per acquistare beni leciti ed effettuare investimenti legittimi che possono includere attrezzature per sostenere attività criminali future, imprese commerciali che generano reddito, come immobili e attività ad alta intensità di contante, oppure profitti derivanti da strumenti finanziari che possono produrre guadagni in conto capitale o reddito da dividendi[169].

Con particolare riferimento alle organizzazioni criminali di tipo mafioso, è bene precisare come di frequente tra le modalità di investimento utilizzate per "ripulire" il denaro illecito, vengano selezionate imprese di piccole e medie dimensioni, in particolare

---

[167] Cfr. sempre DELL'OSSO ALAIN, *Riciclaggio di proventi illeciti e sistema penale*, cit., p. 38.
[168] Cfr. CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, cit., p. 277; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., pp. 97-98.
[169] Cfr. DELL'OSSO ALAIN, *Riciclaggio di proventi illeciti e sistema penale,* cit., pp. 40 ss.

le società a responsabilità limitata. Queste società, spesso nascoste dietro terze persone o società di comodo, diventano uno strumento attraverso cui i fondi illeciti vengono integrati nell'economia legale[170].

Le attività delle organizzazioni mafiose o con partecipazione mafiosa si concentrano in settori economici legali che presentano caratteristiche ideali per il riciclaggio, come un basso livello tecnologico, una forte intensità di manodopera, una deregolamentazione elevata e una spiccata specificità territoriale. Questi settori includono ristoranti, pizzerie, bar, negozi, palestre, centri estetici, strutture turistiche e impianti di rifornimento carburanti con servizi aggiuntivi[171].

Inoltre, alcune di queste imprese sono direttamente strumentali alle attività criminali, come quelle che operano nei settori della logistica, trasporti e consulenze, essenziali per lo svolgimento dei traffici illeciti. Altri settori ancora, detti "protetti", sono quelli in cui la pubblica amministrazione regola l'accesso tramite autorizzazioni o concessioni, e che spesso beneficiano di finanziamenti o contributi pubblici, che possono essere facilmente manipolati per nascondere i proventi illeciti[172].

Muovendo invece dal livello base delle tecniche di riciclaggio ad un livello più apicale[173], tra i metodi più comuni di reintegrazione del denaro nell'economia legale vi è il trasferimento di fondi da una "*shell company"* o "*shell bank*" – rispettivamente, una società o una banca fittizia di proprietà dei riciclatori, così definite in quanto costituiscono nient'altro che le controparti di operazioni puramente formali – verso un istituto bancario legittimo; si aggiungono, inoltre, tra le pratiche di "*integration*", la manipolazione di fatture per sovrastimare il valore di beni o servizi e facilitare il trasferimento di denaro da un Paese all'altro o, ancora, la creazione di società anonime in giurisdizioni che tutelano il segreto bancario[174].

Infine, tra le tecniche di "*integration*", non può non menzionarsi il "*loan back*", consistente nel prendere una somma di denaro illecito, facendola apparire come un

---

[170] Cfr. CARBONE M., *Riflessioni sul contrasto al riciclaggio nel contest di un'economia che cambia*, in *Rivista della Guardia di Finanza*, 1, 2025, pp. 31-32.
[171] *Ibidem*.
[172] *Ibidem*.
[173] Cfr. lo schema sulle aree di infiltrazione nell'economia di CARBONE M., *Riflessioni sul contrasto al riciclaggio nel contest di un'economia che cambia*, cit., pp. 41.
[174] Cfr. DELL'OSSO ALAIN, *Riciclaggio di proventi illeciti e sistema penale,* cit., pp. 40 ss.; cfr. anche CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, cit., p. 277.

prestito legittimo. In pratica, la persona che ha guadagnato denaro in modo illecito (o tramite un prestanome) ottiene un finanziamento da una fonte apparentemente legittima, ma le garanzie offerte per il prestito sono proprio i fondi di origine illecita. In questo modo, i soldi sporchi vengono "ripuliti" e integrati nel sistema economico legale, senza suscitare sospetti[175].

3.2.1. Il supporto dei "professional enablers" alle attività di riciclaggio

Di consueto, le organizzazioni criminali, sia che mettano in atto operazioni di riciclaggio "tradizionale" sia che scelgano canali di tipo "digitale", decidono di affidarsi ad "abilitatori professionisti" (o *professional enablers*), ovvero figure professionali, come avvocati, contabili e banchieri, che mettono a disposizione le proprie competenze tecniche per mascherare la provenienza del denaro illecito.

Gli abilitatori professionisti possono, complici o per negligenza, assistere i criminali attraverso la creazione di società anonime o di altre strutture legali che nascondono i beneficiari effettivi, per commettere frodi, pagare tangenti o accedere a contratti pubblici, attraverso servizi di nomina a società e altre strutture legali, nonché attraverso assistenza ai criminali per l'apertura di conti bancari (a volte anonimi) onshore o offshore per spostare il denaro sporco[176].

La stessa National Crime Agency non manca di valorizzare la rilevanza, e la conseguente pericolosità, di queste figure professionali nel contrasto al riciclaggio delle organizzazioni criminali. Sostiene, infatti, come dalle analisi condotte in materia di riciclaggio emerge come, al di là della varietà degli strumenti e delle tecniche utilizzabili, il vero punto di snodo risiede spesso nell'intervento di soggetti qualificati in grado di offrire al circuito criminale quella copertura e quella anonimizzazione che solo procedure complesse possono garantire[177].

Anche nel report dell'OCSE "*Ending the Shell Game- Cracking down on the Professionals who enable Tax and White Collar Crimes*", di recente pubblicazione, si evidenzia la pericolosità di una ristretta cerchia di consulenti che utilizzano le proprie

---

[175] *Ibidem*.
[176] Cfr. LEVI M., *Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation*, in *Trends in Organized crime*, 24, 2021, pp. 96-110.
[177] National Crime Agency, *High end money laundering strategy and action plan. National Crime Agency*, London, 2014.

competenze specialistiche per supportare attività criminose nel settore economico-finanziario, anche attraverso la creazione di società fittizie in giurisdizioni solitamente non collaborative[178].

La necessità di abilitatori professionisti dipende dalla grandezza dei profitti illeciti e dal livello di occultamento che i criminali desiderano raggiungere. Nei casi di crimini su larga scala, come quelli gestiti da gruppi criminali organizzati, i profitti sono spesso consistenti e richiedono strutture complesse per essere nascosti. Di conseguenza, è normale che questi gruppi si avvalgano di professionisti per gestire e mascherare i fondi illeciti, garantendo così che le loro operazioni rimangano difficili da tracciare e da fermare[179].

Solitamente, nell'ambito del riciclaggio, troviamo professionisti esperti di contesti e strumenti utili alle intercettazioni di operazioni sospette e, dunque, esperti di diritti di proprietà, operazioni di M&A e finanza strutturata, gestioni d'impresa, ristrutturazioni e crisi aziendali, obblighi contrattuali, contabilità, flussi finanziari o bilanci aziendali[180].

Il ruolo degli abilitatori professionisti ben emerge, ad esempio, dallo scandalo "Panama Papers", derivato dalla collaborazione dello studio legale Mossack Fonseca di Panama con oltre 14.000 banche, studi legali, incorporatori di società e altri intermediari, allo scopo di creare persone giuridiche e strutture legali per i loro clienti che fallissero nel verificare l'identità dei propri clienti e nel segnalare transazioni sospette[181]. Alcuni dei clienti, tra cui individui facoltosi, aziende, leader politici e gruppi criminali organizzati, avrebbero utilizzato queste entità come canali per gestire e nascondere fondi illeciti[182].

3.2.2. Dal riciclaggio tradizionale al cyber-laundering

Con "*cyber-laundering*" si intende, come d'altro canto lascia emergere la stessa definizione, un fenomeno che comprende l'insieme delle attività illecite finalizzate a "ripulire" (letteralmente "lavare") non solo il denaro (c.d. *money laundering*), ma più in

---

[178] Cfr. OCSE Report "*Ending the Shell Game- Cracking down on the Professionals who enable Tax and White Collar Crimes*", 25 febbraio 2021.
[179] In proposito, v. LEVI M., *Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation*, cit., pp. 96-110.
[180] Cfr. CARBONE M., *Follow the money a trent'anni dall'uccisione di Giovanni Falcone. Le indagini finanziarie e patrimoniali 3.0*, in *Rivista della Guardia di Finanza*, supplemento al n. 1-2022, p. 149.
[181] International Consortium of Investigative Journalists, *Explore the Panama Papers Key Figures*, 2017.
[182] *Ibidem*; sul punto v. anche CARBONE M., *Riflessioni sul contrasto al riciclaggio nel contest di un'economia che cambia*, cit., p. 34.

generale i capitali, i beni, i valori o altre "utilità" di provenienza delittuosa, ricorrendo a sistemi e mezzi "cibernetici"[183].

Al netto del dibattito dottrinale relativo al controverso inquadramento normativo del *cyber-laundering* nell'ambito della categoria dei *cybercrimes* o nella disciplina tradizionale del riciclaggio[184], ciò che rileva, ai fini del presente lavoro, è evidenziare come funzioni il riciclaggio digitale e in che modo, dunque, l'utilizzo di sistemi di tecnologia abbia modificato il modello trifasico sopra descritto.

In generale, il processo risulta simile a quello del riciclaggio di denaro tradizionale, ma l'impiego delle criptovalute offre notevoli vantaggi operativi ai riciclatori informatici, in termini di guadagni, rapidità e riduzione del rischio di identificazione.

In particolare, le criptovalute presentano almeno due caratteristiche fondamentali che rendono più efficienti le varie fasi del riciclaggio.

In primo luogo, l'anonimato, quasi totale, che è cruciale per limitare le possibilità di monitorare e tracciare i flussi di denaro, sia prima che dopo il completamento delle operazioni. In secondo luogo, la rapidità delle transazioni e il loro svolgimento in tempo reale, che complica il rilevamento durante il trasferimento dei fondi, nonché i conflitti giurisdizionali, che ostacolano l'attuazione delle leggi e l'esercizio di azioni penali[185].

Un modo semplice per nascondere e rendere meno evidenti i trasferimenti di criptovaluta nel sistema finanziario è poi il c.d. "*micro riciclaggio*": seguendo questa pratica, vengono suddivise grandi quantità di criptovalute in piccole somme, che poi vengono scambiate con moneta tradizionale e depositate su conti bancari legittimi.

---

[183] In proposito cfr. PICOTTI L., *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. Trim. Dir. pen. dell'economia*, 3-4, 2018, pp. 590-591.

[184] Il fenomeno del *cyberlaundering*, pur essendo un'attività criminosa commessa nel cyberspazio, solleva interrogativi circa la sua inquadrabilità nella categoria dei *cybercrimes* o, più tradizionalmente, nel riciclaggio di denaro. Se per alcuni autori è chiaro che si tratti di un *cybercrime* (v. PICOTTI L., *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, cit., pp. 592 e 608), altri sottolineano che questa classificazione rischia di ignorare gli aspetti giuridici specifici del reato di riciclaggio, focalizzandosi troppo sugli aspetti informatici (v. LESLIE A., *Legal Principles for Combatting Cyberlaundering, Law, Governance and Technology Series*, 2014, pp. 61-62).
Da un lato, infatti, si potrebbe correre il rischio di perdere di vista la disciplina tradizionale del riciclaggio, concentrandosi solo sull'uso degli strumenti informatici e trascurando la natura del reato. Dall'altro, considerare il *cyberlaundering* esclusivamente come una tecnica di riciclaggio comporta il rischio di semplificare eccessivamente il fenomeno, non tenendo conto del ruolo centrale che il cyberspazio gioca nell'intero processo criminoso.

[185] In argomento, PILLER G., ZACCARIOTTO E., *Cyber-Laundering: The Union Between New Electronic Payment Systems and Criminal Organizations*, in *Transition Study Review*, 2009, pp. 65 e ss.; CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, cit., p. 278-279; KRUISBERGEN E.W., LEUKFELDT E.R., KLEEMANS E.R., ROKS R., *Money talks money laundering choices of organized crime offenders in a digital age,* cit.pp. 574 ss.

Combinando questa tecnica con altri servizi online che mescolano criptovalute, nonché strumenti che proteggono la privacy, i criminali riescono dunque a rendere ancora più anonime e riservate le transazioni[186].

Inoltre, a differenza della moneta tradizionale, la criptovaluta può essere usata sia per entrare che per uscire, in qualsiasi momento, dal processo di riciclaggio, potendo il possessore delle criptovalute usare piattaforme di scambio non registrate o altri intermediari finanziari per aggirare sistemi bancari e autorità di controllo, come quelle che si occupano della verifica dell'identità dei clienti[187].

Non sorprende, allora, che queste nuove forme di riciclaggio siano state ben accolte dalle associazioni criminali che, con il rapido progresso economico e sociale, hanno scelto di concentrarsi maggiormente sull'imprenditoria, di dedicarsi ad operazioni finanziarie e a servizi pubblici, acquisendo sempre più il c.d. "*enterprise syndicate*", ossia una dimensione transnazionale, di natura imprenditoriale[188].

Inoltre, dall'analisi delle tre fasi del *cyber-laundering*, appariranno ancor più evidenti i vantaggi che le organizzazioni criminali possono trarre da questo nuovo fenomeno.

Quanto alla fase di posizionamento, anche detta "*cyber-placement*", qualora si tratti di riciclaggio digitale strumentale, - ovvero quando il denaro è inizialmente presente in forma materiale contante e viene convertito in moneta digitale solo in un momento successivo -, assumono un ruolo essenziale due nuove figure: gli *exchangers* e i *wallet providers.*

Con il termine *exchanger*[189], si fa riferimento alla persona fisica o giuridica che, dietro pagamento di una commissione, mette a disposizione degli utenti un servizio di cambio di moneta avente corso legale con criptomonete.

---

[186] Sempre CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, cit., p. 278-279.
[187] *Ibidem*.
[188] Cfr. PATALANO R., *Riciclaggio e flussi finanziari illeciti nel capitalismo contemporaneo*, in *Riv. Online della politica economica*, 2022, disponibile in https://www.economiaepolitica.it/lavoro-e-diritti/distribuzione-e-poverta/riciclaggio-e- flussi-finanziari-illeciti-nel-capitalismo-contemporaneo/
[189] Si riporta di seguito la definizione fornita dalla BCE, in *Virtual currency schemes*. *A further analysis,* 2015, p. 8: "*Exchangers offer trading services to users by quoting the exchange rates by which the exchange will buy/sell virtual currency against the main currencies (US dollar, renmibi, yen, euro) or against other virtual currencies. These actors, most of them non-financial companies, can be either issuer-affiliated or a third party. They generally accept a wide range of payment options including cash, credit transfers and payments with other virtual currencies. Moreover, some exchanges also provide statistics (e.g. volumes traded and volatility), act as wallet providers and offer (immediate) conversion services for merchants who accepts VCS as an alternative payment method".*

Accanto all'*exchanger*, gioca un ruolo preminente in questa prima fase anche il *wallet provider*[190], che detiene la gestione del denaro virtuale in una sorta di portafoglio elettronico.

Inoltre, con il riciclaggio informatico, contrariamente al "tradizionale", il riciclatore non si affida ai corrieri per soddisfare la strutturazione iniziale nella fase di collocamento: la criptovaluta "sporca" viene convertita ("ripulita") direttamente per via digitale, utilizzando software di miscelazione o provider di servizi di miscelazione[191]. Vari importi della criptovaluta "pulita" vengono depositati in più blockchain di criptovaluta e portafogli virtuali, evitando così il ricorso ad intermediari finanziari regolamentati ed aggirando conseguentemente i requisiti di segnalazione[192].

Quanto alla seconda fase, invece, il c.d. "*cyber-layering*", risulta più semplice il ricorso al trasferimento di fondi in *shell companies* o all'acquisto di beni online che vengono poi rivenduti. A questo proposito, il riciclatore di denaro può utilizzare direttamente la criptovaluta "pulita" presente nella blockchain o nel portafoglio virtuale oppure può convertire la criptovaluta "pulita" in denaro tradizionale per acquisti, trasferimenti e investimenti. Questo diventa quindi un aspetto significativamente più semplice e meno laborioso rispetto al riciclaggio tradizionale[193].

Con riguardo, infine, alla fase di integrazione, c.d. "*cyber-integration*", sebbene tale ultima fase resti abbastanza similare a quella "tradizionale", le tecniche di integrazione, presentano però delle caratteristiche differenti. Mentre, infatti, nel caso del riciclaggio tradizionale si utilizzano, ad esempio, in via preminente false fatture per beni e servizi,

---

[190] Si riporta di seguito la definizione fornita dalla BCE, in *Virtual currency schemes*. *A further analysis,* 2015, p. 8: "*Wallet providers offer a digital wallet to users for storing their virtual currency cryptographic keys and transaction authentication codes, initiating transactions and providing an overview of their transaction history. There are basically two types of wallet, which differs as regards their immediate usability versus their safety from cyber crime: online wallets (hot storage) and offline wallets (cold storage). From a functional perspective, these services for desktop PCs, mobile devices and as cloud-based applications. Nevertheless, users can also set up and maintain a wallet themselves without making use of a wallet provider".*

[191] I *mixing* e *tumbling services* sono strumenti usati nel riciclaggio di denaro con criptovalute, che mescolano fondi provenienti da diverse fonti per renderne difficile la tracciabilità. Il mixing avviene attraverso la separazione delle criptovalute in piccole transazioni e la successiva riaggregazione delle stesse, rendendo il flusso di denaro anonimo.

[192] Cfr. CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, cit., p. 279 ss.

[193] *Ibidem.*

nella "*cyber-integration*", invece, sono le società fittizie, già menzionate durante la fase di "*cyberlayering*", a rivestire un ruolo centrale[194].

3.2.2.1. Recenti casi di cyber-laundering tra le organizzazioni criminali

Sebbene il riciclaggio di denaro tramite criptovalute sia ancora una pratica relativamente marginale rispetto ad altri metodi tradizionali, si osserva un trend in crescita, soprattutto nell'ambito del narcotraffico e di altre attività illecite.

Uno dei casi significativi di riciclaggio di denaro tramite criptovaluta è stato individuato nel 2018 dalla Guardia Civil spagnola, che ha smantellato un'organizzazione criminale impegnata nel traffico di cocaina. Quest'ultima utilizzava Bitcoin per riciclare i proventi delle attività illecite, depositando i fondi su conti bancari colombiani. In totale, sarebbe stati impiegati 174 conti per riciclare circa 8 milioni di euro[195].

Le criptovalute sono state ritenute uno strumento allettante anche per i cartelli messicani. Secondo le segnalazioni della UIF (Unidade de Inteligência Financeira), i cartelli si stanno spostando verso Internet, dove le criptovalute offrono un canale più efficace per "ripulire" le loro ricchezze, come emerso nel dicembre del 2022, quando l'agenzia antidroga americana ha scoperto che il cartello di Jalisco Nuova Generazione aveva trasferito tra i 15 e i 40 milioni di dollari attraverso la piattaforma di scambio di criptovalute Binance, una delle più grandi al mondo[196].

In Europa, tuttavia, il fenomeno del riciclaggio tramite criptovalute non ha ancora raggiunto la stessa intensità che si osserva in America Latina. Europol ha infatti sottolineato che, per quanto le transazioni criminali in criptovalute stiano aumentando, il loro valore complessivo rimane ancora modesto rispetto ad altre forme di pagamento illegale, come il denaro contante. Al contempo, Europol ha comunque rilevato un trend crescente nell'uso delle criptovalute nelle attività criminali e nel riciclaggio di denaro, con segnali di un cambiamento in corso[197].

Pertanto, nonostante il crescente interesse per l'uso delle criptovalute nel crimine, in Italia e in altre parti d'Europa le associazioni criminali, prevalentemente di tipo mafioso,

---

[194] *Ibidem.*
[195] Cfr. GRATTERI N., NICASO A., *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*, Mondadori, 2023, "Criptovalute".
[196] *Ibidem.*
[197] Europol, *Internet Organised crime threat assessment*, IOCTA, 2021, p. 9.

continuano a preferire metodi tradizionali, come il denaro contante, mostrando ancora una certa diffidenza verso le valute digitali[198].

Si riscontrano, tuttavia, episodi, seppur limitati, da cui si deduce un crescente e rapido adattamento alle nuove tecnologie da parte delle organizzazioni criminali, in particolare da parte dell' 'ndrangheta.

Proprio con riferimento ai clan della Locride, nell'aprile 2019, appare la prima traccia mediatica dell'utilizzo dei bitcoin per il pagamento di alcune partite di cocaina acquistate in Brasile. Ebbene, secondo il Centro Studi Internazionale, e anche ai sensi della relazione semestrale della DIA riferita al primo semestre del 2021, tale organizzazione sarebbe dotata di tanta dimestichezza da aver già superato l'utilizzo dei Bitcoin, sperimentando la criptovaluta Monero, che non consentono il tracciamento e sfuggono al monitoraggio bancario [199].

La 'ndrangheta pare quindi essersi portata avanti, ricorrendo addirittura ad una criptovaluta particolarmente difficile da tracciare, la moneta Monero, a causa di una serie di tecnologie avanzate. Segnatamente, con l'impiego di questo tipo di moneta virtuale, risulta ostacolata l'identificazione del reale mittente delle transazioni, attraverso la c.d. "Ring Signature", che crea una firma collettiva mescolando l'autenticazione del mittente con altre persone. In secondo luogo, appare altresì di complessa divulgazione l'indirizzo di destinazione, trattandosi di un indirizzo univoco per ogni transazione. A ciò si aggiunge, infine, l'oscuramento dell'importo delle transazioni, le quali possono in alcuni casi persino essere frazionate[200].

3.2.2.2. Metodi di cyber-laundering: il riciclaggio tramite aste online e piattaforme d'azzardo online

Tra le pratiche più comuni e diffuse di *cyber-laundering* occorre senza dubbio menzionare le aste e il gioco d'azzardo online. Queste ultime, grazie alla loro natura digitale e alla relativa difficoltà di controllo, offrono agli individui coinvolti nel

[198] Ordinanza di applicazione di misure cautelari personali nei confronti di Annunziata Katia + 72, 6 novembre 2018, GIP del Tribunale di Reggio Calabria, p. 223.
[199] Relazione 1 semestre, DIA, 2021, p. 409; Centro Studi Internazionali., *L'uso delle criptovalute nelle attività internazionali della 'ndrangheta*, 2020.
[200] Cfr. GRATTERI N., NICASO A., *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*, cit., "Criptovalute".

riciclaggio di denaro opportunità ideali per nascondere l'origine illecita dei fondi e inserirli nel circuito economico legittimo.

L'utilizzo di aste online per il riciclaggio di denaro, ad esempio, è una delle strategie più sofisticate adottate dai criminali, poiché sfrutta l'apparente legittimità e la trasparenza delle piattaforme di vendita online. Queste aste, come quelle di beni di seconda mano o aste per prodotti di valore (arte, collezionismo, beni di lusso, ecc.), possono essere utilizzate per mascherare transazioni illecite e generare una "copertura" legale per i proventi criminali.

In queste piattaforme, è possibile che un acquirente e un venditore si accordino per scambiare beni che, in realtà, non esistono o non sono mai stati effettivamente trasferiti. Questo tipo di scambio, che coinvolge non solo "oggetti fantasma", ma anche beni falsificati o rubati, avviene a un prezzo concordato in anticipo, che può essere ben al di sopra o al di sotto del valore di mercato[201]. Con specifico riferimento al settore delle opere d'arte, si rileva, in particolare, che ciò che attrae i riciclatori è proprio l'assenza di stime di prezzo ufficiali, essendo le quotazioni dell'opera d'arte puramente indicative, a differenza di altri "beni rifugio"[202].

Dopo aver acquisito la proprietà di determinati beni, che si prestano facilmente ad essere scambiati a prezzi stabiliti in modo convenzionale dalle parti coinvolte, la transazione viene registrata a un valore fittizio, sovra o sottostimato, cosicché una delle parti riesca nell'attività di drenaggio dei propri fondi illeciti[203].

L'operazione, dunque, permette di far sembrare che il denaro proveniente dal crimine sia stato guadagnato legittimamente attraverso la vendita di prodotti, camuffando così il flusso di capitali sporchi come redditi derivanti da attività legittime[204]. In particolare, la fase di "*layering*" (stratificazione) in questo caso viene effettuata dal venditore, poiché l'acquirente non dovrà mascherare l'origine dei proventi illeciti e, una volta che la vendita

---

[201] Cfr. NIMMA S., *Money Laundering In The Cyberworld: Emerging Trends*, in *Indian Journal of Integrated Research in Law*, 2, 2, 2022, p. 10.
[202] Cfr. DELL'OSSO A.M., *Riciclaggio di proventi illeciti e Sistema penale,* cit., p. 42.
[203] Cfr. CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, cit., p. 281; DELL'OSSO A.M., *Riciclaggio di proventi illeciti e Sistema penale,* cit., p. 42; Cfr. anche NIMMA S., *Money Laundering In The Cyberworld: Emerging Trends*, cit., p. 10.
[204] Cfr. GRABOSKY P., *The Internet, Technology and Organised crime*, cit., pp. 146-161.

è stata finalizzata, i proventi ripuliti possono essere poi investiti in attività legalizzate (integrazione)[205].

Come accade nel gioco d'azzardo tradizionale, anche il gioco d'azzardo online rappresenta un metodo rapido ed efficace per legittimare fondi illeciti e aggirare il fisco, soprattutto in presenza di casinò offshore situati in giurisdizioni con normative più permissive, che permettono di riciclare e distribuire grosse somme di denaro[206].

I siti di casinò virtuali offrono ai visitatori l'esperienza di giochi da casinò reali. Tuttavia, a differenza dei casinò fisici, dove è necessario interagire direttamente con il personale e i giocatori, le piattaforme di gioco online offrono un ambiente virtuale che consente agli utenti di partecipare al gioco con informazioni personali ridotte al minimo.

L'anonimato diventa un'opportunità per i criminali, che possono approfittare della situazione utilizzando carte di credito rubate, identità false o criptovalute. Inoltre, molti siti di gioco online permettono agli utenti di creare più account, una possibilità che i malintenzionati sfruttano per trasferire denaro tra i vari conti, mascherando l'origine dei fondi, come denaro ottenuto dalle vincite di gioco, e rendendo difficile per le autorità rintracciare il flusso di denaro illecito[207].

In particolare, facendo riferimento allo schema tradizionale del riciclaggio di denaro, le piattaforme di gioco online possono essere sfruttate da attori illeciti in ciascuna delle tre fasi del riciclaggio di denaro: nella fase di collocamento, i fondi illeciti vengono introdotti nel sistema finanziario tramite il deposito di denaro su conti di gioco; nella fase di stratificazione, la fonte dei fondi viene nascosta tramite transazioni complesse che coinvolgono più scommesse, trasferimenti e prelievi all'interno della piattaforma di gioco; nella fase di integrazione, i fondi riciclati vengono prelevati o utilizzati per transazioni legittime[208].

---

[205] Cfr. CHOO K.R., SMITH R.G., *Criminal Exploitation of Online Systems by Organised Crime Groups,* in *Asian Criminology*, 3, 2008, pp. 47-48.
[206] Cfr. SICURELLA S., *Le mafie italiane nel cyberspazio/ nuova frontiera o terreno di sperimentazione?*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, XVI, 2022, p. 25; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 102.
[207] In proposito cfr. DUMITRACHE A., MODIGA G., *New trends and perspectives in the money laundering process, in Challenges of the Knowledge Society*, 1, 2011, p. 55.
[208] Cfr. CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, cit., p. 281; cfr. anche CHOO K.R., SMITH R.G., *Criminal Exploitation of Online Systems by Organised Crime Groups,* cit., pp. 48-49.

Quanto ai metodi e alle tecniche impiegate per il riciclaggio del denaro attraverso i casinò, l'*International Financial Action Group* ne fornisce una esemplificativa elencazione.

In primo luogo, si ravvisano alcune tecniche che coinvolgono strumenti di valore dei casinò (denaro, fiches da casinò, crediti su macchine da gioco, certificati regalo), come la tecnica di "*chip dumping*"[209], consistente nel perdere intenzionalmente chips a favore di un altro giocatore a un tavolo di poker online per trasferire fondi in modo nascosto.

In secondo luogo, tra le tecniche di "*layering*", finalizzate a nascondere l'origine illecita dei fondi attraverso una serie di transazioni complesse e stratificate, si annoverano le scommesse coordinate; o ancora, la tecnica di "*gnoming*" o "*multiaccounting*"[210], ossia l'impiego di più account, c.d. "gnomi", per controllare il gioco: il criminale informatico prolifera il gioco utilizzando gli gnomi e fa perdere gli altri giocatori, piazzando tatticamente le mosse degli account falsi; infine, è un metodo altrettanto comune il favoreggiamento di dipendenti, come la falsificazione da parte dei dipendenti del casinò di valutazioni e altri registri che riguardano il giocatore al fine di giustificare l'accumulo di fiches o crediti da macchine da gioco[211].

Inoltre, recenti indagini hanno messo in evidenza l'adozione di strategie sofisticate da parte soprattutto delle organizzazioni mafiose nel settore delle scommesse online e del gioco d'azzardo legale. Un aspetto cruciale di queste attività illecite è l'uso delle tecnologie informatiche per manipolare le piattaforme di gioco, tra cui la manomissione delle schede elettroniche per disconnettere il collegamento con la rete dei Monopoli di Stato. Questa operazione consentiva di registrare un numero inferiore di giocate, evitando così il pagamento delle imposte, e alterava le percentuali di vincita, permettendo guadagni illeciti maggiori[212].

---

[209] Cfr. DUNCAN P., LORD N.*, Organized crime money laundering through online gambling businesses in Great Britain*, in *The Private Sector and Organized Crime*, Ed. ZABYELINA Y., THACHUK K, Routledge, London, New York, p. 9; LEVI M., *Money Laundering Risks And E-Gaming: A European Overview And Assessment*, in *Era Forum*, *Journal of the Academy of European law*, 10, 2010, pp. 543-546; WRONKA C., *"Cyber laundering": the change of money laundering in the digital age*, in *Journal of Money Laundering Control*, 25, 2, 2021, pp. 330-344.

[210] Cfr. United Nations Office on Drugs and Crimes, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*, 2024, p. 4.

[211] FAFT Report, *Vulnerabilities of Casinos and Gaming Sector*, 2009, p. 28, http://www fatf-gafi.org/dataoecd/47/49/42458373.pdf.

[212] Cfr. GRATTERI N., NICASO A., *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*, cit., par. VII "Gioco d'azzardo e scommesse online".

Oltre alla manipolazione delle schede, le organizzazioni mafiose hanno sfruttato le piattaforme di scommesse sportive online, gestendo siti illegali dislocati in Paesi esteri, senza concessioni per operare in Italia. Questi siti violavano le normative italiane, ma permettevano comunque ai giocatori di accedere e scommettere, eludendo i controlli statali[213].

Le operazioni di gioco illegale erano spesso organizzate tramite una rete di siti web non autorizzati, accessibili da apparecchiature installate in numerose sale da gioco italiane ed ubicati in Paesi come Stati Uniti e Romania, fuori dal controllo dei Monopoli di Stato, permettendo alle organizzazioni criminali di operare in modo indisturbato[214].

Un'altra strategia rilevante è la creazione di una struttura gerarchica, con vari livelli (National, Regional, District, Club), in cui i guadagni derivanti dal gioco online venivano distribuiti tramite carte prepagate o rimesse dirette in contante. I considerevoli profitti venivano temporaneamente trasferiti tramite circuiti finanziari internazionali per poi essere investiti in beni immobili, soprattutto in Italia[215].

A completamento di queste attività, le mafie ricorrevano anche alla falsificazione di documenti di gioco, stampando il logo dei Monopoli di Stato su ricevute e cedole per eludere i controlli e ingannare i giocatori. Questo ha reso il settore delle scommesse online un obiettivo primario per il riciclaggio di denaro e le violazioni fiscali, dato che la mancanza di tracciabilità rende le operazioni difficili da individuare e sanzionare.

La Commissione parlamentare antimafia ha sottolineato come le tecnologie informatiche abbiano facilitato l'ingresso delle mafie nel settore del gioco d'azzardo, consentendo loro di riciclare enormi somme di denaro in modo quasi invisibile, grazie alla difficoltà di accertare le condotte illegali e alla bassa entità delle pene previste[216].

Ne è la prova l'operazione “Gambling”, che ha evidenziato l'enorme giro d'affari legato al gioco d'azzardo illegale, con il sequestro di numerosi siti di gambling online, società estere e punti di raccolta scommesse in Italia, per un valore stimato di 2 miliardi di euro[217].

---

[213] *Ibidem.*
[214] *Ibidem.*
[215] *Ibidem.*
[216] Commissione parlamentare antimafia, *Relazione sulle infiltrazioni mafiose e criminali nel gioco*, 6 luglio 2016.
[217] Commissione parlamentare antimafia, *Relazione sulle infiltrazioni mafiose e criminali nel gioco*, 6 luglio 2016.

3.2.2.3. Il riciclaggio tramite money mules

Il fenomeno dei "muli di denaro" rappresenta una delle forme più insidiose di criminalità organizzata nel contesto delle nuove tecnologie e dell'economia digitale.

Con il termine "*money mule*" si fa riferimento ad una persona che riceve denaro, solitamente da una terza parte, sul proprio conto bancario, per poi trasferirlo a un altro conto o prelevarlo in contante per consegnarlo a qualcun altro, ricevendo, di consueto, una commissione per il servizio[218]. Questi individui, dunque, spesso inconsapevoli di essere coinvolti in attività illecite, fungono da "scudo" per i criminali, essendo più vulnerabili ad essere catturati e puniti.

Non a caso, il reclutamento dei muli di denaro avviene in molti casi attraverso tecniche persuasive, mirate a persone vulnerabili, sedotte da offerte di guadagni facili, come quelle che promettono lavoro da casa e commissioni per il trasferimento di fondi, un processo che può essere visto come una forma di "*grooming*". La vulnerabilità di questi soggetti, che può derivare da difficoltà finanziarie, isolamento sociale, mancanza di supporto familiare o bassa autostima, li rende dunque più inclini a cadere in trappola[219].

Le reti che sfruttano i muli di denaro fanno parte di un più ampio contesto di criminalità organizzata, spesso legato a traffici internazionali come il traffico di droga, il finanziamento del terrorismo, e altre forme di contrabbando[220].

Queste organizzazioni criminali, oltre a usare i muli per il riciclaggio del denaro, mantengono strutture aziendali sofisticate, come società di comodo in giurisdizioni offshore, e impiegano diverse tecniche per occultare il flusso di denaro illecito, come l'uso di bitcoin o di broker internazionali[221].

Non è raro poi che le reti di criminalità organizzata impieghino anche i forum online per reclutare specialisti oppure costruiscano la loro rete attraverso contatti sociali già

---

[218] Cfr. PICKLES R., *'Money Mules': Exploited Victims or Collaborators in Organised Crime?*, in *Irish Probation Journal*, 18, 2021, p. 232.
[219] *Ivi*, p. 238.
[220] Cfr. Europol, *Serious and Organised crime threat assessment, A Corrupting Influence: The Infiltration And Undermining Of Europe's Economy And Society By Organised Crime*, 2021, in *https://www.europol.europa.eu/publications-events/main-reports/socta-report*, p. 30.
[221] *Ibidem*.

esistenti offline[222]. In effetti, come si è detto, i legami sociali offline continuano a svolgere un ruolo cruciale nelle reti criminali informatiche[223].

Nel quadro delle attività delle organizzazioni criminali, i muli di denaro rappresentano una risorsa preziosa per i riciclatori di denaro, che gestiscono e trasferiscono i proventi illeciti senza attirare l'attenzione delle autorità[224].

Un aspetto cruciale di questo processo di riciclaggio è l'uso di strumenti tecnologici avanzati, come le "schede nere", carte di credito false o manipolate, utilizzate per camuffare le transazioni finanziarie illecite. Le schede nere vengono gestite da hacker specializzati, che sfruttano le vulnerabilità dei sistemi bancari per movimentare ingenti somme di denaro, eludendo i controlli finanziari e facendo scomparire le tracce delle transazioni. Questo sistema si avvale di una rete di complicità che coinvolge non solo i criminali informatici, ma anche direttori di banca e altre figure in grado di favorire la diffusione e il riciclaggio del denaro.

L'impiego di queste schede è stato ben ricostruito da Megna[225], il quale racconta di come sia stato possibile ricostruire un ampio schema di riciclaggio di denaro, operante tra diverse nazioni, dal Montenegro all'Inghilterra, passando per Parma, Milano e persino la Svezia[226]. Il cuore dell'operazione ruotava attorno alla gestione di queste schede nere da parte di hacker esperti, che avevano la capacità di fare sparire le tracce del denaro[227].

Megna, parlando con i suoi interlocutori, spiegava che grazie a questo sistema, le somme movimentate, che ammontavano a centinaia di milioni, venivano trasferite senza lasciare alcuna traccia visibile, grazie anche alla complicità tra gli stessi hacker e dei direttori di banca coinvolti, che si prendevano una percentuale sui guadagni[228].

Figure specializzate possono essere poi impiegate per operazioni di *cyber-laundering* attraverso l'utilizzo di altri strumenti. Si parla, in particolare, di "box", ovvero di conti correnti criptati che, non rientrando nella contabilità bancaria, risultano formalmente

---

[222] Cfr. CHOO K. R., *Organised crime groups in cyberspace a typology,* in *Trends in Organised crime*, 2008, p. 271; GRABOSKY P., *The Internet, Technology and Organised crime*, cit., p. 152.
[223] Sul punto v. LEUKFELDT, E. R., LAVORGNA A., KLEEMANS E. R., *Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, in *European Journal on Criminal Policy and Research*, 23, 3, 2017, p. 293.
[224] Cfr. CHOO K. R., *Organised crime groups in cyberspace a typology,* cit., p. 271.
[225] Mario Megna, nipote del boss di Papanice, frazione del comune di Crotone, intercettato dalla Procura di Catanzaro. Cfr. Procura della Repubblica presso il Tribunale di Catanzaro, richiesta di applicazione di misure cautelari personali nei confronti di A.N. + 122, pp. 3268-69.
[226] *Ibidem*.
[227] *Ivi*, p. 3285.
[228] *Ibidem*.

inesistenti, nonostante negli stessi vengano poi depositati ingenti somme di denaro. L'operazione di "scarico" consiste nel trasferire o svuotare i fondi contenuti in questi conti in modo fraudolento, senza lasciare tracce evidenti o segnali che possano attivare i sistemi di sicurezza bancari[229].

È indubbio, dunque, che queste operazioni su tali conti correnti non possano che avvenire con la collaborazione di alcune figure. Anzitutto, i funzionari di banca, in grado di fornire i codici di accesso, facilitando le transazioni sospette senza attivare le dovute verifiche antiriciclaggio[230]. In secondo luogo, lo scarico fraudolento del denaro deve comunque essere effettuato da una rete di hacker specializzati, che operano da postazioni remote, utilizzando tecniche sofisticate per accedere ai box senza far scattare allarmi nei sistemi informatici della banca. Una volta che gli hacker riescono a entrare nel box bancario, il passo successivo è svuotarlo, trasferendo i fondi in altri conti correnti e, dopo aver svuotato il box, il denaro viene trasferito attraverso una serie di transazioni bancarie che sono strutturate in modo da mascherare l'origine dei fondi[231].

Con riguardo al coinvolgimento degli istituti bancari nelle dinamiche di riciclaggio, importanti indicazioni provengono dalle dichiarazioni dei magistrati della Dda di Catanzaro, le quali hanno fatto emergere, a seguito del sequestro di un vademecum informatico nell'ambito dell'operazione Glicine Acheronte, un quadro particolarmente dettagliato delle modalità operative adottate. È stato evidenziato, in primo luogo, come il vantaggio per le banche consenzienti consista nella percezione di percentuali nettamente superiori a quelle del mercato legale, pari al 5% a fronte dello 0,01% normalmente praticato. Nel documento viene sottolineata altresì la necessità che l'istituto di credito "aderisca al gioco", accettando consapevolmente le condizioni imposte dall'organizzazione criminale. Per quanto concerne le transazioni, infine, esse si fondano sull'impiego di software e dispositivi non reperibili sul mercato comune e non forniti direttamente dalle banche, ma messi a disposizione da trader coinvolti, i quali si fanno

[229] *Ivi*, p. 3268. Le dichiarazioni di Giuseppe Antonio Mancuso sulle operazioni box sono tratte dall'ordinanza di custodia cautelare dell'operazione Glicine Acheronte.
[230] Cfr. GRATTERI N., NICASO A., *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*, cit., par. VIII "*Cyberlaundering*".
[231] *Ibidem.*

carico anche della predisposizione di documentazione bancaria di compliance falsificata allo scopo di giustificare le movimentazioni.[232]"

[232] Cfr. Procura della Repubblica presso il Tribunale di Catanzaro, richiesta di applicazione di misure cautelari personali nei confronti di A.N. + 122, 22 luglio 2022, pp. 3389-3390.

CAPITOLO IV

La migrazione digitale delle mafie: problematiche giuridiche e strategie di contrasto

SOMMARIO: **1.** Premessa – **2.** Continuità negli scopi, mutamento degli strumenti: la "migrazione digitale" della criminalità organizzata – **3.** I profili giuridici e le criticità applicative dei nuovi strumenti digitali al servizio del crimine – **3.1.** Comunicazioni criptate: ostacoli investigativi e processuali – **3.1.1.** La giurisprudenza precedente alle Sezioni Unite e le prime critiche dottrinali – **3.1.2.** La prospettiva europea: la posizione della Corte di Giustizia. – **3.1.3.** Il contributo delle Sezioni Unite: punti risolutivi e questioni aperte. – **3.2**. Criptovalute e riciclaggio digitale: opacità e sfide regolatorie. – **3.2.1.** De individualizzazione dell'azione criminosa. – **3.2.2.** Delocalizzazione dell'azione criminosa – **3.2.3.** Dematerializzazione dell'oggetto del reato – **3.3**. Il dark web tra investigazione tecnologica e vuoti normativi: criticità attuali – **4.** Prospettive di intervento e strategie di contrasto alle sfide della criminalità digitale – **4.1.** Verso un'armonizzazione sovranazionale della disciplina probatoria e della circolazione dei dati digitali – **4.2.** Prospettive di riforma normativa nella gestione processuale delle comunicazioni criptate – **4.3.** Nuove tecniche investigative digitali e crisi delle categorie probatorie tradizionali – **4.4.** Verso una regolazione integrata dei crypto-asset – **4.5.** Prospettive di riforma per una sistematizzazione penalistica del fenomeno delle criptoattività – **4.6**. Strumenti investigativi e nuove tecniche per il contrasto ai cripto-reati

1. Premessa

Il presente capitolo è dedicato all'analisi dei profili giuridici che emergono dall'interazione tra criminalità organizzata e tecnologie digitali, con l'obiettivo di esplorare le criticità normative, le tensioni interpretative e le possibili risposte offerte – o ancora da elaborare – dal sistema giuridico di fronte al mutamento della criminalità organizzata nell'era digitale.

Con riferimento al crimine organizzato tradizionale migrante nel *cyberspace*, alla luce della progressiva digitalizzazione di pratiche illecite consolidate, come il riciclaggio di denaro o il traffico di sostanze stupefacenti e del ricorso sempre più frequente a strumenti tecnologici avanzati – quali criptovalute, comunicazioni criptate, piattaforme digitali, software di anonimizzazione – si intende esaminare i profili di problematicità giuridica che questi strumenti pongono sia in sede investigativa, sia sul piano probatorio e

processuale. La domanda che sorregge questo primo asse di ricerca è, dunque, se e in che misura il sistema normativo attuale – nelle sue componenti sostanziali e processuali – sia dotato della necessaria elasticità e capacità adattiva per affrontare le sfide poste da una criminalità organizzata che si evolve tecnologicamente senza perdere i tratti fondamentali della sua natura associativa. In parallelo, si darà conto delle risposte già sperimentate o in corso di elaborazione, sia sul piano nazionale, sia a livello europeo e sovranazionale, evidenziando le strategie normative e operative attualmente introdotte per fronteggiare una criminalità sempre più digitalizzata.

2. Continuità negli scopi, mutamento degli strumenti: la "migrazione digitale" della criminalità organizzata

Un aspetto centrale nell'attuale riflessione sul rapporto tra criminalità organizzata e ambiente digitale è rappresentato dal fenomeno della migrazione online delle organizzazioni criminali tradizionali, che pur adattandosi ai nuovi strumenti tecnologici, mantengono intatte le proprie finalità e la propria struttura associativa di base.

Si tratta di un processo che non implica una trasformazione ontologica della criminalità organizzata, bensì una sua traslazione funzionale all'interno del cyberspazio, in risposta alle opportunità offerte dall'innovazione tecnologica.

Come osservano Choo e Smith[233], i gruppi mafiosi e le reti criminali consolidate ricorrono alle tecnologie dell'informazione e della comunicazione (ICT) principalmente per "*facilitare o potenziare*" le attività illecite già esistenti nel mondo reale, come il traffico di droga o il riciclaggio di denaro.

L'uso delle criptovalute, dei sistemi di comunicazione criptata, delle piattaforme di pagamento digitale e del dark web costituisce, dunque, un'evoluzione strumentale del *modus operandi* mafioso, non una sua ridefinizione sostanziale.

Anche Lavorgna evidenzia questa logica di continuità di scopi della criminalità organizzata tradizionale: solo alcune organizzazioni criminali tradizionali, e in particolare i cosiddetti "*migrated mafia groups*"[234], sembrano oggi in grado di sfruttare le opportunità

[233] CHOO K.R., SMITH R.G., *Criminal Exploitation of Online Systems by Organised Crime Groups*, cit., p. 39.
[234] Cfr. LAVORGNA A., *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?*, in *Narratives On Organised Crime In Europe Criminals, Corrupters & Policy*, cit.

offerte dalle ICT per portare avanti le proprie attività tradizionali. Tali soggetti integrano i nuovi strumenti nella propria strategia criminale, senza modificare la struttura gerarchica o gli obiettivi principali, che restano ancorati alla ricerca del profitto e al controllo delle economie illegali territoriali.

Questa dinamica adattiva, simile a quella delle imprese legali che si digitalizzano per restare competitive, è stata ricondotta da parte della dottrina al modello della *criminal enterprise*[235].

Tale modello propone una visione economica dell'organizzazione criminale, descrivendola come un'entità razionale e orientata al profitto, analoga sotto molti aspetti a un'impresa commerciale legale. Secondo questa prospettiva, il crimine organizzato si struttura e opera per massimizzare l'efficienza e garantire continuità all'offerta di beni e servizi illegali, sfruttando meccanismi di mercato simili a quelli del settore legittimo, sebbene adattati a un contesto privo di regole formali di tutela dei diritti[236].

In tale cornice teorica si colloca anche l'analisi proposta da Catino, per il quale, nonostante le differenze storiche e culturali, le principali organizzazioni mafiose condividono norme, strutture e problematiche gestionali con le imprese legittime. Analogamente a queste ultime, anche le mafie sono sottoposte alle stesse pressioni ambientali, tecnologiche[237], ed economiche, dettate, ad esempio, dalle limitazioni concorrenziali[238].

Nel caso della migrazione delle mafie nel cyberspazio, pare, infatti, che questa logica imprenditoriale trovi naturale applicazione: l'adozione delle tecnologie digitali risponde alla necessità di mantenere competitività e capacità operativa in un ambiente criminale in continua evoluzione. La criminalità organizzata, dunque, non si digitalizza per mutare la propria essenza, ma per ottimizzare tempi, risorse e modalità di azione: la tecnologia diventa un mezzo per aumentare il rendimento criminale, ridurre il rischio e ampliare il raggio d'azione transnazionale[239].

---

[235] *Ivi*, pp. 207 e ss.
[236] *Ibidem*.
[237] Cfr. CATINO M., *Mafia Organizations, The Visible Hand of Criminal Enterprise*, Cambridge University Press, 2019, p. 258.
[238] *Ivi*, p. 114.
[239] Cfr. LAVORGNA A., *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?*, cit., pp. 207 e ss.

Pertanto, la continuità degli scopi e il contestuale mutamento dei mezzi rispondono al simultaneo perseguimento da parte delle organizzazioni criminali tradizionali di una duplice strategia: una strategia di *exploitation*, ossia di valorizzazione delle risorse e competenze esistenti per ridurre i costi e consolidare il vantaggio competitivo, e una di *exploration*, ovvero di esplorazione di nuove configurazioni di risorse per accedere a mercati precedentemente preclusi[240].

L'approccio imprenditoriale consente anche di comprendere perché non tutte le organizzazioni criminali tradizionali abbiano effettivamente compiuto questa transizione: l'adozione delle ICT richiede risorse, competenze e un adeguato rapporto costi-benefici. Per Lavorgna, sono soprattutto i gruppi classificabili come "*mixed criminal networks"* o "*migrated mafia groups"* ad aver compiuto questa evoluzione, in quanto dotati della flessibilità necessaria per integrare strumenti digitali nella propria operatività[241].

Proprio in questa chiave va letta, ad esempio, l'adozione selettiva di strumenti digitali da parte delle mafie calabresi, che sfruttano le piattaforme digitali non solo per ragioni di sicurezza, ma anche come veri e propri strumenti di lavoro, commercializzati e testati internamente[242].

La tecnologia, in questa prospettiva, rafforza la resilienza organizzativa, la capacità di operare su scala transnazionale e l'adattamento ai mercati illeciti globali, senza alterare le gerarchie familiari, la cultura di clan o il controllo territoriale. Anche la maggiore fluidità organizzativa introdotta dalle tecnologie – in particolare nella comunicazione e nella logistica – non implica una smaterializzazione delle organizzazioni criminali. Anzi, come osservato in dottrina, la tecnologia ha permesso "*continuance and resilience of the groups*", mantenendo intatti i legami intergenerazionali e diasporici delle organizzazioni mafiose nel tempo e nello spazio[243].

Inoltre, nella logica imprenditoriale che sottende il modello della *criminal enterprise*, di cui si è detto, le organizzazioni criminali tradizionali non necessariamente acquisiscono internamente nuove competenze tecniche, ma, per efficienza, riservatezza e capacità di

---

[240] Cfr. CATINO M., *Mafia Organizations, The Visible Hand of Criminal Enterprise*, cit., p. 107.
[241] Cfr. LAVORGNA A., *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?*, cit., pp. 207 e ss.
[242] Cfr. LAVORGNA A., SERGI A., *Intergenerational and technological changes in mafia- type groups/ a transcultural research agenda to study the 'ndrangheta and its mobility*, cit., p. 2.
[243] *Ibidem*.

adattamento, tendono piuttosto a ricorrere a una logica di esternalizzazione funzionale: delegano all'esterno alcune attività altamente specializzate — come il riciclaggio di denaro, l'accesso a infrastrutture digitali sicure, o la consulenza finanziaria e legale — rivolgendosi, come già visto, a soggetti professionali reperibili sul mercato criminale o grigio[244].

Questa strategia organizzativa si fonda non solo su ragioni economiche, ma anche su considerazioni di sicurezza e compartimentazione. Come osserva Catino, l'esternalizzazione consente di interporre livelli di intermediazione tra il vertice dell'organizzazione e le attività operative più esposte, riducendo così i rischi di compromissione in caso di arresti o intercettazioni[245].

In un contesto caratterizzato da asset *specificity* e segretezza, le mafie tendono a internalizzare le funzioni di controllo e protezione, ma preferiscono delegare a soggetti esterni quei compiti che non richiedono l'appartenenza all'organizzazione. Tali soggetti, spesso legati da meri rapporti contrattuali, ricevono incarichi ben delimitati nel tempo e nello spazio e, in caso di arresto, dispongono solo di informazioni circoscritte, limitate alla propria fase operativa, riducendo così l'esposizione dell'intero network criminale[246].

In conclusione, come visto nel dettaglio nei precedenti capitoli, emerge con chiarezza come le organizzazioni criminali tradizionali non siano entità monolitiche o statiche, bensì strutture dotate di una notevole plasticità organizzativa, in grado di adattarsi ai mutamenti ambientali pur mantenendo salda la propria identità.

In particolare, esse si caratterizzano per un carattere polimorfico che consente loro di esibire, simultaneamente, sia tratti di conservazione che di adattamento: da un lato, si osserva una tendenza alla cristallizzazione della struttura interna, con un'organizzazione che permane ancorata a codici simbolici e normativi rigidi, volti a garantire la coesione interna e la riproduzione del potere, anche in chiave familiare o clanica; dall'altro, si evidenzia una marcata apertura verso l'esterno, che si traduce in una costante rimodulazione del *modus operandi* in risposta a mutamenti tecnologici, economici e repressivi[247].

---

[244] Cfr. CATINO M., *Mafia Organizations, The Visible Hand of Criminal Enterprise*, cit., 2019; EUROPOL, *Serious and Organised crime threat assessment, A Corrupting Influence: The Infiltration And Undermining Of Europe's Economy And Society By Organised Crime*, cit., p. 29.
[245] Cfr. CATINO M., *Mafia Organizations, The Visible Hand of Criminal Enterprise*, cit., 2019, p. 11.
[246] Cfr. CATINO M., *Mafia Organizations, The Visible Hand of Criminal Enterprise*, cit., 2019, pp. 104 ss.
[247] Sul punto v. SCIARRONE R., *Le mafie dalla società locale all'economia globale*, in *Meridiana*, 43, 2002.

3. I profili giuridici e le criticità applicative dei nuovi strumenti digitali al servizio del crimine

3.1. Comunicazioni criptate: ostacoli investigativi e processuali

Nel dibattito giurisprudenziale italiano sull'utilizzabilità delle comunicazioni criptate acquisite tramite ordine europeo di indagine (OEI), la giurisprudenza di legittimità si è occupata, tra il 2022 e il 2024, dei casi delle piattaforme EncroChat e SkyEcc, piattaforme che, nella loro diversità, presentano caratteristiche tecniche e modalità di infiltrazione sostanzialmente analoghe, così come analoghe appaiono le questioni giuridiche sollevate.

In particolare, l'utilizzo da parte delle autorità giudiziarie italiane di messaggi estratti da piattaforme come SkyEcc ed Encrochat, mediante operazioni di hacking condotte da autorità estere, ha sollevato complesse questioni relative alla loro utilizzabilità, legittimità e compatibilità con i diritti della difesa, soprattutto quando tali comunicazioni, raccolte inizialmente nell'ambito di procedimenti stranieri, sono state trasmesse in Italia attraverso l'ordine europeo di indagine[248].

Da qui sono sorti i principali nodi interpretativi su cui sia la dottrina sia la giurisprudenza, e da ultimo le Sezioni Unite, hanno avuto modo di pronunciarsi: la validità del ricorso all'OEI per l'acquisizione di dati già in possesso dell'autorità esecutiva; la qualificazione delle attività di decrittazione dei messaggi; le implicazioni sulla catena di custodia e sulla verifica difensiva delle prove informatiche.

3.1.1. La giurisprudenza precedente alle Sezioni Unite e le prime critiche dottrinali

Una prima questione giuridica, che ha fatto estremamente discutere la dottrina e la giurisprudenza, ha riguardato le modalità di acquisizione e utilizzo probatorio delle conversazioni cifrate, scambiate mediante applicazioni ad elevata protezione crittografica, qualora trasmesse da autorità straniere tramite ordine europeo di indagine (O.E.I.).

[248] Ad esempio, nel caso SkyEcc, le autorità italiane hanno richiesto alla Francia con OEI la trasmissione di questi dati attraverso un Ordine Europeo di Indagine (OEI), previsto dalla Direttiva 2014/41/UE e recepito in Italia con il d.lgs. n. 108/2017.

Il vero nodo problematico della questione attiene alla corretta qualificazione giuridica di tali dati, da cui dipende la disciplina applicabile e, dunque, l'utilizzabilità processuale.

Guardando, anzitutto, all'orientamento giurisprudenziale consolidatosi prima dell'intervento delle Sezioni Unite[249], le chat Sky-ECC non rientrerebbero nella categoria delle intercettazioni, né telefoniche né telematiche, disciplinate dagli artt. 266 e ss. c.p.p., perché difetterebbero di due requisiti imprescindibili tipicamente riconducibili al concetto giuridico di intercettazione: da un lato, il "flusso in tempo reale" delle comunicazioni; dall'altro, la "captazione occulta", cioè l'acquisizione clandestina e diretta della conversazione da parte dell'autorità inquirente.

Ne derivava, pertanto, che le conversazioni decifrate e successivamente salvate su supporti digitali da un'autorità giudiziaria estera avrebbero dovuto piuttosto qualificarsi come documenti informatici, ai sensi dell'art. 234-bis c.p.p.[250], in quanto contenuti statici, già registrati e archiviati, trasmessi su supporti fisici come CD-ROM e file digitali.

Tuttavia, considerare tale tipo di comunicazioni "già concluse", alla stregua di documenti, significa considerarle prove precostituite, formatesi al di fuori del procedimento[251]. In tal modo, secondo l'indirizzo richiamato, i dati trasmessi in Italia sarebbero stati perfettamente utilizzabili. Non solo per la natura "documentale" dei messaggi che, conformemente alla nozione delineata dalla Corte di Cassazione[252], riconosce come documento informatico qualsiasi rappresentazione comunicativa fissata su base digitale. Ma anche in virtù della presenza del consenso del legittimo titolare richiesto dall'art. 234-*bis* c.p.p.: nel caso di specie, sarebbe l'autorità giudiziaria francese — che ha legalmente acquisito e conservato i dati — ad avere validamente autorizzato il trasferimento verso l'Italia, esercitando la propria legittima disponibilità sul materiale probatorio.

Infine, a sostegno dell'utilizzabilità probatoria dei dati, vi sarebbero senza dubbio differenti principi fondamentali, primo tra tutti il principio di cooperazione giudiziaria

---

[249] Si consultino, ad esempio, le seguenti pronunce: Cass., sez.VI, 27 aprile 2020, n. 12975; Cass., sez. IV, 12 aprile 2023, n. 18523; Cass., sez. IV, 18 aprile 2023, n. 16347; nonché le ordinanze del Trib. Reggio Calabria, del 5 novembre 2022, n. 801 e del 19 novembre 2022, n. 868.

[250] In proposito, si vedano le seguenti pronunce, Cass. pen. sez. I, 13 ottobre 2022, n. 6363 e 6364; Cass. pen. sez. IV, 5 aprile 2023, n. 16347; Cass. pen. sez. IV, 4 aprile 2023, n. 18514.

[251] Cfr. DANIELE M., *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/ Encrochat in attesa delle Sezioni Unite*, in Sistema Penale, 2023.

[252] Cfr. Cass. pen. sez.I, 1luglio 2022, n. 34059, in *www.dejure.it*.

europea, che poggia a sua volta su pilastri normativi fondamentali, quali il mutuo riconoscimento degli atti, la fiducia reciproca tra Stati membri e il canone di diritto internazionale del *locus regit actum*, per cui la validità dell'atto va valutata in base alla legge dello Stato in cui l'atto viene compiuto e non quella del Paese richiedente.

Tale orientamento, pur consolidandosi in alcune pronunce di legittimità e di merito, non convince del tutto. La questione dell'utilizzabilità delle comunicazioni cifrate provenienti dalla piattaforma SkyEcc nel processo penale italiano solleva numerosi profili di criticità giuridica e costituzionale, che possono essere sistematicamente ricondotti alle seguenti categorie problematiche.

Già la prima questione, relativa alla qualificazione giuridica della messaggistica in esame come documento informatico ex art. 234-*bis* c.p.p. presenta delle criticità a fronte della struttura e della funzione di tali comunicazioni.

Sul punto, infatti, la Corte Costituzionale, con la sentenza n. 170 del 2023[253], ha statuito che le comunicazioni interpersonali — sincrone o asincrone — tra soggetti determinati, protette da sistemi crittografici avanzati, e spesso veicolanti contenuti di natura strettamente confidenziale, seppur rappresentazioni statiche di fatti, restano espressioni dinamiche del pensiero, rientranti a pieno titolo nella nozione di "corrispondenza" tutelata dall'art. 15 della Costituzione[254].

Ne consegue che la tutela costituzionale della corrispondenza non viene meno per il solo fatto che la comunicazione non è più "*in itinere*": finché il messaggio conserva una sua attualità ed è accessibile ai destinatari, permane la necessità di un intervento giudiziale motivato per qualsiasi forma di apprensione. Di conseguenza, qualificare tali dati come documenti informatici acquisibili senza le garanzie previste per le intercettazioni potrebbe, secondo parte della dottrina[255], rappresentare una finzione giuridica funzionale ad aggirare la disciplina più rigorosa prevista dagli artt. 254 e 266 e ss. c.p.p., con effetti pregiudizievoli per i diritti fondamentali dell'imputato.

La conseguenza, sul piano pratico, della "degradazione" di una comunicazione a semplice documento informatico, solo perché non più in transito, è quello di confinare

[253] Cfr. C. cost., 27 luglio 2023, n. 170, in *www.cortecostituzionale.it*.
[254] Ai sensi dell'art. 15 Cost., la loro limitazione potrà avvenire solo con atto motivato dell'autorità giudiziaria e con le forme e le garanzie stabilite dalla legge.
[255] In proposito si veda RAMPIONI M., *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, cit., 10, 2023.

l'art. 15 Cost. in un ambito applicativo sempre più ristretto**,** finendo per svuotarne la portata effettiva, specialmente in un contesto in cui la quasi totalità delle comunicazioni personali avviene tramite sistemi digitali istantanei. Non è detto, infatti, che le mail, i messaggi criptati o le chat, seppur recapitate, perdano così facilmente la loro natura di "corrispondenza", continuando invece a riflettere quella sfera privata e inviolabile che la Carta costituzionale intende presidiare con strumenti rigorosi, tra cui la riserva di legge e di giurisdizione**.**

È proprio in virtù della "*stretta attinenza della libertà e della segretezza della comunicazione al nucleo essenziale dei valori della personalità*"**,** come afferma la stessa Corte, che la protezione costituzionale va interpretata in senso estensivo e rafforzato**.** Così, l'art. 15 Cost. non sarebbe ridotto a mera clausola formale, ma si estenderebbe, piuttosto, al contenuto delle conversazioni, e anche ai cosiddetti dati esteriori delle stesse (ad esempio, i tabulati telefonici, già ritenuti coperti da garanzia costituzionale).

Non a caso, - prosegue la Corte **-** se i dati esteriori di una comunicazione (quali quelli contenuti nei tabulati) godono della copertura dell'art. 15 Cost.**,** *a fortiori* deve ritenersi tutelato in modo pieno anche il contenuto dei messaggi elettronici, anche se già recapitati, avendo l'acquisizione di questi ultimi una portata ancor più intrusiva se si consente di accedere non solo all'identità dei corrispondenti, ma anche al contenuto effettivo delle conversazioni, con ricadute gravi sul diritto alla riservatezza.

Sulla scia tracciata dalla Consulta, si inserisce anche parte della giurisprudenza di legittimità[256], secondo cui l'oggetto dell'acquisizione all'estero della messaggistica criptata sulla piattaforma SkyEcc non costituisce dato informatico, bensì vero e proprio flusso comunicativo. Si distingue, così, tra l'ipotesi in cui oggetto dell'attività di acquisizione siano comunicazioni avvenute nella fase "dinamica"[257], caso nel quale opererebbe la disciplina delle intercettazioni telematiche ex artt. 266 e ss. c.p.p.; dall'altra ipotesi, in cui oggetto della criptazione sarebbero, invece, comunicazioni avvenute nella fase "statica", a cui invece si applicherebbero le disposizioni in materia di perquisizione e sequestro di cui all'art. 254 c.p.p.

Altro punto critico riguarda l'identificazione del "legittimo titolare" del dato, il cui consenso è condizione necessaria per l'utilizzabilità ex art. 234-*bis* c.p.p.

---

[256] Sul punto cfr. Cass., sez.VI, 2 novembre 2023, n. 44154 e sez. IV, 26 ottobre 2023, n. 44155.

[257] Si tratta, secondo la pronuncia di cui sopra, n. 44154 del 2023 con fase "dinamica" si intende la captazione di comunicazioni telefoniche, ambientali o di flussi telematici in corso.

Secondo parte della giurisprudenza[258], tale ruolo sarebbe validamente esercitato dall'autorità giudiziaria estera che dispone dei dati – nel caso specifico, quella francese, - poiché avendo svolto una attività investigativa autonoma per l'acquisizione dei dati, sarebbe legittimata a disporne nel contesto della cooperazione giudiziaria.

Secondo tale interpretazione, il legittimo titolare all'acquisizione, richiesto dall'art. 234-*bis* sarebbe la "*persona giuridica che di quei documenti o di quei dati poteva disporre in forza di un legittimo titolo secondo l'ordinamento giuridico del paese estero, identificabile non soltanto nella persona fisica e/o giuridica che procede alla trasmissione e alla conservazione dei dati, ma anche nella polizia giudiziaria, nell'autorità giudiziaria, nella persona offesa, nell'amministrazione pubblica, nella società che gestisce il servizio telefonico, nell'Internet service provider*"[259].

Tuttavia, la conseguenza problematica di tale lettura sarebbe la dilatazione del concetto di "legittimo titolare" a chiunque detenga materialmente il dato, a prescindere dalla sua titolarità originaria[260].

Occorre evidenziare, infine, come SkyEcc fornisca agli utenti delle sim-card che non permettono l'identificazione diretta dei titolari, ma che, utilizzando la rete telefonica convenzionale, lasciano comunque tracce tecniche – come i codici IMSI e IMEI – quando si collegano alle celle telefoniche. Questi cosiddetti "dati esteriori di comunicazione", pur non rivelando il contenuto dei messaggi, consentono di risalire a informazioni molto personali, come i luoghi frequentati, gli orari e i dispositivi utilizzati, rendendoli particolarmente sensibili. Le autorità italiane hanno utilizzato questi dati, incrociandoli con i messaggi decodificati forniti dalla magistratura francese, per identificare i soggetti coinvolti nell'uso di dispositivi SkyEcc.

Tuttavia, tale modalità di acquisizione solleva problemi di compatibilità sia con l'articolo 15 della Costituzione italiana – che tutela la segretezza anche dei dati esterni delle comunicazioni – sia con la giurisprudenza europea, che negli ultimi anni ha adottato una linea più rigorosa. In particolare, la Corte di Giustizia dell'Unione Europea, nella

---

[258] Cfr. ad esempio Cass., sez. IV, 18 aprile 2023, n. 16347, secondo cui, se per consenso deve intendersi l'assenso proveniente dal soggetto legittimato a disporre dei documenti o dei dati, la presenza di tale requisito – in alternativa all'ipotesi in cui si tratti di documenti di pubblico dominio – legittima pienamente l'acquisizione diretta della documentazione all'estero; diversamente, in assenza di tale consenso, si sarebbe reso necessario il ricorso alle procedure di cooperazione giudiziaria internazionale.

[259] Così Cass., sez. I, 15 febbraio 2023, n. 6364; Cass., sez. I ,1 luglio 2022 ,n. 3405.

[260] Cfr. RAMPIONI M., *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, cit.

sentenza del 2021[261], ha stabilito che l'accesso ai dati di traffico e localizzazione deve essere strettamente limitato a casi di criminalità grave o di minacce gravi alla sicurezza pubblica. Inoltre, tale accesso deve essere autorizzato da un'autorità giudiziaria o amministrativa indipendente, e non può essere generalizzato o indiscriminato.

Nel caso SkyEcc, invece, molte delle comunicazioni risultano essere state acquisite e conservate senza un'autorizzazione specifica o senza la presenza di una notizia di reato: infatti, i provvedimenti autorizzativi emessi dai giudici francesi riguardavano solo una parte dei dati raccolti, rimanendo scoperta una enorme parte di messaggi da una verifica selettiva, e non essendo stata effettuata alcuna cancellazione dei dati non autorizzati, come richiesto dalla normativa comunitaria[262].

3.1.2. La prospettiva europea: la posizione della Corte di Giustizia

La vicenda giudiziaria connessa all'utilizzo nel processo penale dei dati intercettati attraverso le piattaforme in esame e, in particolare, nel caso di cui si dirà, attraverso la piattaforma EncroChat, ha generato un importante contenzioso anche a livello europeo, culminato nella sentenza della Corte di Giustizia dell'Unione Europea del 30 aprile 2024 (causa C-670/22).

Come per SkyEcc, anche in questo caso, le autorità francesi, mediante un'operazione di hacking massiva, avevano acquisito una grande mole di dati criptati da dispositivi utilizzati da utenti EncroChat, tra cui soggetti localizzati in Germania. Furono proprio le autorità tedesche, una volta ricevuti i dati tramite ordine europeo di indagine (OEI), a dichiararli inammissibili da un punto di vista probatorio. In particolare, il Tribunale Regionale di Berlino sollevava dubbi sulla legittimità dell'OEI tedesco, emesso dalla Procura per acquisire la totalità dei dati EncroChat relativi agli utenti in Germania, senza una preventiva individualizzazione dei soggetti sospettati; in secondo luogo, risultava

---

[261] Cfr. Corte di giustizia dell'Unione europea, sentenza 2 marzo 2021, H.K. c. Prokuratuur, C-746/18. Nella citata sentenza Corte ha affermato che la direttiva 2009/136/CE, letta alla luce degli artt. 7, 8, 11 e 52, par. 1, della Carta dei diritti fondamentali dell'Unione Europea, si oppone a normative nazionali che consentano l'accesso ai dati relativi al traffico o alla localizzazione degli utenti in modo generalizzato o non sufficientemente delimitato. Tali dati, idonei a rivelare informazioni significative sulle comunicazioni e sulla posizione delle apparecchiature utilizzate, possono essere acquisiti legittimamente solo nell'ambito di indagini relative a forme particolarmente gravi di criminalità o per prevenire gravi minacce alla sicurezza pubblica.

[262] Cfr. RAMPIONI M., *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, cit.

controversa la compatibilità dell'OEI con il diritto tedesco laddove emesso senza autorizzazione giudiziale; infine, veniva messa in dubbio la compatibilità con il diritto di difesa, stante l'impossibilità di quest'ultima di accedere ad atti e dati fondamentali, rendendo difficile contestarne validità, integrità e rilevanza[263].

Contrariamente alla visione delle autorità tedesche, invece, il parere presentato il 26 ottobre 2023 dall'Avvocato Generale della CGUE[264] riteneva legittimamente ammissibili i dati acquisiti tramite l'OEI da parte delle autorità tedesche, sulla base del principio di mutuo riconoscimento: i dati ottenuti in origine dagli investigatori francesi, già autorizzati dalle autorità giudiziarie francesi, non avrebbero potuto dunque essere rimessi in discussione da parte dello Stato richiedente, se non a fronte di specifiche violazioni[265].

Nella menzionata sentenza del 30 aprile 2024, la CGUE ha poi confermato che l'emissione di un OEI volto alla trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione non richiede necessariamente l'intervento di un giudice, purché l'atto possa essere disposto anche da un pubblico ministero secondo il diritto interno dello Stato di emissione[266]. In altre parole, secondo l'interpretazione della Corte di Giustizia, nulla osta a che un pubblico ministero adotti un OEI volto alla trasmissione di prove ottenute mediante intercettazioni di comunicazioni cifrate, come quelle operate su EncroChat, a condizione che siano rispettate le condizioni previste dal diritto dello Stato di emissione per un caso interno analogo.

Infine, quanto al diritto di difesa, si consente al giudice nazionale di espungere dal procedimento le prove acquisite tramite OEI, se la persona indagata non ha potuto

---

[263] La domanda di pronuncia pregiudiziale verteva sull'interpretazione dell'articolo 2, lettera c) (sul concetto di "autorità di emissione" dell'OEI, dell'articolo 6, paragrafo 1 (le condizioni di emissione e trasmissione di un OEI da parte dell'autorità di emissione), e dell'articolo 31 (notifica allo Stato membro nel quale si trova la persona soggetta a intercettazione e la cui assistenza tecnica non è necessaria) della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale, nonché sui principi di equivalenza e di effettività.

[264] Conclusioni dell'Avvocato Generale Ćapeta: un pubblico ministero può emettere un ordine europeo di indagine (OEI) diretto al trasferimento di prove già raccolte in un altro Stato membro, cfr. comunicato stampa n. 163/23, Corte di Giustizia dell'Unione europea, in curia.europa.eu

[265] Cfr. GUAGLIARDI G., *Utilizzo nel processo penale di messaggi criptati ottenuti tramite una operazione di hacking massiva all'estero e acquisiti in Italia tramite Ordine Europeo di Indagine. Il fine giustifica i mezzi?*, in *Giurisprudenza Penale*, 6, 2024, p. 38; La Redazione diritto e giustizia, *EncroChat e procedimenti penali transfrontalieri: la CGUE precisa le condizioni per la trasmissione e l'utilizzo delle prove*, in *Diritto e Giustizia*, 2024; LIGUORI F., *Il principio di mutuo riconoscimento nell'ambito della cooperazione giudiziaria in materia penale: le condizioni di ammissibilità dell'Ordine europeo di indagine penale*, in *Quaderni AISDUE - Rivista quadrimestrale*, 1, 2024.

[266] *Ibidem*.

esercitare pienamente il diritto di difesa rispetto a esse e se tali elementi incidono in modo determinante sull'esito del processo.

Con tale decisione la Corte andava dunque a risolvere alcune opacità segnalate, come l'assenza di trasparenza sulle modalità tecniche usate per l'hacking che comprometteva l'integrità dei dati, o il rifiuto delle autorità di fornire alla difesa documenti essenziali del fascicolo in contrasto con il principio del contraddittorio[267].

D'altro canto, tuttavia, la Corte pare non attribuire di per sé rilevanza decisiva al fatto che una prova sia stata acquisita in violazione di legge dello Stato richiedente, conferendo invece sostanziale rilevanza ad eventuali violazioni delle garanzie difensive fondamentali di quello Stato[268].

3.1.3. Il contributo delle Sezioni Unite: punti risolutivi e questioni aperte

Al fine di risolvere le criticità fin qui esaminate, le Sezioni Unite sono intervenute con due sentenze gemelle emesse il 14 giugno 2024[269], pronunciandosi sulle varie questioni controverse.

Circa la natura giuridica dell'acquisizione di chat cifrate da parte di autorità estera, le Sezioni Unite si sono pronunciate per chiarire se i messaggi cifrati su SkyEcc, decrittati da un'autorità giudiziaria estera e trasmessi in Italia, dovessero essere considerati dati informatici (art. 234-bis c.p.p.) o documenti (art. 234 c.p.p.), o se dovessero essere ricondotti ad altre modalità di acquisizione della prova.

Le S.U. hanno escluso che tale operazione di acquisizione rientrasse nell'ambito dell'art. 234-*bis* c.p.p., inquadrandola invece come acquisizione di "atti di altro procedimento penale", disciplinata – a seconda dei casi – dagli artt. 78 disp. att., 238 o 270 c.p.p. Non si trattava, dunque, né di mera prova documentale, né di dati informatici ai sensi dell'art. 234-bis c.p.p., bensì di atti già formati in un altro procedimento penale estero, trasmessi in Italia tramite cooperazione giudiziaria[270].

Le Sezioni Unite decidono di fare riferimento alla disciplina dettata dall'art. 78 disp. att. c.p.p. relativo all'acquisizione della "documentazione di atti di un procedimento

---

[267] *Ibidem*.
[268] Sul *punto* cfr. LORENZETTO E., *Il caso Encrochat e l'ordine europeo di indagine penale nella staffetta fra Corte di Giustizia e diritto dello stato di emissione*, in *Cass. pen.*, 9, 2024, pp. 2887-2897.
[269] S.U. penali, 14 giugno 2024, n. 23755 e n. 23756.
[270] Sent. sopra citata, n. 23756, p. 15, par. 3 e p. 36, par. 12.2; sent. sopra citata, n. 23755, p. 29, par. 9.2.

penale compiuti da autorità giudiziaria straniera", poiché ritengono che, nel caso di specie, non rilevino tanto le regole di "formazione" della prova – essendo questa già formata - , quanto quelle sulla "circolazione" della stessa fra procedimenti diversi[271].

Ne derivava, pertanto, che in base all'interpretazione fornita dalla Corte di cassazione, nei casi in cui si fosse trattato di acquisire in Italia prove già raccolte all'estero, le uniche norme rilevanti in materia probatoria sarebbero state quelle contenute nell'art. 238 c.p.p., richiamato dall'art. 78 disp. att. c.p.p.; laddove, invece, le prove fossero consistite in intercettazioni di comunicazioni, la disciplina applicabile sarebbe state quella di cui all'art. 270 c.p.p. Quest'ultima disposizione, pur non essendo espressamente menzionata, risulta comunque applicabile in forza della coerenza sistematica e della *ratio* dell'art. 78 disp. att. c.p.p[272].

Veniva precisato, infatti, come l'ambito di operatività dell'art. 234-*bis* c.p.p. fosse circoscritto all'acquisizione di particolari tipologie di elementi di prova presenti all'estero e rimessa direttamente all'autorità giudiziaria procedente, non estendendosi, invece, all'acquisizione di elementi di prova "transfrontalieri", realizzata tramite la collaborazione tra autorità giudiziarie di Stati diversi[273].

In secondo luogo, in ordine all'utilizzabilità delle prove e alla necessità di un controllo di legittimità, alternativamente, preventivo o successivo, da parte dell'autorità giudiziaria italiana, le Sezioni Unite, pur escludendo la necessità di una verifica preventiva da parte dello Stato di emissione dell'OEI, reputavano comunque imprescindibile che fosse garantito il rispetto dei diritti fondamentali previsti da quello Stato, con particolare riferimento al diritto di difesa e di un equo processo[274].

Di per sé, poi, nulla osta a che il giudice dello Stato di emissione svolga un controllo giurisdizionale *ex post* sulle prove già raccolte all'estero. Le principali perplessità, tuttavia, non sorgevano nella presenza o meno di tale controllo, quanto intorno ai suoi limiti, dovendosi svolgere tale verifica alla luce delle norme che regolano l'utilizzabilità delle prove nei procedimenti interni.

Sul punto, le considerazioni delle Sezioni Unite non sono state poi così limpide considerando che se, da un lato, l'utilizzabilità del contenuto di comunicazioni scambiate

---

[271] Sent. n. 23755, p. 28, par. 9.2.
[272] Cfr. DANIELE M., *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*, in *Sistema penale*, 2024.
[273] Sent. n. 23755, p. 20, par. 6.1.
[274] Sent. n. 23755, p. 33, par. 11.3.

tramite criptofonini avrebbe dovuto essere esclusa qualora il giudice italiano avesse accertato una violazione dei diritti fondamentali[275], dall'altro lato, tuttavia, le Sezioni ritenevano esistente una "presunzione relativa" di conformità ai diritti fondamentali delle attività istruttorie svolte dalle autorità giudiziarie degli altri Stati membri, addossando, in tal modo, in capo alla difesa che avesse voluto eccepire l'inutilizzabilità, l'onere di prova di un'eventuale violazione dei diritti fondamentali.

Proseguivano, poi, le Sezioni Unite negando la necessità in capo al pubblico ministero italiano di un'autorizzazione da parte del giudice finalizzata alla richiesta dell'OEI per la trasmissione delle intercettazioni già eseguite all'estero, fermo restando, tuttavia, il rispetto dei diritti fondamentali previsti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione europea.

Ciò veniva consentito in quanto, secondo quanto condiviso anche dai giudici della Corte di Giustizia sul caso Encrochat[276], il pubblico ministero figurerebbe tra le autorità competenti a emettere OEI ai sensi dell'art. 2 lett.c) della relativa direttiva n. 41 del 2014[277], a condizione che, secondo il diritto dello Stato di emissione, in un procedimento interno analogo, la raccolta di tali prove potesse essere ordinata dal pubblico ministero stesso.

Infine, sulla eventuale violazione del diritto di difesa potenzialmente causata dalla mancata conoscenza da parte della difesa dell'algoritmo usato per la decriptazione dei messaggi dal Paese di provenienza, le Sezioni hanno manifestato parere negativo. Vale a dire, non hanno ritenuto necessario che la difesa avesse accesso all'algoritmo usato dall'autorità giudiziaria estera per decrittare i messaggi cifrati considerando, invece, la correttezza della decrittazione *in re ipsa*: secondo la Corte, non ci sarebbe margine di manipolazioni perché, se l'algoritmo usato fosse sbagliato, il testo stesso non sarebbe intellegibile. In altri termini, se la decrittazione produce un testo leggibile, allora si presume che sia anche autentico e corretto.

Tale posizione, tuttavia, non è stata esente da critiche e ha suscitato forti perplessità sotto il profilo delle garanzie difensive del contraddittorio e dell'attendibilità della prova,

[275] Cfr. sent. n. 23755 del 2024, p. 38, par. 13.
[276] Corte giust., 30 aprile 2024, *M.N.*, C-670/22, par. 69 ss.
[277] Si tratta della Direttiva del Parlamento e del Consiglio europeo, relativa all'ordine di indagine europeo, e trasposta nel nostro ordinamento con d.lgs. n. 108 del 2017.

pilastri fondamentali del giusto processo[278]. Posto che il principio della parità delle armi postula che la difesa abbia accesso agli stessi strumenti conoscitivi dell'accusa, compresa dunque la fonte tecnica della prova, l'affidamento incondizionato ed insindacabile della difesa ad una procedura tecnica di tale natura, che pertanto preclude la verifica di eventuali errori, manipolazioni o limiti tecnici della decriptazione, implica l'accettazione acritica di una prova dalla "genesi ignota"[279].

All'impossibilità per la difesa di accedere ai file originali e ai software impiegati per la decriptazione[280], consegue una rottura nella catena di custodia del dato informatico. Il trattamento dei dati criptati (dalla raccolta all'analisi) segue una catena di conservazione che, se corretta e tracciabile, rappresenta il "processo di produzione del risultato": nello specifico, i dati intercettati vengono conservati come "dati grezzi", non immediatamente leggibili, e da questi dati, tramite elaborazione informatica, si ricavano i brogliacci che riportano in maniera chiara i contenuti delle chat. È proprio il processo di trasformazione dal dato grezzo a quello leggibile che risulta oscuro alla difesa[281].

La tracciabilità sarebbe dunque minata nel caso in cui l'intero processo di trasposizione del dato, da grezzo a probatorio, si svolgesse senza il controllo delle parti interessate[282]. Attraverso la delega di tali operazioni di decodifica a soggetti terzi che utilizzano strumentazioni informatiche non accessibili alla giurisdizione italiana si avrebbe dunque un affidamento cieco a fonti esterne[283].

Secondo parte della dottrina, infatti, le operazioni di decrittazione, in quanto operazioni complesse, andrebbero trattate alla stregua di accertamenti tecnici non ripetibili ai sensi dell'art. 360 c.p.p. Tuttavia, nella prassi, ciò non avviene: né vi è avviso all'indagato né possibilità di nominare un consulente tecnico, negandosi in tal modo le garanzie difensive previste per la prova scientifica[284].

---

[278] Cfr. GAITO A., *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC),* in *Archivio Penale*, 1, 2024, p. 6; PUJIA P., *L'acquisizione della messaggistica criptata conservata su server straniero tra classificazioni concettuali e divergenze giurisprudenziali*, cit., p. 18.
[279] Cfr. FILIPPI L., *Criptofonini SKY- ECC e messaggi criptati: la Corte di cassazione attua i principi di diritto enunciati dalle Sezioni Unite*, in *Penale Diritto e Procedura*, 11 aprile 2024.
[280] Cfr. GAITO A., *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC),* cit., p. 4
[281] *Ivi,* p. 10.
[282] *Ibidem*, secondo cui "*la mancata disponibilità di tale programma ha, in concreto, impedito di poter ripercorrere il processo di produzione del risultato non consentendo la tracciabilità [...] della catena di conservazione del dato*."
[283] *Ivi*, p. 4.
[284] Ivi, p. 13.

D'altra parte, altro nodo, non meno irrilevante, lasciato aperto dalle Sezioni Unite riguarda l'ambiguità giuridica dell'attività investigativa estera. Infatti, pare ci sia stato un disinteresse sulla natura dell'attività di indagine "a monte", quella che aveva consentito l'originaria infiltrazione nella piattaforma criptata[285].

Da ultimo, ulteriore questione irrisolta riguarda le condizioni di legittimità per l'emissione dell'ordine europeo di indagine, in particolare sotto i profili della necessità, proporzionalità ed equivalenza. La Corte sembra accogliere, senza particolari riserve, la possibilità che l'autorità giudiziaria italiana possa acquisire e utilizzare dati ottenuti da piattaforme criptate, anche quando la captazione estera riguardi interi flussi comunicativi, senza specifica selezione dei destinatari e in assenza di una preventiva valutazione individuale della rilevanza probatoria. È evidente, dunque, che un'acquisizione di dati, tanto vasta e non circoscritta, non soddisfi a pieno i criteri di stretta necessità, come invece richiesto dalla Direttiva 2014/41/UE e dalla giurisprudenza della Corte di Giustizia dell'Unione Europea[286].

A ciò si aggiungono significative perplessità sulla conformità al principio di equivalenza, che impone di rispettare le stesse condizioni di legge previste nello Stato di emissione per atti analoghi. Per quest'ultima valutazione, l'esatta qualificazione giuridica dell'attività di captazione svolta all'estero diventa centrale: se si tratta di intercettazione, allora dovrebbe essere sottoposta alle stesse garanzie richieste per le intercettazioni telematiche in Italia, inclusa l'autorizzazione giudiziaria. Tuttavia, l'attività estera appare caratterizzata da una natura ibrida, che sfugge alle classificazioni tradizionali: una combinazione di intercettazione, sequestro, acquisizione di documenti e corrispondenza, ottenuta tramite l'impiego di strumenti informatici invasivi come i *trojan*[287].

Il punto critico, pertanto, non è soltanto tecnico-giuridico, ma tocca direttamente il principio di legalità nella formazione e nella circolazione della prova. L'assenza di una normativa chiara che disciplini come ed entro quali limiti possano essere svolte attività investigative tanto invasive genera un evidente squilibrio tra efficienza investigativa e tutela dei diritti fondamentali. Il ricorso a tecniche di intrusione profonda, non

[285] Cfr. MURRO O, NOCERINO W., *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini*, in *Penale Diritto e Procedura*, 2024.
[286] *Ibidem*.
[287] *Ibidem*.

espressamente tipizzate, rischia dunque di collocarsi fuori dal perimetro della legalità processuale, rendendo vulnerabile l'intero sistema delle garanzie[288].

3.2. Criptovalute e riciclaggio digitale: opacità e sfide regolatorie

Come anticipato, lo sviluppo delle tecnologie digitali e la progressiva diffusione delle monete virtuali hanno profondamente influenzato le dinamiche economico-finanziarie della società contemporanea. In particolare, gli strumenti di scambio alternativi alla moneta legale, per quanto concepiti per finalità lecite e innovative, si sono rivelati suscettibili di utilizzo illecito poiché funzionali alla commissione di reati, prevalentemente di tipo economico-finanziario.

È indubbio, infatti, che determinate peculiarità delle criptovalute – quali l'anonimato, la decentralizzazione, la dematerializzazione – favoriscano l'impiego di tali monete per operazioni di riciclaggio di denaro, autoriciclaggio, frodi informatiche o trasferimenti illeciti di fondi, di cui si è ampiamente parlato.

È peraltro inevitabile che tali fenomeni mettano in crisi, sul piano dogmatico e sistematico, la disciplina giuridico-normativa e, sotto vari profili, anche il diritto penale. Si ravvisano, in proposito, diverse problematiche concernenti la qualificazione giuridica del bene oggetto di tutela, l'individuazione dell'autore del reato, la definizione di *locus commissi delicti.*

Tali questioni saranno, pertanto, analizzate nel dettaglio di seguito, attraverso l'esame delle criticità giuridiche derivanti dall'utilizzo illecito delle criptovalute, sino alla individuazione delle risposte normative e giurisprudenziali formulate a livello nazionale e sovranazionale.

3.2.1. De-individualizzazione dell'azione criminosa

Uno degli effetti più significativi dell'impiego delle criptovalute nel contesto della criminalità economica è la progressiva de-individualizzazione dell'azione criminosa, che

[288] *Ibidem*.

inevitabilmente incide profondamente sulle categorie classiche del diritto penale, segnatamente quelle relative all'individuazione del soggetto agente del reato.

La combinazione tra dinamiche economiche globali, progresso tecnologico e applicazioni crittografiche, rese possibili dalla blockchain e dalle criptovalute, ha contribuito alla nascita di nuove forme di illegalità che sfuggono al controllo sociale e ai tradizionali strumenti giuridici di qualificazione e repressione del reato.

In particolare, la crittografia asimmetrica tipica dei trasferimenti di criptovalute ha spinto al limite il processo di anonimizzazione delle condotte illecite, determinando una vera e propria de-individualizzazione dell'autore, così come i nodi della Blockchain hanno compromesso la struttura classica dell'azione penalisticamente intesa, obbligando il diritto criminale "a fare i conti con gli invisibili"[289].

Si registra un'indistinta opacità dell'autore del reato, spesso mascherato da pseudonimi digitali o nascosto dietro complessi sistemi informatici, che rende sempre più sfumato il legame tra soggetto e condotta, e quindi tra azione e responsabilità. In tale scenario, "il diritto penale non tratta più dell'autore che entra in un conflitto personale con la vittima o con la società", ma reagisce a "processi disfunzionali[290]".

Stante dunque la crescente difficoltà di identificazione del soggetto attivo del reato e la conseguente dissociazione tra operatore e operazione, risultano compromessi i presupposti classici dell'imputazione penale: l'azione illecita perde così i suoi tradizionali riferimenti soggettivi, rendendo problematica, se non impossibile, la riconduzione dell'evento a un soggetto penalmente responsabile[291].

3.2.2. Delocalizzazione dell'azione criminosa

Nel contesto delle criptovalute, e dei reati commessi attraverso le stesse, il fenomeno del *forum shopping*, volto all'individuazione del luogo dove instaurare il giudizio in caso di più fori astrattamente competenti per una determinata controversia, rappresenta una delle principali criticità sul piano dell'accertamento giurisdizionale.

Come già ampiamente riferito, le criptovalute hanno natura intrinsecamente transnazionale, operando senza vincoli territoriali, attraverso reti decentralizzate e spesso

[289] Cfr. NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, in *Penale Diritto e Procedura*, 2022, p. 2.
[290] VOLK K., *Criminalità organizzata e criminalità economica*, cit., pp. 364 ss.
[291] Cfr. PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio,* cit., p. 605.

distribuite su server ubicati in più Stati. Ciò rende estremamente complessa la determinazione del foro competente a conoscere il reato.

Altri fattori complicano ulteriormente il quadro: la difficoltà nel determinare chi possa essere convenuto in giudizio, l'incertezza dello status giuridico delle criptovalute nelle diverse giurisdizioni, la complessità nell'individuazione della legge applicabile[292].

Ad aggravare il problema del forum shopping vi è indubbiamente la possibilità tecnica, insita nell'uso delle criptovalute, di frammentare le operazioni illecite in una pluralità di atti esecutivi distribuiti nel tempo e nello spazio, sfruttando la completa ubiquità operativa offerta dalle tecnologie digitali. Il cyberspazio, infatti, consente l'esecuzione di transazioni da qualunque luogo e in qualunque momento, impedendo la localizzazione geografica dell'agente o dei server coinvolti. In questo modo, l'agente criminale può deliberatamente pianificare le proprie operazioni, in modo da coinvolgere ordinamenti giuridici differenti, dando così luogo al fenomeno del *forum shopping*[293].

Sul fronte giuridico, ciò comporta, da un lato, un'incertezza nella determinazione del *locus commissi delicti* e, dall'altro, la concreta possibilità che più giurisdizioni si contendano, o al contrario trascurino, l'esercizio dell'azione penale. Il fenomeno del *forum shopping* mina, pertanto, i principi della certezza e della prevedibilità dell'azione penale, dal momento che va a paralizzare o frammentare l'azione repressiva creando conflitti di competenza o stalli processuali[294].

3.2.3. Dematerializzazione dell'oggetto del reato

Ulteriore fattore destabilizzante per le categorie tradizionali del diritto penale e processuale è la dematerializzazione che caratterizza le criptovalute.

In questo caso, quando si parla di "dematerializzazione" non si fa riferimento ad un'avvenuta conversione digitale di entità precedentemente materiali (come avviene con i documenti cartacei o con il denaro fisico), bensì ad una realtà fisiologicamente fondata sull'immaterialità: le criptovalute sono nativamente dematerializzate, vale a dire che per

[292] Cfr. DAMAP N.Y., MAZA K. D., *Jurisdictional Challenges in Cryptocurrency Disputes: Navigating the Legal Maze of a Borderless Technology*, 17, 1, 2025.
[293] Cfr. NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, in Penale Diritto e Procedura, 2022, p. 2; POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, cit., pp. 164 ss.
[294] *Ibidem*.

natura questo tipo di monete non possono esistere nella realtà materiale, né essere manualmente trasferite, se non tramite rete internet[295].

Questa caratteristica ontologica incide direttamente sull'inquadramento giuridico dei fatti commessi tramite criptovalute, essendo messa in discussione la configurabilità dell'oggetto materiale del reato.

La giurisprudenza e la dottrina si interrogano, ad esempio, sulla controversa qualificazione dei Bitcoin nell'ambito della nozione penalistica di "denaro" o di "bene", presente nei reati di riciclaggio e reimpiego di cui, rispettivamente, agli artt. 648-*bis* e *ter* del codice penale[296].

La tesi oggi prevalente tende a escludere l'assimilabilità delle criptovalute al denaro, in assenza di corso legale e di un formale riconoscimento da parte dello Stato[297].

Tuttavia, l'ampia formulazione delle fattispecie incriminatrici, che ricomprendono anche ogni "altra utilità", viene in soccorso nel caso di specie, consentendo di includere nel novero dei possibili oggetti materiali del reato quelle entità, diverse dal denaro, dotate di valore economico apprezzabile e, dunque, suscettibili di essere impiegate in attività di trasferimento, sostituzione e occultamento di proventi illeciti[298].

Ad ulteriore rafforzamento di questa interpretazione estensiva, si pone l'art. 810 c.c. secondo cui "sono beni le cose che possono formare oggetto di diritti", potendosi ricomprendere nella nozione di "bene", non solo quello materiale, ma anche quello immateriale. Pertanto, non può escludersi che la valuta virtuale rientri in quest'ultima

---

[295] Cfr. LIVI A., *I diversi settori del FinTech - Problemi e prospettive*, (a cura di) CORAPI E., LENER R., Wolters Kluwer, Cedam, Università degli studi di Roma "Tor Vergata", Collana pubblicazioni Facoltà di Giurisprudenza - Dipartimenti di Diritto Privato e di Diritto Pubblico, Terza serie, 2019, pag. 118.

[296] Art. 648-*bis* c.p., Riciclaggio: «Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto, 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 5.000 a 25.000 euro [...]».
Art. 648-*ter* c.p., Impiego di denaro, beni o utilità di provenienza illecita: «Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da 5.000 a 25.000 euro [...]».

[297] Cfr. DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, in *Diritto penale contemporaneo*, 10, 2018, p. 41; anche BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. inf*., 2017, 1, pp. 29 ss. il quale ritiene che le tre funzioni tipicamente associate alla moneta, ovvero quella di riserva di valore, unità di conto e mezzo di scambio, non siano assolte dalla moneta virtuale. A suo avviso, la volatilità del Bitcoin ne impedirebbe l'uso come riserva di valore; la mancanza di controllo statale e la necessità di un accordo tra le parti ne limiterebbero l'efficacia come mezzo di scambio; infine, l'instabilità del mercato dei cambi ne comprometterebbe l'unità di conto.

[298] Cfr. DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, cit., p. 41.

categoria, sebbene parte della dottrina si opponga a tale estensione considerando a numero chiuso il novero dei beni immateriali[299].

Sul fronte processuale, la dematerializzazione della moneta ha dei riflessi significativi sul piano dell'accertamento del reato e della formazione della prova. La tradizionale impostazione probatoria, infatti, fondata sull'esistenza fisica dell'oggetto del reato, si scontra con una realtà priva di beni tangibili e tracciabili con strumenti convenzionali, potendosi basare l'investigazione unicamente su transazioni di blockchain, indirizzi virtuali e dati informatici[300].

3.3.Il dark web tra investigazione tecnologica e vuoti normativi: criticità attuali

Come visto, anche l'emersione del dark web, quale infrastruttura digitale sotterranea, ha fatto sì che una significativa parte delle attività illecite della criminalità organizzata migrassero in ambienti opachi, frammentati e tecnologicamente protetti.

Se infatti, in passato, l'azione penale contava su coordinate territoriali definite e su strumenti di indagine tradizionali, ad oggi, invece, ciò non accade vista la conversione dell'azione criminale ai mercati illeciti decentralizzati, alle transazioni anonime e alle identità irrintracciabili.

In questo contesto, il diritto penale non può che confrontarsi con sfide sistemiche: dalla crisi del principio di territorialità, di cui si è già detto, alla vulnerabilità della prova digitale.

Nell'ambito del dark web, uno degli ostacoli più rilevanti per il diritto penale è certamente l'anonimato garantito dalle architetture crittografiche avanzate.

La tracciabilità delle comunicazioni è alterata dall'utilizzo di particolari reti, come Tor, che applicano un sistema a cipolla in cui il traffico di dati viene cifrato a ogni nodo[301]. Il risultato è la separazione sistemica tra identità e attività che priva l'indagine penale degli

---

[299] *Ibidem*.

[300] Cfr. LUPARIA L., *Computer crimes e procedimento penale,* in *Trattato di Procedura penale*, *Modelli differenziati di accertamento*, a cura di Garuti G., VII, I, Torino, 2011., pp. 369 – 386 ss.

[301] Per un approfondimento sul funzionamento delle reti di *onion routing* e, più in generale, sulle darknet, con particolare riguardo al ruolo che esse svolgono nel garantire l'anonimato delle comunicazioni, alla conseguente attrattività per fenomeni criminali quali traffico di sostanze stupefacenti, frodi e attività di hacking, nonché alle difficoltà riscontrate nell'attività di individuazione e contrasto da parte delle autorità competenti, v. KAREEM K.M., *Cybersecurity in Onion Routing Environments: Strategies to Thwart Cyber Threats,* in *Journal Of High-Frequency Communication Technologies*, 2024.

indicatori tradizionali come l'indirizzo IP, il log d'accesso, i metadati di rete[302]. Si tratta di un fenomeno che la dottrina definisce come "*formidable attribution challenges*", facendo riferimento alla difficoltà da parte delle autorità investigative di individuare e collegare con certezza un'attività criminale ad un soggetto specifico a causa di barriere tecniche, giuridiche ed operative[303].

Sebbene questi sistemi fossero stati concepiti in origine a tutela della privacy e della libertà di espressione, ad oggi rappresentano, dunque, dei sistemi di offuscamento della responsabilità penale. In questo modo, le attività delle organizzazioni criminali operano coperte da un velo tecnologico a plurimi livelli, protette dunque da una forma di invisibilità giuridica[304].

La migrazione delle attività delle organizzazioni criminali sul dark web e sui mercati illeciti digitali presenta, inoltre, un'ulteriore sfida per il diritto.

Il diritto penale infatti è per sua natura legato al principio di territorialità, secondo cui la legge applicabile fa riferimento ai limiti spaziali dello Stato che l'ha emanata. I crimini commessi nel dark web, e in generale nei mercati illegali digitali, sfuggono tuttavia a tali limiti, manifestandosi attraverso azioni distribuite su più giurisdizioni[305]. Si rileva, in particolare, la tendenza dei marketplace illegali a localizzare server e nodi critici in stati con minori capacità di enforcement o quadri normativi più deboli[306].

In uno scenario simile, l'individuazione della giurisdizione competente viene messa in crisi e, purtroppo, le procedure di cooperazione giudiziaria che dovrebbero soccorrere tale vuoto, si rivelano lente, frammentarie e spesso inefficaci[307].

A ciò si aggiunge, poi, il contesto normativo disomogeneo da cui il fenomeno del *cybercrime* che si sviluppa sul dark web trae vantaggio. Vale a dire, che l'eterogeneità di

---

[302] Cfr. SHEKHAWAT KS., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*, disponibile in Academia EDU, p. 3.
[303] *Ibidem*.
[304] Cfr. SINGH J., AHLUWALIA J.K., *Dark Web And Cybercrime: Challenges In Legal Enforcement*, in *Tijer international research journal*, 12, 4, 2025.
[305] *Ibidem*.
[306] Cfr. SHEKHAWAT KS., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*cit., p. 3, dove l'Autore parla di "*weaker enforcement capabilities or legal frameworks*" per riferirsi, da un lato, a capacità ridotte delle autorità competenti nell'attuare e far rispettare le norme — ad esempio a causa di scarse risorse investigative, mancanza di strumenti tecnologici adeguati o insufficiente cooperazione internazionale — e, dall'altro, a quadri normativi meno solidi o non aggiornati, che risultano inadeguati a disciplinare efficacemente fenomeni criminali complessi come quelli che si sviluppano nelle darknet.
[307] *Ibidem*.

approcci di prevenzione e contrasto diversi tra gli Stati - talvolta anche contrastanti rispetto alla tipizzazione delle condotte, alla soglia di offensività, alla responsabilità degli intermediari, alla disciplina della prova digitale - non può che produrre effetti distorsivi[308].

Sul fronte processuale, nel contesto dei reati commessi sul dark web, la prova digitale rappresenta spesso l'unica fonte probatoria disponibile, ma si rivela al contempo estremamente vulnerabile sotto il profilo dell'ammissibilità processuale. Ciò in quanto le evidenze informatiche sono caratterizzate da maggiore volatilità, possono essere facilmente alterate, cancellate o manipolate, richiedendo di conseguenza che sia rispettata rigorosamente la catena di custodia e che siano definite specificamente le regole tecniche di acquisizione. In mancanza di un protocollo probatorio armonizzato - sia a livello interno che internazionale - anche l'accertamento della responsabilità penale si espone al rischio elevato che le indagini si interrompano in un punto morto, non per assenza di colpevolezza, ma per mancanza di strumenti tecnici e giuridici idonei a garantire la prova secondo i canoni dell'equo processo[309].

Per quanto concerne gli strumenti legali tradizionali e le ordinarie misure di *enforcement* - come il sequestro di domini o ordini di rimozione dei contenuti -, anche questi si rivelano inadeguati, per cui occorrerebbe sostituirli con delle procedure forensi *ad hoc* di tipo avanzato che tuttavia sollevano questioni di proporzionalità e tutela delle garanzie difensive[310].

Infatti, a fronte dell'inefficacia dei metodi tradizionali, fondati ad esempio sull'acquisizione di dati tramite soggetti terzi o tracciamento degli indirizzi IP - vari stati, in particolare negli Stati Uniti, scelgono di adottare strumenti tecnologici altamente invasivi noti come "*network investigative techniques"* che, nella sostanza, non sono altro che operazioni di hacking statale legittimato mirate all'infiltrazione occulta nei dispositivi elettronici sospettati di essere impiegati per attività criminali. In particolare, tali tecniche

---

[308] Cfr. SINGH J., AHLUWALIA J.K., *Dark Web And Cybercrime: Challenges In Legal Enforcement*, cit.

[309] *Ibidem*; per un'analisi delle problematiche legate all'uso delle prove digitali (digital evidence) nei processi relativi a reati sul dark web, evidenziando le difficoltà di garantire trasparenza e ammissibilità, il ruolo degli algoritmi di profilazione nella fase investigativa e la necessità di giustificare al giudice i metodi utilizzati per raccogliere le prove, si veda European Commission, *Policing the Dark Web: Ethical and Legal Issues,* Horizon 2020 Framework Programme of the European Union, Ref. Ares, 2019, 1666154 - 13/03/2019.

[310] Cfr. SHEKHAWAT KS., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*, cit., p. 3.

prevedono l'installazione remota di malware sui computer bersaglio, in assenza del consenso e della consapevolezza dell'utente; ciò consente agli investigatori di avere il controllo da remoto del dispositivo, raccoglierne le informazioni in tempo reale, disporre dell'accesso ai file e ai dati memorizzati e, in taluni casi, persino di attivare microfoni webcam per sorveglianza audio-video. Attraverso questi strumenti i limiti derivanti dall'anonimato della rete Tor vengono in parte raggirati, dal momento che non è necessario più localizzare il soggetto, essendo sufficiente che quest'ultimo interagisca con il contenuto controllato dagli investigatori per attivare automaticamente l'esecuzione del malware.

Se, da un lato, l'impiego di queste tecniche rappresenta una modalità decisiva per ridurre il divario investigativo generato dalle tecnologie di anonimizzazione, dall'altro lato, non può negarsi come tali strumenti sollevino però interrogativi giuridici non indifferenti: si tratta, infatti, di tecniche che vanno ad alterare la configurazione tradizionale degli strumenti investigativi e a mettere in crisi una pluralità di diritti fondamentali, tra cui la riservatezza delle comunicazioni, la libertà personale e la tutela dei dati sensibili[311].

L'adozione di queste nuove tecniche investigative da parte del singolo Stato comporta, peraltro, un'estensione senza precedenti della sua stessa giurisdizione: gli strumenti di hacking statale operano infatti senza limiti territoriali e vanno a colpire i dispositivi situati in paesi stranieri sulla base di un mandato statale, senza che tale espansione extraterritoriale sia accompagnata da un controllo normativo o da accordi multilaterali, risultando così in una minaccia per il principio della sovranità degli Stati[312].

Un ulteriore ostacolo processuale è senza dubbio rappresentato dalla carenza strutturale di personale qualificato a svolgere le indagini sul dark web. Questo tipo di investigazioni, infatti, richiede competenze avanzate in analisi forense digitale, blockchain forensics, deanonimizzazione, data recovery. Purtroppo, si rileva un deficit di competenze specialistiche all'interno delle forze dell'ordine e delle procure che comporta

---

311 Cfr. GHAPPOUR A., *Searching Places Unknown/ Law Enforcement Jurisdiction on the Dark Web*, Stanford Law review 69, 4, 2017, p. 1097.

312 *Ivi*, p. 1081; quanto alla compatibilità tra i diritti sulla privacy e di difesa con le "remote forensics", ovvero tecniche informatiche invasive che permettono alle forze di polizia di accedere da remoto ai dispositivi digitali, conducendo attività investigative direttamente dal computer, senza che l'indagato ne sia consapevole, si veda VACIAGO G., *Remote forensics and cloudcomputing: an italian and european legal overview*, in *Digital evidence and electronic signature law review*, 8, 2011, pp. 124 ss.

un'inevitabile dipendenza da soggetti esterni come aziende private specializzate o unità di polizia internazionale, che rallentano i tempi dell'azione penale. Non solo. La scarsa formazione tecnica mina anche la capacità di identificare le condotte penalmente rilevanti nell'ambito di ecosistemi digitali così dinamici e complessi[313].

Sotto il profilo normativo, il diritto si dimostra ancora strutturalmente inadeguato a fronteggiare la velocità con cui le tecnologie emergenti si evolvono e modificano di conseguenza anche le modalità esecutive dei reati. Si registra, dunque, un divario crescente tra prassi criminale e fattispecie incriminatrici. Ogni avanzamento investigativo, inoltre, viene rapidamente neutralizzato da aggiornamenti di rete e dalla continua e sempre più costante decentralizzazione dei marketplace, registrandosi un ritardo normativo cronico: le leggi vengono sempre più formulate su presupposti tecnici che però si rivelano già superati[314].

Tali lacune normative non solo ostacolano l'incriminazione tempestiva di nuove condotte, ma mettono in crisi anche il principio di legalità, dal momento che la difficoltà di inquadrare comportamenti nuovi all'interno di fattispecie incriminatrici adeguate può dar luogo a vuoti sanzionatori, oltre che ad interpretazioni analogiche lesive delle garanzie dell'imputato[315]. Inoltre, l'assenza di un diritto penale sovranazionale genera spazi normativi eterogenei nei quali gli attori criminali vanno a selezionare le giurisdizioni più permissive o meno attrezzate: probabile, infatti, che finché persisteranno approcci nazionali divergenti, anche la deterrenza rimarrà asimmetrica, consentendo la migrazione di attività illecite verso "*safe heavens*" legislativi[316].

---

[313] Cfr. SINGH J., AHLUWALIA J.K., *Dark Web And Cybercrime: Challenges In Legal Enforcement*, cit.; v. anche KAREEM K.M., *Cybersecurity in Onion Routing Environments: Strategies to Thwart Cyber Threats,* cit., p. 175.
[314] Cfr. SHEKHAWAT KS., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*, cit.
[315] Cfr. SINGH J., AHLUWALIA J.K., *Dark Web And Cybercrime: Challenges In Legal Enforcement*, cit.
[316] Cfr. SHEKHAWAT KS., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*, cit.

4. Prospettive di intervento e strategie di contrasto alle sfide della criminalità digitale

4.1. Verso un'armonizzazione sovranazionale della disciplina probatoria e della circolazione dei dati digitali

Le divergenze normative tra gli ordinamenti europei riguardano, come visto, non solo i presupposti giuridici per l'accesso ai dati, ma anche le modalità tecniche ed operative di raccolta degli stessi, nonché le garanzie del contraddittorio che permettano alla difesa di verificare la genuinità e l'integrità dei dati.

In questo quadro, è dunque auspicabile un intervento del legislatore che preveda una normativa uniforme e coerente in materia di circolazione di dati digitali tra Stati membri.

Infatti, l'assenza di un *corpus* comune europeo in materia probatoria pone l'operatore giuridico di fronte ad un paradosso: si riporrebbe totale affidamento verso atti investigativi formatisi sulla base di parametri ignoti e non controllabili secondo gli standard nazionali. Non basta, infatti, che l'atto probatorio sia "astrattamente previsto" da entrambi gli ordinamenti, ma occorre che le modalità concrete con cui è stato acquisito e trasmesso siano effettivamente compatibili con il modello di giusto processo previsto a livello nazionale e sovranazionale[317].

Segnatamente, appare imprescindibile un processo di armonizzazione sovranazionale che miri a superare le lacune della direttiva 2014/41 sull'ordine europeo di indagine e che incida, soprattutto, su quegli strumenti cooperativi europei che, seppur pensati per facilitare le indagini penali oltre i confini nazionali, si trasformano in concreto in mezzi di aggiramento delle garanzie processuali previste in ciascun ordinamento[318].

A questo proposito, il tradizionale modello di assistenza giudiziaria - di consueto basato su una logica di collaborazione occasionale fra Stati - appare strutturalmente inadeguato sul piano operativo e sistemico: considerata, infatti, la complessità delle indagini digitali e l'impiego sempre più frequente di piattaforme cifrate e tecniche di acquisizione massiva di dati, occorrerebbe un'evoluzione concettuale e normativa che porti al superamento dell'idea di "assistenza" tra Stati a favore invece di una

---

[317] Cfr. LIGUORI F., *Il principio di mutuo riconoscimento nell'ambito della cooperazione giudiziaria in materia penale: le condizioni di ammissibilità dell'Ordine europeo di indagine penale*, cit..

[318] Cfr. MURRO O, NOCERINO W., *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini*, cit.

"cooperazione" tra Stati, paritaria, e fondata su principi comuni. In altre parole, siffatta cooperazione dovrebbe fondarsi su una visione funzionale della cooperazione giudiziaria, non potendo quest'ultima consistere in una semplice facilitazione tecnica dello scambio di prove tra Stati, ma dovendo bensì aspirare alla costruzione di uno *ius commune* europeo in materia di prova penale, che vada a bilanciare l'efficacia degli strumenti investigativi con il rispetto dei diritti fondamentali[319].

In questo senso, occorre ribadire che instaurare una fiducia tra autorità giudiziarie europee non vuol dire lasciare spazio ad automatismi nel riconoscimento della prova in virtù di una cooperazione solo astratta che acceleri i procedimenti, e colmi, solo all'apparenza, le lacune operative degli ordinamenti nazionali. Il ruolo del giudice nazionale non può essere infatti ridotto a semplice ricevitore passivo di prove prodotte altrove, dovendo invece mantenere una funzione attiva di filtro costituzionale verificando che l'atto straniero non sia in contrasto con il nucleo di diritti fondamentali, tra cui il diritto di difesa e il principio del giusto processo.

Si tratta, pertanto, di ripensare all'intero assetto della cooperazione penale in chiave sistemica riconoscendo che la fiducia reciproca tra Stati può reggere solo se effettivamente fondata su regole comuni, certe e condivise[320].

4.2. Prospettive di riforma normativa nella gestione processuale delle comunicazioni criptate

Le strategie di contrasto all'impiego criminale delle piattaforme di comunicazione criptate si sono fondate su un adattamento forzato degli strumenti investigativi esistenti, senza una riformulazione sistematica della cornice normativa.

I più recenti contributi dottrinali mettono in luce l'urgenza di un aggiornamento normativo che coinvolga in particolare tre ambiti complementari: la regolazione

---

[319] Cfr. RAMPIONI M., *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, cit., pp. 7-8; per una panoramica sulla cooperazione giudiziaria europea, con un particolare focus sull'ordine europeo di indagine, si veda ERTOLA F., *L'ordine europeo di indagine penale,* in *Trattato di Procedura penale*, XLIV.3, diretto da Ubertis G. e Voena G.P., Giuffrè, 2025; quanto, invece, ai limiti della cooperazione giudiziaria europea cfr. MONTALDO S., *I limiti della cooperazione in materia penale nell'Unione europea*, Editoriale scientifica Napoli, 2015.
[320] Cfr. RAMPIONI M., *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali,* cit., pp. 7-8.

amministrativa delle piattaforme; la tipizzazione processuale delle tecniche investigative e l'armonizzazione del diritto europeo sulla prova digitale.

Una prima proposta prevede un intervento normativo sul piano amministrativo e regolatorio, attraverso la modifica del Codice delle comunicazioni elettroniche[321], finalizzato a definire un sistema autorizzativo vincolante che identifichi espressamente quali piattaforme possano legittimamente offrire servizi di comunicazioni cifrata sul territorio nazionale[322].

In particolare, la creazione di un registro ufficiale delle piattaforme certificate rappresenterebbe uno strumento utile per distinguere gli operatori conformi, ovvero vincolati a standard di trasparenza e collaborazione investigativa, da quelli che invece offrono servizi dalla finalità chiaramente elusiva o criminogena. In questo senso, tali piattaforme avrebbero l'obbligo di inserire nei propri sistemi dei protocolli tecnici di "accessibilità condizionata", vale a dire si aprono alla possibilità di fornire alle autorità giudiziarie munite di provvedimento motivato dati identificativi e metadati che ricolleghino le comunicazioni a soggetti determinati[323].

Sul piano processuale, emerge la necessità di introdurre nel codice di procedura penale una nuova fattispecie di mezzo di ricerca della prova che sia specificamente dedicata alla sorveglianza digitale e all'acquisizione remota di dati cifrati. Considerato che, ad oggi, le tecniche impiegate per l'accesso alle comunicazioni criptate, come i trojan di Stato o le operazioni di decodifica con software forensi, sono inquadrate, in maniera non ancora del tutto chiara, nell'ambito di categorie già esistenti, come quella delle intercettazioni o del sequestro informatico o dell'accertamento tecnico irripetibile, altrettanto sfumate appaiono di conseguenza le garanzie applicabili. Ne consegue la proposta di costruire delle norme processuali *ad hoc* con l'obiettivo di sottrarre queste attività investigative ad ogni automatismo operativo, riducendo il rischio di captazioni arbitrarie e non documentate, in virtù della riserva di legge e di giurisdizione[324].

---

[321] D. lgs. 1 agosto 2003, n. 259, con ultima modifica risalente al d.lgs. 24 marzo 2024, n. 48.

[322] Cfr. MURRO O, NOCERINO W., *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini*, cit..

[323] *Ibidem*. Ad oggi, esiste un registro ufficiale gestito dall'ANAC che elenca le piattaforme di approvvigionamento digitale certificate utilizzare nel settore degli appalti pubblici, ma non esiste un registro analogo specifico per le piattaforme di comunicazioni criptate.

[324] Cfr. sempre MURRO O, NOCERINO W., *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini*, cit.; una verifica sulla compatibilità delle investigazioni esperite sulle piattaforme criptate con le categorie probatorie già esistenti viene svolta da CURTOTTI D., RIZZI V., NOCERINO W., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e prova penale*, cit., pp. 173 ss.

Le proposte dottrinali si spingono anche su un terreno europeo ed internazionale.

Al centro delle questioni dibattute si colloca certamente l'ordine europeo di indagine che, come visto, sebbene sia ispirato al principio di mutuo riconoscimento, difetta ancora di una valutazione sostanziale sulle modalità di acquisizione della prova da parte dello Stato richiedente[325].

La valutazione del giudice emittente si limita infatti a verificare che l'atto richiesto sia previsto dal proprio ordinamento, senza tuttavia vagliare la legittimità delle specifiche modalità esecutive dell'estrazione dei dati all'estero. Da qui, la proposta di riformulare in senso estensivo il principio di proporzionalità contenuto nell'art. 6 della Direttiva sull'ordine europeo di indagine, prevedendo che l'ordine europeo di indagine possa essere emesso solo se le modalità concrete di acquisizione della prova all'estero siano compatibili con le garanzie del processo penale interno. Sarebbe a questo fine necessaria una modifica interpretativa e auspicabilmente normativa della direttiva[326].

Altra dottrina si muove in direzione analoga, proponendo un riassetto del bilanciamento tra esigenze investigative e diritti fondamentali fondato su parametri di origine internazionale: esplicitamente richiama i principi della Corte Edu in materia di corrispondenza privata (art. 8) e il principio di parità delle armi (art. 47), suggerendo che la prova digitale possa essere ritenuta ammissibile non solo alla luce della sua rilevanza, ma anche alla luce della "necessità democratica dell'ingerenza", intesa come la capacità dello Stato di giustificare l'intrusione sulla base di criteri rigorosi di idoneità, proporzionalità e sussidiarietà. Per tali ragioni, è necessario che l'ordinamento si doti di una disciplina specifica per l'acquisizione, conservazione e utilizzo di dati digitali cifrati, con l'obbligo di conservare il dato originario, nonché la descrizione tecnica delle operazioni di decrittazione e l'obbligo di assistenza difensiva nelle fasi non ripetibili. Solo in presenza di questi elementi sarebbe preservato il principio del contraddittorio anche nei confronti di una prova scientifica complessa[327].

---

[325] In proposito, si veda LIGUORI F., *Il principio di mutuo riconoscimento nell'ambito della cooperazione giudiziaria in materia penale: le condizioni di ammissibilità dell'Ordine europeo di indagine penale*, in *Quaderni AISDUE - Rivista quadrimestrale*, 1, 2024.

[326] Cfr. LIGUORI F., *Il principio di mutuo riconoscimento nell'ambito della cooperazione giudiziaria in materia penale: le condizioni di ammissibilità dell'Ordine europeo di indagine penale*, cit.

[327] Cfr. GAITO A., *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC),* cit., p. 6; sul bilanciamento tra digitalizzazione e giusto processo si veda PRETATTO R. *Digitalizzazione e giusto processo: la digital evidence nella giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *DPCE online*, 1, 2024, p. 721 ss.; FLOR R., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in Diritto penale contemporaneo, 2012.

4.3. Nuove tecniche investigative digitali e crisi delle categorie probatorie tradizionali

In ultima analisi, la disciplina delle nuove tecniche investigative digitali potrebbe destare preoccupazioni nel prossimo futuro qualora le autorità giudiziarie e di polizia saranno chiamate a svolgere un ruolo attivo operando direttamente sui server e sui dati localizzati anche all'interno del territorio nazionale. Tale scenario rende urgente un ripensamento delle categorie probatorie tradizionali, rivelatesi inadeguate a disciplinare fenomeni sempre più tecnologicamente avanzati.

Come detto, l'utilizzo di strumenti come i criptofonini, i trojan e le piattaforme criptate, ha determinato una profonda metamorfosi nelle modalità di acquisizione della prova.

Non essendo ipotizzabile né rimettere alla discrezionalità degli inquirenti la scelta di ricorrere in maniera indiscriminata a nuovi strumenti investigativi, né legittimarne l'uso tramite interpretazioni giurisprudenziali estensive, si impone un intervento sistematico e consapevole del legislatore per tipizzare il complesso delle attività esperibili tramite inedite tecniche investigative.

Sul punto, la giurisprudenza appare ancora ancorata a categorie formali obsolete, tanto da far emergere quella che viene definita dalla dottrina una "tirannia" delle categorie giuridiche desuete[328].

Ne risultano degli evidenti effetti distorsivi, poiché mezzi probatori tecnologicamente similari vengono sottoposti a discipline differenti. Si pensi, ad esempio, alla disparità di trattamento tra intercettazioni informatiche – soggette a rigorosa autorizzazione giudiziaria – e altri strumenti più invasivi, come le video riprese nei luoghi riservati o le perquisizioni digitali, per le quali invece appare sufficiente un decreto motivato del pubblico ministero[329].

È dunque evidente l'esistenza di una asimmetria, frutto dell'inerzia del legislatore, che ha lasciato irrisolto il tema della proporzionalità e della necessaria graduazione delle

---

[328] Cfr. NICOLICCHIA F., *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla querelle giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero*, in *Sistema Penale*, 2, 2024.

[329] Cfr. DANIELE M., *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Processo penale e giustizia*, 5, 2018, p. 832.

garanzie a seconda del livello di intrusività dello strumento impiegato. La disciplina introdotta con il d.lgs. 216 del 2017 incarna pienamente tale problematica: nonostante si affermi di voler limitare l'impiego dei *trojan* ai soli reati gravi, la norma ne consente tuttavia l'uso pressoché generalizzato nei procedimenti per reati distrettuali, categoria ampia e non sempre omogenea, che nella prassi si traduce in un impiego potenzialmente illimitato dello strumento. Inoltre, le condizioni operative richieste dalla norma risultano facilmente eludibili a causa delle difficoltà tecniche nella geolocalizzazione e nell'attivazione selettiva del dispositivo[330].

Altrettanto allarmante è il vuoto normativo che riguarda le perquisizioni online, ovvero le operazioni mediante le quali, attraverso software come *trojan*, le autorità accedono da remoto all'intero contenuto di un sistema informatico, potendone captare flussi, password, dati in entrata e in uscita. Anche in questo caso risulta complesso, in assenza di una base legale esplicita, inquadrare tali operazioni altamente invasive negli schemi normativi esistenti, tanto da doversi qualificare secondo parte della dottrina come giuridicamente inesistenti[331].

A livello sovranazionale, il quadro è ancora più critico visto che le attuali regole di cooperazione giudiziaria non sono adeguate ad evitare che le prove digitali raccolte all'estero eludano le tutele previste dai vari ordinamenti nazionali. In questi casi, la tradizionale distinzione tra *lex loci* e *lex fori*[332] si dissolve dando vita ad un vuoto normativo in cui il regime applicabile alla raccolta della prova diventa imprevedibile: in particolare, come si è detto il rischio risiede nell'applicazione esclusiva della legge dello Stato che materialmente esegue l'acquisizione della prova, indipendentemente dai requisiti di legalità e proporzionalità previsti dall'ordinamento nel quale i dati si trovano[333].

A fronte di queste criticità risulta sempre più condivisibile la proposta di superare le categorie formali classiche e di introdurre una nuova categoria probatoria fondata sul

---

[330] *Ivi*, pp. 833-834; si veda anche CURTOTTI D., RIZZI V., NOCERINO W., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e prova penale*, cit., pp. 173 ss.
[331] *Ibidem*.
[332] Si veda sul punto RAUCCI P., *L'ordine europeo di indagine e prove digitali: tra presunzione di legittimità degli atti compiuti all'estero e diritti fondamentali*, in *Penale diritto e procedura*, 2025.
[333] Cfr. DANIELE M., *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, cit., p. 837.

criterio sostanziale dell'ingerenza che dia rilievo non tanto allo strumento impiegato, quanto all'intensità dell'invasione nella sfera privata[334].

4.4. Verso una regolazione integrata dei crypto-asset

Il quadro giuridico attuale in materia di regolamentazione delle criptovalute, considerato nella sua dimensione europea ed internazionale, riflette l'evoluzione normativa volta a rispondere a fenomeni emergenti come il riciclaggio di capitali, il finanziamento del terrorismo, l'elusione fiscale, tutti veicolati da asset digitali.

L'Unione europea ha adottato un approccio progressivamente sistemico, culminato nell'adozione di un pacchetto legislativo coordinato, focalizzato sul profilo della trasparenza e sulla responsabilizzazione degli operatori di asset digitali.

Il Regolamento UE 2023/1114, noto come *Markets in Crypto-Assets* (MiCA), in vigore dal 30 dicembre 2024, è il primo corpus normativo vincolante ed integrato a livello europeo per la regolazione dei *crypto-asset*, riguardante l'emissione, l'offerta al pubblico e l'ammissione alla negoziazione di token, nonché l'attività dei fornitori di servizi cripto (CASP). Con riguardo proprio a questi ultimi, tra le varie novità, viene introdotto a loro carico l'obbligo di ottenere una licenza presso l'autorità nazionale competente di uno Stato membro, al fine di essere abilitati, tramite il meccanismo del "*passporting*", ad operare in tutto il mercato unico europeo; in secondo luogo, il regolamento impone altresì requisiti patrimoniali minimi, obblighi di condotta, doveri informativi e procedure per la gestione dei conflitti di interesse con un impianto sanzionatorio dettagliato in caso di inadempienza[335].

In parallelo, il Regolamento UE 2023/1113, definito *Transfer of Funds Regulation* (TFR), estende al settore dei *crypto-asset* la già menzionata "*Travel Rule*", in base alla quale si impone agli intermediari, e anche ai CASP, di raccogliere e trasmettere informazioni complete e verificabili sul mittente e sul destinatario di ogni operazione finanziaria, senza soglia minima, a pena di sospensione o interruzione forzata delle

---

[334] Cfr. NICOLICCHIA F., *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla querelle giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero*, cit., p. 201; CURTOTTI D., RIZZI V., NOCERINO W., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e prova penale*, cit., pp. 173 ss.

[335] Per maggiori dettagli sul processo autorizzativo si veda il Regolamento europeo sulle cripto-attività Reg. Ue 2023/1114, in https://eur-lex.europa.eu/IT/legal-content/summary/european-crypto-assets-regulation-mica.html.

transazioni. Tali dati vengono poi condivisi tra gli operatori coinvolti in modo da garantire continuità informativa e consentire una cooperazione efficace tra le giurisdizioni[336]. D'altro canto, sul punto, le linee guida dell'Autorità Bancaria Europea (EBA) stabiliscono che i fornitori debbano mantenere tali dati accessibili per le autorità competenti, in modo da garantire che siano adeguatamente protetti e tracciabili, per la trasparenza e la prevenzione del riciclaggio[337].

Contestualmente, la Direttiva UE 2024/1640, la *Sesta Direttiva Antiriciclaggio* (AMLD6), estende formalmente gli obblighi di identificazione e segnalazione a tutti i soggetti che operano nel settore degli asset digitali. Ne consegue che anche i CASP dovranno sottostare ai medesimi obblighi degli enti finanziari tradizionali, come l'identificazione e verifica della clientela, la conservazione dei dati o la segnalazione di operazioni sospette[338]. Sebbene la direttiva sia stata formalmente adottata, il suo recepimento da parte degli Stati membri è ancora in corso.

Infine, il pacchetto normativo sarà completato dall'operatività dell'*Autorità europea antiriciclaggio* (AMLA), la cui attività ha preso avvio il 1° luglio 2025. Tale organismo avrà competenza diretta su entità finanziarie ad alto rischio, inclusi i CASP più rilevanti, e fungerà da coordinatore delle autorità nazionali. Nella prospettiva di una strategia più ampia di centralizzazione della vigilanza AML a livello europeo, l'Autorità opererà tramite l'effettuazione di ispezioni tematiche, la definizione di standard tecnici vincolanti e l'irrogazione di sanzioni pecuniarie nei casi più gravi[339].

Tuttavia, nonostante i significativi progressi, il sistema europeo di regolazione dei *crypto-asset* presenta ancora margini di criticità. È indubbio, infatti, che la piena implementazione delle direttive AML dipenderà dalla tempestività ed efficacia del recepimento delle stesse da parte degli Stati membri, nonché dalla capacità delle autorità

---

[336] Cfr. NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, cit.; PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio,* cit.; POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione,* cit.

[337] Per una maggiore approfondimento sulla Travel rule, si veda European Banking Authority, *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 "Travel rule Guidelines*", 2024.

[338] Direttiva (UE) 2024/1640 del Parlamento europeo e del Consiglio, del 31 maggio 2024, relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica la direttiva (UE) 2019/1937, e modifica e abroga la direttiva (UE) 2015/849 (Testo rilevante ai fini del SEE), in https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32024L1640.

[339] Per maggiori dettagli sulle funzioni AMLA, si veda Intervento di Sebastiano Laviola, *La nuova vigilanza antiriciclaggio alla luce dell'AML Packag*e, Banca d'Italia, 2025.

nazionali di applicare e far rispettare in modo uniforme i nuovi standard. Inoltre, resta ancora da definire un quadro organico di interoperabilità con i regimi extra-UE, al fine di evitare zone grigie giurisdizionali che potrebbero essere sfruttate a fini illeciti.

A livello internazionale, il principale punto di riferimento sono le raccomandazioni del GAFI (Financial Action task force), che fin dal 2019 ha esteso il proprio ambito di azione anche ai *virtual asset service providers* (VASP)[340], equiparando questi ultimi operatori agli altri soggetti già obbligati nell'ambito dell'*anti-money laundering* (AML). In proposito, tale organismo, come verrà illustrato dettagliatamente nel prosieguo, ha richiesto l'applicazione del principio "*know your customer*" (KYC), quale insieme di procedure per verificare l'identità dei clienti e valutare il loro profilo di rischio, oltre all'adozione di sistemi di controllo del rischio basati su metodologie proporzionate alla minaccia specifica, nonché, infine, l'attuazione, anche per i trasferimenti in asset digitali, della cosiddetta "*Travel rule*".

Tuttavia, l'implementazione di tali raccomandazioni a livello nazionale risulta ancora disomogenea, con paesi che, da un lato, hanno integralmente recepito le disposizioni internazionali nelle proprie legislazioni, e altri che, dall'altro lato, per motivi politici ed economici, mantengono ancora normative permissive, alimentando così il fenomeno del "*regulatory arbitrage*", ossia la tendenza degli operatori criminali a stabilirsi in giurisdizioni più tolleranti o meno vigilate per eludere gli obblighi di controllo[341]. In tale scenario, si registra un evidente indebolimento delle strategie nazionali di prevenzione e un ampliamento delle aree grigie in cui possono proliferare attività illecite come il riciclaggio di capitali.

La natura intrinsecamente transnazionale delle criptovalute e la loro crescente adozione nell'ambito di attività illecite, come il riciclaggio di denaro da parte delle

---

[340] Cfr. FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2019., dove i Virtual asset service providers sono definiti come "Fornitore di servizi di asset virtuali (Virtual Asset Service Provider, VASP): qualsiasi persona fisica o giuridica che, non essendo già disciplinata altrove nelle raccomandazioni, esercita per conto proprio o di altri una o più delle seguenti attività: scambio tra asset virtuali e valute fiat; scambio tra diversi asset virtuali; trasferimento di asset virtuali; custodia e/o gestione di asset virtuali o strumenti che consentono il controllo sugli stessi; partecipazione a offerte o vendite di asset virtuali e fornitura di servizi finanziari correlati.

[341] Cfr. SHEKHAWAT KS., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*, cit., p. 3; HARINAM V., BARAK A., *Law enforcement Strategies for Disrupting Cryptomarkets. A Practical Guide to Network Structure, Trust Dynamics, and Agent-Based Modelling Approaches*, cit., p. 68.

organizzazioni criminali, rende, pertanto, sempre più urgente lo sviluppo di soluzioni di armonizzazione internazionale.

Senza dubbio, la stipula di accordi multilaterali e il rafforzamento di meccanismi di cooperazione giudiziaria rappresentano un passo fondamentale non solo per armonizzare le normative penali e procedurali relative alle criptovalute, ma anche per garantire l'interoperabilità tecnica tra le autorità inquirenti e giudiziarie degli Stati aderenti[342].

Attraverso l'adozione di un trattato multilaterale dedicato al *cyberlaundering*, mirato ad armonizzare il quadro normativo e ad adottare standard comuni di acquisizione probatoria, creando canali prioritari di comunicazione tra le autorità inquirenti, le disfunzionalità nelle attività di cooperazione giudiziaria, le disparità normative e i ritardi procedurali sarebbero superati[343].

Al centro del dibattito sull'armonizzazione internazionale si colloca la regolamentazione preventiva degli intermediari digitali, come gli *exchangers*, i *wallet providers* e le piattaforme di pagamento decentralizzate. Tali operatori, rappresentando spesso l'unico punto di contatto tra l'universo virtuale delle criptovalute e le economie reali, dovrebbero essere sottoposti ad obblighi giuridici vincolanti sul piano internazionale, a sistemi di licenza, obblighi di segnalazione, audit indipendenti e meccanismi di responsabilità in caso di concorso in reati finanziari[344].

Si richiede dunque un intervento normativo, anche a livello internazionale, che regoli in maniera uniforme l'attività degli intermediari e che incida non solo sul piano preventivo, ma anche sull'efficacia dell'azione repressiva, identificando le controparti delle operazioni sospette e ricostruendo le catene di transazioni cripto finanziarie[345].

È dunque fondamentale rafforzare gli obblighi di trasparenza e tracciabilità imposti a questi operatori e vincolare l'apertura e la gestione dei conti digitali a sistemi di verifica dell'identità dell'utente[346].

In secondo luogo, occorre recepire a livello nazionale gli standard condivisi, come quelli proposti dal GAFI. In particolare, principio cardine dell'approccio proposto dal

---

[342] Cfr. DAMAP N.Y., MAZA K. D., *Jurisdictional Challenges in Cryptocurrency Disputes: Navigating the Legal Maze of a Borderless Technology*, in African Journal of stability and devolpment, 17, 1, 2025, pp. 132-160.
[343] Cfr. PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio,* cit., p. 614.
[344] Cfr. DAMAP N.Y., MAZA K. D., *Jurisdictional Challenges in Cryptocurrency Disputes: Navigating the Legal Maze of a Borderless Technology*, cit.
[345] Si veda, sul punto, NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, cit.
[346] *Ibidem*.

GAFI è il cosiddetto *risk-based approach* secondo cui le misure di prevenzione devono essere calibrate proporzionalmente al livello di rischio associato ai soggetti o alle operazioni coinvolte. L'applicazione di questo modello comporta l'estensione degli obblighi antiriciclaggio anche agli operatori che agiscono al di fuori del circuito bancario tradizionale come gli *exchangers*, i *wallet providers* e gli altri *virtual asset service providers* (VASPs), i quali, secondo le raccomandazioni del GAFI, devono essere sottoposti agli stessi obblighi previsti per gli enti finanziari tradizionali[347].

Ulteriore strumento incisivo, in questo ambito, è la già menzionata "*Travel rule*", oltre la registrazione obbligatoria degli operatori presso le autorità nazionali ed internazionali: la previsione di registri pubblici, affiancata da sanzioni rigorose in caso di inadempienza, consente di rendere più trasparente l'attività di tali operatori e di individuare rapidamente eventuali soggetti operanti al di fuori del perimetro legale[348].

4.5. Prospettive di riforma per una sistematizzazione penalistica del fenomeno delle criptoattività

Le specificità tecniche degli asset digitali, quali la decentralizzazione, l'anonimato e la natura immateriale dei valori coinvolti, impongono una riflessione anche sotto il profilo strettamente penalistico, mettendo in evidenza, in particolare, alcune lacune normative e difficoltà applicative che rendono necessario un intervento legislativo mirato. In questa prospettiva, occorre quindi esaminare le principali proposte normative e i principali contributi dottrinali per individuare possibili linee evolutive e soluzioni finalizzate al rafforzamento del contrasto all'utilizzo illecito delle criptovalute.

Un primo ambito di intervento attiene alla revisione del sistema penale sostanziale per colmare le lacune esistenti nella disciplina delle condotte illecite connesse all'impiego dei *crypto-asset*. In particolare, si evidenzia la necessità di includere esplicitamente nel catalogo delle fattispecie incriminatrici comportamenti quali il riciclaggio tramite

[347] Sul punto, v. Cfr. FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2019; cfr. anche NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, cit.; PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio,* cit.; POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione,* cit.
[348] *Ibidem*.

criptovalute, la creazione di diffusione di token privi di valore economico reale con finalità fraudolente, a simulazione di progetti imprenditoriali inesistenti[349].

In alternativa alla creazione di nuove incriminazioni, parte della dottrina propone altresì l'utilizzo estensivo delle categorie penali esistenti, in particolare delle fattispecie relative al riciclaggio e all'autoriciclaggio, alle operazioni effettuate tramite blockchain e smart contract. Sulla base di questo approccio, il concetto di "trasferimento" o "impiego" di beni di provenienza illecita potrebbe includere anche spostamenti di valore digitale realizzati tramite strumenti decentralizzati, mantenendo la finalità di ostacolare l'identificazione dell'origine delittuosa dei fondi[350].

È opportuno sottolineare, in secondo luogo, l'urgenza di elaborare una disciplina puntuale in materia di misure ablative con riferimento ai wallet digitali, nonché l'introduzione di protocolli operativi per la conservazione giudiziaria, il trasferimento e l'eventuale liquidazione degli asset digitali confiscati[351].

Un ulteriore elemento di riflessione riguarda l'estensione della responsabilità penale ai soggetti che, pur non partecipando direttamente alla condotta criminosa, mettono però a disposizione strumenti tecnologici idonei a favorirla, come creatori di software per la generazione di indirizzi anonimi, gestori di *exchange* non regolamentati, fornitori di servizi di *mixing* e *tumbling*. Il chiaro presupposto per l'applicazione di tale responsabilità sarebbe la consapevolezza da parte di tali attori della finalità illecita perseguita mediante l'utilizzo delle loro piattaforme[352].

---

[349] Per una riflessione di diritto penale sulla previsione nel nostro ordinamento di crimini commessi tramite criptovalute e l'eventuale necessità di un intervento legislativo per tutelare beni giuridici già protetti, nonché per un'analisi sui crimini economici già esistenti commessi tramite criptovalute, cfr. CALEMME C., *Criptovalute e diritto penale: progresso tecnologico, limiti normativi, linee di riforma*, Insubria, 2024.

[350] Cfr. PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio,* cit., p. 610.

[351] Cfr. NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, cit.; sulla confisca nella disciplina antiriciclaggio e sulla moneta virtuale come prodotto finanziario acquistato con finalità di investimento cfr. DIOTALLEVI G., *Riciclaggio, autoriciclaggio (...ed altro ancora) nel tempo della moneta virtuale e della cybersicurezza)*, in *Questione Giustizia*, 2024, p. 22; per un'analisi sulle procedure da seguire per l'esecuzione di misure cautelari reali su beni digitali, si veda altresì SAVASTANO L., *La regola "follow the money" nello spazio virtuale della blockchain: l'individuazione ed il sequestro di asset digitali*, in *Il mercato dei non fungible tokens tra arte, moda e gamification*, a cura di CANEPA A., Milano University Press, 2024, pp. 51 ss.; DELLA RAGIONE L., *D.Lgs. 203/2023: l'Italia si adegua alla normativa europea in tema di congelamento e confisca*, in *Il Quotidiano Giuridico*, *Rivista on line*, 2024. Sul sequestro di wallet vedi IOVINO P., *Le criptovalute nella fase di layering del riciclaggio*, in *Giurisprudenza penale*, 3, 2022, p. 7; sul sequestro probatorio delle criptovalute nei reati tributari cfr. recente sentenza della Cass. pen., n. 1760, ud. 20 novembre 2024, dep. 15 gennaio 2025, con cui la Corte si è espressa sulla questione della esecuzione di un sequestro probatorio per evasione fiscale su un asset digitale come il Bitcoin.

[352] Sulla responsabilità per riciclaggio di *exchangers, wallet providers, mixers* e *miners*, v. CROCE M., *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy*, in *Sistema penale*, 4, 2021, p. 127 ss.

Come poi già specificato sotto il profilo della armonizzazione internazionale, nel contesto della prevenzione, una delle proposte maggiormente condivise è l'inclusione esplicita degli operatori di servizi legati alle criptovalute tra i soggetti obbligati alla disciplina antiriciclaggio, in modo analogo agli intermediari finanziari tradizionali. Ne deriverebbe, a carico di tali operatori, l'introduzione di rigorosi obblighi di due diligence, tra cui l'identificazione della clientela (*Know Your Customer* – KYC), la conservazione della documentazione delle transazioni, la segnalazione di operazioni sospette alle autorità competenti e l'adozione di sistemi interni di controllo. A supporto di tali misure, di carattere preventivo, non può mancare un apparato sanzionatorio efficace, che contempli, oltre a pene pecuniarie proporzionate, la possibilità della sospensione temporanea o definitiva dell'attività in caso di gravi violazioni[353].

5. Strumenti investigativi e nuove tecniche per il contrasto ai cripto-reati

Anche il panorama investigativo contemporaneo è profondamente influenzato dalla crescente complessità dei crimini finanziari che sfruttano le criptovalute. La natura decentralizzata di tali monete virtuali presenta notevoli sfide per le forze dell'ordine e per le autorità giudiziarie, rendendo indispensabile l'adozione e l'adattamento di nuove tecniche investigative e strumenti di analisi forense.

Un primo e fondamentale requisito è il potenziamento delle tecniche di analisi delle blockchain. Nonostante strumenti come Chainalysis ed Elliptic consentano già di mappare le transazioni, identificare wallet sospetti, tracciare connessioni con piattaforme offshore e ricostruire flussi economici illeciti, occorre comunque la corretta interpretazione dei dati e la capacità di "deanonimizzare" i soggetti coinvolti[354].

Appare poi essenziale la definizione di un quadro normativo chiaro e aggiornato che disciplini l'utilizzo degli strumenti di analisi avanzata nel contesto delle indagini sulle criptovalute, soprattutto per garantire una regolamentazione efficace delle attività

[353] Sul punto v. SICIGNANO G.J., *Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain?,* in *Diritto Penale Contemporaneo*, 4, 2020, pp. 146 ss; NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, cit., pp. 8 ss.; POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione,* cit., pp. 172 ss.

[354] Cfr. SHEKHAWAT KS., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*, cit., pp. 6 ss.

investigative più complesse e per chiarire in maniera puntuale i presupposti giuridici e i limiti di utilizzabilità processuale delle prove digitali acquisite mediante gli strumenti investigativi.

Alla disponibilità di capacità tecniche deve poi affiancarsi un adeguato investimento nella formazione specialistica delle forze di polizia, con l'introduzione di unità specializzate in cyber-finanza presso le procure e le forze dell'ordine, con una formazione sia tecnica che giuridica[355].

Inoltre, sotto il profilo preventivo, risulta necessaria la regolamentazione di attività di monitoraggio preventivo, intercettazione e conservazione dei dati derivanti da wallet, smart contract, piattaforme decentralizzate, e l'implementazione di un sistema automatizzato di segnalazione delle transazioni ad alto rischio, rigorosamente sottoposto al controllo delle autorizzazioni giudiziarie competenti[356].

Elemento determinante per l'efficacia delle indagini è poi l'accesso alle informazioni detenute dagli intermediari digitali, in particolare dagli *exchangers* di criptovalute: l'ottenimento di dati relativi alle operazioni effettuate e all'identità dei soggetti titolari degli indirizzi è infatti un passaggio fondamentale per la ricostruzione dei flussi finanziari illeciti. Tale cooperazione risulta effettivamente praticabile solo laddove vengano previsti, come già illustrato, degli obblighi normativi specifici, in materia di tracciabilità e trasparenza, in capo agli operatori del settore[357].

Le criticità operative si intensificano quando le indagini vengono estese alle piattaforme decentralizzate, dove l'assenza di un soggetto centralizzato ostacola l'applicazione delle modalità tradizionali di acquisizione probatoria come la perquisizione e il sequestro diretto di asset digitali[358]. In tale scenario, dunque, l'azione investigativa deve necessariamente ricorrere a metodologie investigative più invasive, come l'infiltrazione informatica e l'impiego controllato di fondi, similmente a quanto già sperimentato nel contrasto alla pedopornografia online e alle attività illecite sui marketplace del dark web. Per tali ragioni, risulta imprescindibile la predisposizione di

---

[355] *Ibidem*.
[356] Cfr. NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, cit., pp. 8
[357] *Ibidem*.
[358] Quanto alle critiche dottrinali circa la mancata introduzione nel codice di procedura penale di una nuova disciplina organica per le indagini informatiche si veda LUPARIA L., *Computer crimes e procedimento penale*, cit.; v. BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in LUPARIA L., (a cura di) *Sistema penale e criminalità informatica*, Milano, 2009, p. 196.

protocolli operativi specifici per l'intercettazione dei flussi digitali e per l'utilizzo legittimo di tali strumenti informatici più intrusivi, in modo da garantire la conformità alle garanzie processuali e l'integrità delle prove acquisite.

Accanto alle tecniche investigative di tipo reattivo, emerge l'importanza dell'impiego di strumenti di intelligence finanziaria preventiva, finalizzati all'intercettazione anticipata di attività sospette in ambito cripto finanziario. In particolare, questa strategia si fonda sull'integrazione di fonti eterogenee di informazione provenienti da banche dati pubbliche, con segnalazioni di operazioni sospette e con l'analisi comportamentale dei wallet ad alto rischio, potenzialmente associati a flussi illeciti, anche attraverso l'impiego di sistemi di intelligenza artificiale programmati al riconoscimento di schemi di transazioni atipiche. In alcune giurisdizioni, per esempio, le Unità di informazione finanziaria (FIU) hanno già adottato metodologie simili, anticipando l'azione penale attraverso la tempestiva segnalazione di anomalie operative[359].

Un aspetto innovativo e particolarmente rilevante nel contrasto alla criminalità digitale - in particolare nell'ambito delle attività illecite condotte sul dark web – riguarda, infine, l'adozione e l'applicazione di misure coercitive di natura patrimoniale nei confronti degli asset digitali[360]. Come già anticipato, misure come il sequestro e la confisca delle criptovalute rappresentano una leva fondamentale per disarticolare i flussi finanziari illeciti e privare le organizzazioni criminali delle risorse economiche necessarie al proseguimento delle loro attività criminali. Tuttavia, l'effettiva attuazione di tali misure si scontra con ostacoli di natura tecnica e giuridica, stante la progettazione di alcune criptovalute incentrate sulla tutela della privacy, come Monero e Zcash, che rende estremamente difficile il tracciamento delle transazioni e l'attribuzione dei wallet a specifici soggetti, ostacolando l'identificazione del patrimonio digitale e di conseguenza l'esecuzione di provvedimenti cautelari reali.

Dal momento che l'efficacia delle azioni patrimoniali dipende dalla possibilità di stabilire un collegamento concreto tra le operazioni registrate e le identità reali degli utenti coinvolti, risulta pertanto necessario ricorrere a strategie investigative complementari,

[359] Per una approfondita disamina degli strumenti di intelligence preventiva, che impiegano sistemi di intelligenza artificiale, si veda CONFENTE L., *Intelligenza artificiale e investigazioni. La tecnologia come strumento nella lotta alla mafia*, Corso di Dottorato in Studi sulla criminalità organizzata, Unimi, 2024.
[360] Vedi nt. n. 351.

come l'accesso diretto ai dispositivi degli indagati, le operazioni sotto copertura o la cooperazione con *exchangers* regolamentati[361].

In conclusione, alla luce delle criticità riscontrate nell'attuazione delle misure patrimoniali nel contesto digitale, si rende pertanto necessaria l'adozione di un complesso organico di riforme normative e soluzioni operative mirate. In particolare, appare indispensabile lo sviluppo di strumenti giuridici aggiornati e coerenti con le trasformazioni tecnologiche in atto, accompagnato da un quadro legislativo in grado di rispondere efficacemente alle peculiarità degli asset digitali.

[361] Cfr. SHEKHAWAT K.S., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*, cit., pp. 6 ss.

SEZIONE III

CRIMINALITÀ ORGANIZZATA NATIVAMENTE DIGITALE: PROFILI STRUTTURALI, LOGICHE OPERATIVE E RIFLESSI NORMATIVI

CAPITOLO V

Le organizzazioni criminali cibernetiche o "*cyber organised criminals*"

SOMMARIO: **1.** Nel cuore del cyberspazio: le organizzazioni criminali cibernetiche – **2.** L'impatto della tecnologia sulla struttura dei gruppi criminali cibernetici – **2.1.** Debolezza e flessibilità strutturale e gerarchica – **2.2.** La permanenza dei membri del gruppo – **2.3.** Il valore dei legami sociali per la costituzione del network criminale– **2.4.** Le competenze tecniche dei membri del gruppo criminale– **2.5.** Assenza dell'elemento della forza fisica– **2.6.** La suddivisione dei ruoli all'interno del gruppo– **3.** Classificazione teleologica dei cyber criminali – **4.** Principali attività dei cybercriminali– **5.** Le associazioni a delinquere esclusivamente cibernetiche o gruppi di tipo I – **5.1.** Le due diverse configurazioni dei gruppi dei cybercriminali: *swarms* e *hubs* – **5.2.** Le comunità online di pedofili: struttura, tecniche operative e capacità di adattamento – **5.3.** Le organizzazioni di hacktivisti – **6**. Le associazioni a delinquere parzialmente cibernetiche o gruppi di tipo II – **6.1.** Le due diverse configurazioni dei gruppi ibridi dei cybercriminali: *clustered* ed *extended* – **6.2.** Le associazioni dedite alle truffe online – **6.3.** Le comunità criminali operanti nei mercati online illegali – **7.** Conclusioni

1. Nel cuore del cyberspazio: le organizzazioni criminali cibernetiche

Come anticipato, la seconda sezione del presente lavoro si concentrerà sui gruppi di tipo I e II, ossia quelle organizzazioni che operano esclusivamente, o parzialmente, nel cyberspazio, commettendo crimini in cui la tecnologia non rappresenta un semplice strumento, ma un elemento centrale e imprescindibile del crimine stesso, come sarà analizzato nel dettaglio nel prosieguo.

Il fenomeno del *cyber organized crime* emerge, dunque, come una sintesi di due categorie socio-criminologiche distinte: il *cybercrime* e la *criminalità organizzata*, dando

vita a un nuovo tipo di organizzazione criminale che agisce e si struttura interamente, o prevalentemente, online.

Sebbene il concetto di *cyber organized crime* possa sembrare facilmente comprensibile, definire con precisione i contorni di tale fenomeno non è un'impresa semplice. Le difficoltà derivano principalmente dall'incertezza che caratterizza la definizione di questo nuovo tipo di criminalità, che solleva rilevanti interrogativi non solo di natura giuridica, ma anche di politica penale.

Il dibattito intorno al concetto e all'inquadramento di questi gruppi criminali nell'ambito dell'"*organised crime*" ha condotto alla formazione di due principali schieramenti dottrinali.

Da un lato, una parte della letteratura sostiene che i gruppi di cybercriminali possono essere inclusi sotto la categoria di criminalità organizzata e, conseguentemente, propone l'aggiornamento delle definizioni normative esistenti al fine di ricomprendervi anche le forme più fluide e tecnologicamente avanzate di crimine. Si tratta di contributi che escludono l'impiego di un approccio troppo rigido, basato esclusivamente sui modelli tradizionali di organizzazione criminale, che non sarebbero in grado di cogliere le trasformazioni in atto nel fenomeno.

Dall'altro lato, altri autori mantengono una posizione più prudente, basandosi sulle significative differenze tra i gruppi di cybercriminali e le tradizionali organizzazioni criminali, soprattutto alla luce delle implicazioni che l'etichetta di "*organised crime*" di questi gruppi potrebbe avere in termini di politiche penali e di intervento legislativo.

Questa questione, ora brevemente introdotta, sarà trattata in dettaglio nel prosieguo, in sede di inquadramento giuridico e normativo del fenomeno (v. capitolo VI).

Il presente capitolo si propone, invece, di analizzare il ruolo della tecnologia e la sua influenza, a livello strutturale e teleologico, nelle organizzazioni criminali cibernetiche, fonte di crescenti preoccupazioni tra le autorità e le agenzie preposte al contrasto della criminalità.

Queste ultime hanno infatti rilevato come i cybercriminali stiano divenendo sempre più sofisticati e interconnessi, trasformandosi in una risorsa strategica per la criminalità organizzata contemporanea[362].

[362] Cfr. GABRIELLI I., *Come le mafie si muovono nel mondo della rete, in Scintille. Trimestrale della fondazione Scintille di futuro*, 2023, 1, p. 28.

A suscitare ulteriore allarme è l'eterogeneità che contraddistingue tali gruppi dal punto di vista della provenienza nazionale, un fenomeno facilitato dalla natura immateriale e ubiqua della rete internet.

Come già visto per le organizzazioni criminali tradizionali, anche per i gruppi criminali cibernetici è necessario ora analizzarne la struttura e le attività, nonché il ruolo fondamentale che la tecnologia gioca all'interno di questi gruppi.

2. L'impatto della tecnologia sulla struttura dei gruppi criminali cibernetici

Nell'ambito delle associazioni per delinquere cibernetiche - che, dal punto di vista processual-penalistico, vedono la contestazione di un reato di associazione per delinquere caratterizzato dallo scopo di commettere *cybercrimes*[363] - è possibile distinguere ulteriormente tra associazioni esclusivamente cibernetiche e parzialmente cibernetiche.

L'elemento scriminante risiede nell'elemento organizzativo che nelle prime si colloca nel cyberspazio, esattamente come il programma criminoso dell'associazione, mentre nelle seconde è collocato prevalentemente nel mondo fisico[364]. Si tratta, in quest'ultimo caso, di associazione per delinquere cibernetiche di tipo ibrido, rientranti nel gruppo di tipo II, a cui sarà dedicata apposita trattazione (v. sez. III, cap. V, par. 6).

Tale precisazione concettuale si rivela fondamentale, in quanto risponde a una scelta metodologica ben definita, mirata a strutturare l'analisi in modo chiaro e sistematico, al fine di porre solide basi la successiva fase di questa ricerca, dedicata all'esame dell'inquadramento giuridico-normativo dei fenomeni analizzati.

La tecnologia riveste un ruolo imprescindibile nelle organizzazioni criminali cibernetiche, determinando profondi mutamenti sia nella loro struttura che nelle loro attività. A differenza delle organizzazioni tradizionali, queste entità si sviluppano e operano prevalentemente nel cyberspazio, dove la rete offre una flessibilità superiore e garantisce un anonimato difficilmente perseguibile in contesti fisici. Grazie alla tecnologia, tali gruppi possono adottare modelli organizzativi meno rigidi, caratterizzati

---

[363] Sul punto, cfr. PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, in *Meridiana*, 106, 2023, p. 164.
[364] *Ibidem*.

da una distribuzione più dinamica delle funzioni e da una gestione fluida e decentralizzata. Inoltre, le attività criminose vengono amplificate e diversificate, sfruttando le immense potenzialità offerte dal mondo digitale. In questo scenario, l'innovazione tecnologica, dunque, incide in modo determinante sull'evoluzione e sul funzionamento di queste organizzazioni.

Questa analisi trova, pertanto, il suo punto di partenza nell'esame delle caratteristiche strutturali che contraddistinguono queste entità criminali cibernetiche, anche in contrapposizione ai modelli organizzativi delle associazioni criminali tradizionali, inquadrate nei gruppi di tipo III, e già trattate nella sezione II, del presente lavoro.

2.1. Debolezza e flessibilità strutturale e gerarchica

I gruppi di cybercriminali presentano una struttura più fluida ed una maggiore flessibilità organizzativa.

Se in passato le organizzazioni criminali strutturate erano necessarie per commettere crimini complessi, richiedendosi a questo fine un grado significativo di organizzazione e sofisticazione, ad oggi, con l'evoluzione delle tecnologie dell'informazione e della comunicazione, alcune tradizionali strutture organizzative risultano invece superflue. Un singolo individuo, o un numero ristretto di coautori dotati di adeguate competenze informatiche, può infatti raggiungere un livello di efficienza paragonabile a quello di una rete criminale strutturata secondo i modelli tradizionali.

Pertanto, all'aumentare della padronanza delle tecnologie da parte degli imprenditori del crimine, si assiste a una progressiva marginalizzazione della necessità di strutture organizzative rigide, con un conseguente indebolimento del concetto classico di organizzazione criminale[365].

Pare ci sia quindi un rapporto inversamente proporzionale tra tecnologia e organizzazione: più i criminali padroneggiano le competenze ICT, meno organizzazione sarà necessaria[366].

---

[365] Tale concetto viene ribadito da WALL D.S., *Cybercrime: the transformation of crime in the information age*, cit.

[366] Cfr. LAVORGNA A., *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?,* cit., p. 209; anche NURSE J., BADA M., *The Group element of cybercrime: types, dynamics and criminal operations*, in *The Oxford handbook of cyberpsychology*, DOI: 10.1093/oxfordhb/9780198812746.013.36, 2018, p. 14.

Le organizzazioni criminali online, quindi, tendono a ridurre l'importanza di strutture gerarchiche formali, mettendo in risalto una struttura più fluida, contestuale e laterale. Queste reti non sono più vincolate da confini nazionali, territoriali o culturali, poiché i criminali informatici, come tutti gli utenti del cyberspazio, condividono una cultura globale che trascende le frontiere fisiche e geopolitiche. Di conseguenza, mentre le organizzazioni criminali tradizionali erano spesso caratterizzate da rigide strutture locali, quelle online tendono a sviluppare alleanze anche globali, adattandosi a un ambiente dinamico e interconnesso[367].

Tuttavia, sebbene le reti criminali cibernetiche non presentino una gerarchia rigida, ciò non implica che siano del tutto fluide, potendosi riscontrare altresì relazioni di interdipendenza e ruoli funzionali distinti. Nella maggior parte delle reti analizzate, infatti, emergono tre categorie principali: i membri centrali, gli abilitatori e i "*money mules*". I membri centrali sono coloro che avviano e coordinano gli attacchi, dirigendo le operazioni; gli abilitatori, invece, forniscono i servizi tecnici necessari per eseguire i crimini e lavorano autonomamente, mettendo a disposizione le loro competenze per diverse reti; i "*money mules*", infine, sono impiegati specificamente per nascondere le tracce finanziarie, spostando i fondi illeciti verso destinazioni sicure. Se questi ultimi sono facilmente sostituibili e non indispensabili per la realizzazione degli attacchi, i membri centrali e gli abilitatori rappresentano invece il cuore operativo delle reti criminali[368].

Pertanto, come vedremo meglio, anche le reti criminali cibernetiche possono essere caratterizzate da una complessa interdipendenza, con ciascun membro che ricopre un ruolo preciso e funzionale all'interno della rete[369].

Un esempio interessante di tale dinamica può essere osservato nei forum online dedicati al crimine informatico. Questi forum fungono da mercato per beni e servizi illeciti, operando principalmente su piattaforme web o su canali di chat. Tra i prodotti comunemente scambiati ci sono dati rubati, informazioni su carte di credito e malware, mentre alcuni servizi, come attacchi DDoS o hacking, vengono offerti da cybercriminali

---

[367] Cfr. BRENNER S.W., *Organized cybercrime? How cyberspace may affect the structure of criminal Relationships*, cit., pp. 42 ss.

[368] Cfr. LEUKFELDT R.E., LAVORGNA A., KLEEMANS R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., pp. 290 ss.; per un maggiore approfondimento sui money mules e sulle attività di riciclaggio v. PICKLES R., *'Money Mules': Exploited Victims or Collaborators in Organised Crime?*, cit.

[369] Cfr. FLOR R., LUPARIA L., *Criminalità organizzata e criminalità informatica ("cyber-organized-crime")*, in *Diritto penale contemporaneo*, 2019, p. 226 ss.

specializzati. Nonostante l'apparente fluidità di queste organizzazioni, anche nei forum si riscontra una gerarchia, con amministratori e moderatori, la cui posizione gerarchica dipende dall'affidabilità, dalle abilità o dai favori che un membro riesce a ottenere dai livelli superiori. Alcuni forum, come il DarkMarket, hanno addirittura sviluppato sistemi di garanzia per le transazioni, simili a quelli delle organizzazioni mafiose tradizionali, per proteggere i membri da truffe e garantire la sicurezza degli scambi. Tali meccanismi di governance criminale rappresentano una nuova evoluzione del crimine informatico, che integra la funzionalità tecnica con una struttura di controllo e protezione sempre più sofisticata [370].

2.2. La permanenza dei membri del gruppo

A seconda delle attività intraprese, la struttura di un gruppo di criminalità organizzata cibernetica si configura prevalentemente come una rete mutevole, in cui i membri si uniscono per periodi limitati, al fine di compiere mansioni specifiche. Al termine di tali incarichi e una volta raggiunti gli obiettivi prefissati, i membri si separano senza che vi sia un impegno a lungo termine[371].

Questo modello operativo si contraddistingue, dunque, per la sua transitorietà, poiché i gruppi di criminalità cibernetica non sono caratterizzati da una continuità stabile, ma da

---

[370] Cfr. LUSTHAUS J., *How organised is organised cybercrime?*, in *Global Crime Journal*, 14, 1, 2013, pp. 54-55; per un approfondimento sulla formazione dei gruppi criminali e sulla interazione dei loro membri all'interno dei forum online, cfr. anche NURSE J., BADA M., *The Group element of cybercrime: types, dynamics and criminal operations*, cit., p. 14; anche Cfr. LEUKFELDT R.E., LAVORGNA A., KLEEMANS R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., pp. 290 ss., in cui distingue tra quattro tipologie di formazione di reti criminali: (I) interamente attraverso contatti sociali offline; (II) contatti sociali offline come base e forum online per il reclutamento di specialisti; (III) forum online come base e contatti sociali offline per il reclutamento di criminali locali; (IV) interamente attraverso forum online. Emblematico è il caso di LulzSec, gruppo i cui membri non si sono mai incontrati nel mondo reale e che operava tra Stati Uniti e Regno Unito, dimostrando così la natura globalizzata e decentrata di tali reti. Parallelamente, altra letteratura ha evidenziato come i forum di "carding" – tra cui Shadowcrew, Cardersmarket e Darkmarket – svolgano un ruolo cruciale nell'economia criminale sotterranea, in quanto sedi di scambio di dati di carte di credito sottratti e di condivisione di tecniche per ottenerli. Attraverso dati di interazione, si è osservato che tali piattaforme sviluppano veri e propri meccanismi socio-economici di regolazione (controllo e coordinamento formale, networking sociale, mitigazione dell'incertezza identitaria e della qualità), che li rendono mercati clandestini sofisticati, paragonabili per dinamiche a quelli legittimi. In questo senso, i forum di carding si rivelano strumenti robusti, capaci di sostenere e alimentare l'espansione dell'economia criminale online.

[371] Sul punto, v. CHOO K. R., *Organised crime groups in cyberspace: a typology,* cit., p. 276.

un'aggregazione di individui che si uniscono in funzione di vantaggi economici reciproci e che si dissolvono non appena tali vantaggi vengono meno[372].

Questa configurazione esclude la possibilità di una leadership rigida e gerarchica, poiché la natura fluida e transitoria della rete rende inefficace qualsiasi struttura di comando autoritaria. Sebbene una forma di leadership sia indubbiamente necessaria per l'orientamento delle attività, la struttura si fonda principalmente su un modello di consenso, che valorizza l'autonomia dei membri e promuove un'azione collettiva e cooperativa piuttosto che una concentrazione regimentata delle forze. L'organizzazione, pertanto, non si caratterizza per un'impostazione rigida, ma per una notevole flessibilità operativa, che consente ai membri di adattarsi rapidamente alle esigenze del contesto[373].

Poiché le alleanze all'interno di tali gruppi sono circoscritte ad obiettivi specifici e limitati nel tempo, è frequente che i criminali informatici appartengano a più di una rete simultaneamente, il che testimonia l'estrema fluidità e l'adattabilità delle loro interazioni.

Questo modello organizzativo diffuso, decentralizzato e globalmente connesso, privo di confini nazionali o culturali, si distingue da quello delle organizzazioni criminali tradizionali, che di regola operano su scala locale e gerarchicamente strutturata[374].

Proprio in virtù di tale flessibilità strutturale che consente l'intercambiabilità dei membri e delle reti stesse, che non necessitano di legami duraturi, i gruppi cibernetici sono in grado altresì di avvalersi più agevolmente di risorse esterne, come soggetti che operano al di fuori del cyberspazio, per realizzare attività specifiche. Tali individui vengono reclutati per operazioni particolari, funzionali agli scopi ultimi dell'organizzazione[375].

È indubbio, pertanto, che questo tipo di flessibilità non solo consente ai gruppi di adattarsi rapidamente alle mutevoli necessità operative, ma favorisce anche una vasta gamma di competenze, rendendo l'organizzazione sempre più pervasiva e sofisticata.

---

[372] Cfr. LAVORGNA A., *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?*, cit., p. 197.
[373] Cfr. BRENNER S.W., *Organized cybercrime? How cyberspace may affect the structure of criminal Relationships*, cit., pp. 42 ss.
[374] *Ibidem*.
[375] Cfr. FLOR R., LUPARIA L., *Criminalità organizzata e criminalità informatica ("cyber-organized-crime")*, cit., p. 226 ss., in cui gli autori riportano, a titolo esemplificativo, il coinvolgimento di figure quali il security manager di un istituto bancario o un dipendente infedele di un'impresa, chiamati a collaborare per singole operazioni, come ad esempio l'installazione fisica di key loggers su dispositivi o server.

2.3. Il valore dei legami sociali per la costituzione del network criminale

I legami sociali all'interno delle organizzazioni di crimine informatico sono più fluidi e meno strutturati rispetto a quelli propri dei gruppi criminali tradizionali, nei quali le relazioni personali e le connessioni sociali consolidate rivestono un ruolo fondamentale.

I gruppi di crimine informatico organizzato si distinguono da quelli tradizionali principalmente per la modalità di interazione dei loro membri, che, pur collaborando verso obiettivi comuni, si conoscono prevalentemente o esclusivamente nell'ambito virtuale, senza alcuna connessione sociale preesistente o legame personale consolidato. A differenza delle organizzazioni criminali tradizionali, che si fondano su reti di relazioni interpersonali e su una struttura sociale radicata, i gruppi cibernetici si formano spesso tramite piattaforme digitali, dove individui con interessi convergenti si uniscono per perseguire finalità illecite. Questi gruppi, dunque, non richiedono conoscenze reciproche antecedenti alla loro formazione ma il loro legame si sviluppa, piuttosto, sulla base di obiettivi comuni, resi possibili dalla capacità di incontrarsi virtualmente e di coordinare operazioni criminali attraverso internet[376].

In termini di relazioni sociali, gli studi condotti sulle reti hanno permesso di identificare, in base alla modalità di formazione e crescita di queste organizzazioni, la sussistenza, da un lato, di gruppi in cui i contatti sociali offline costituiscono la base delle reti con l'utilizzo di forum online per reclutare specialisti e, dall'altro lato, di gruppi che si fondano principalmente su forum online, in cui la connessione tra i membri avviene virtualmente[377].

Emerge, pertanto, che alcune reti criminali informatiche, pur avvalendosi di piattaforme digitali, mantengono un legame fondamentale con i contatti sociali preesistenti. La maggior parte delle reti, infatti, si è originata e sviluppata attraverso interazioni sociali offline, come il legame tra i co-autori, che spesso condividevano esperienze comuni, come la stessa provenienza geografica, l'appartenenza a comunità o

---

[376] Cfr. CHOO K. R., *Organised crime groups in cyberspace: a typology,* cit., p. 278; si veda anche NURSE J., BADA M., *The Group element of cybercrime: types, dynamics and criminal operations*, cit., p. 14

[377] *Ivi*, p. 13, in cui gli autori evidenziano come la reputazione rappresenta una vera e propria "moneta" di scambio: identità digitali riconosciute incentivano la cooperazione e l'accesso a forum esclusivi, pur scontrandosi con la necessità di mutare periodicamente pseudonimi per ridurre i rischi di identificazione; viene altresì evidenziato come la dinamica fiduciaria sia sostenuta da meccanismi di segnalazione, attraverso i quali i criminali comunicano affidabilità tramite segnali difficilmente imitabili dagli attori non credibili; i forum, a loro volta, istituiscono procedure interne per rafforzare la fiducia reciproca, come requisiti di reputazione, sistemi di classificazione dei venditori ("trusted sellers") e procedure di ammissione selettive, sul modello mafioso, come nel caso di Darkode.

gruppi sociali o l'esperienza nel contesto criminale. Pertanto, sebbene le piattaforme online siano essenziali per la crescita e l'espansione del gruppo, i contatti offline restano cruciali, soprattutto per il reclutamento di figure chiave come gli abilitatori o i *money mules*, che vengono spesso introdotti attraverso conoscenze pregresse[378].

In altri casi, invece, la relazione tra i membri del network si costruisce e si consolida online, tramite *blackmarkets*, forum protetti, chat criptate, social network o punti di contatto oscuri. La connessione tra i membri di queste reti, per quanto meno radicata geograficamente o culturalmente, si fonda su criteri di affidabilità, sulla "fama" nel cyberspazio, sul successo delle operazioni precedenti e si instaura per il perseguimento di obiettivi specifici, come l'esecuzione di attacchi cibernetici mirati o la fornitura di servizi ad altri gruppi criminali[379].

I "contact points" online, che fungono da snodi centrali per la gestione di queste reti, sono regolati da regole severe, e l'ingresso o la partecipazione in forum, chat criptate o mercati neri può richiedere l'approvazione o la sponsorizzazione di un membro ritenuto affidabile all'interno del cyberspazio o dell'underground informatico. Pertanto, in questi contesti, la partecipazione non è solo una questione di abilità tecnica, ma dipende anche dalla capacità di essere riconosciuti come degni di fiducia da altri membri della comunità, che fungono da garanti del comportamento e delle intenzioni degli altri[380].

2.4. Le competenze tecniche dei membri del gruppo criminale

I membri delle organizzazioni di crimine informatico organizzato sono generalmente dotati di competenze altamente specializzate, in materia di vulnerabilità di *software* e *hardware*, dei sistemi operativi, nonché nell'ambito della programmazione. Questi individui, spesso con un livello di istruzione superiore, si avvalgono di risorse

---

[378] Cfr. LEUKFELDT R.E., LAVORGNA A., KLEEMANS R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit.. 290 ss.

[379] *Ibidem*; anche NURSE J., BADA M., *The Group element of cybercrime: types, dynamics and criminal operations*, cit., p. 13.

[380] Cfr. FLOR R., LUPARIA L., *Criminalità organizzata e criminalità informatica ("cyber-organized-crime")*, cit., p. 226 ss.; si veda anche Cfr. LEUKFELDT R.E., LAVORGNA A., KLEEMANS R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., pp. 292 ss.

accademiche e tecniche sofisticate per eludere le difese e sfruttare le debolezze dei sistemi informatici[381].

All'interno di queste reti, i membri hanno accesso a punti di contatto che permettono loro di organizzare azioni collaborative, creando alleanze per perseguire specifici obiettivi criminali e, quando necessario, intraprendere azioni di ritorsione contro rivali o agenzie governative. Le strutture di leadership all'interno di tali gruppi si distinguono per la loro natura più egualitaria rispetto a quelle riscontrabili nelle organizzazioni criminali tradizionali. Infatti, i gruppi operanti nel cyberspazio tendono ad essere composti da individui con abilità tecniche simili, dove l'attitudine di un individuo come criminale informatico dipende in gran parte dalla sua esperienza e competenza nel settore tecnico[382].

In questo contesto, la competenza tecnica rappresenta non solo un fattore di affiliazione, ma anche una porta d'accesso per l'individuo a una forma di imprenditoria illecita indipendente. Ogni membro del crimine informatico, avendo acquisito un certo grado di esperienza, è potenzialmente in grado di operare come un imprenditore autonomo nel vasto panorama del cyberspazio, sfuggendo così a strutture di leadership centralizzate e gerarchiche proprie dei tradizionali gruppi criminali[383].

2.5. Assenza dell'elemento della forza fisica

Nel contesto del crimine informatico, la forza fisica risulta essere irrilevante.

Un hacker non necessita dell'impegno congiunto di decine di individui per superare le difese di una vittima, ma può farlo attraverso l'utilizzo di tecnologie avanzate e tecniche automatizzate che gli consentono di eludere facilmente le misure di protezione elettroniche. In altre parole, in questo contesto, la vera "forza" risiede nel *software*, non nel numero degli individui coinvolti ed è pertanto la capacità tecnica a determinare il successo del gruppo, piuttosto che la sua dimensione o la sua presenza fisica sul territorio[384].

---

[381] Cfr. CHOO K. R., *Organised crime groups in cyberspace: a typology,* cit., p. 277.
[382] *Ibidem*.
[383] Cfr. BRENNER S.W., *Organized cybercrime? How cyberspace may affect the structure of criminal Relationships*, cit., pp. 42 ss.; sul punto, si veda anche NURSE J., BADA M., *The Group element of cybercrime: types, dynamics and criminal operations*, cit., p. 6.
[384] *Ivi*, p. 27.

Le risultanze investigative mostrano infatti come, nell'ambito delle organizzazioni criminali di matrice cibernetica, l'impiego della violenza fisica rappresenti un elemento residuale e non strutturale: le dinamiche interne di tali gruppi sembrano infatti orientate verso forme di coercizione indiretta o pressione psicologica, piuttosto che verso l'uso diretto della forza.

Analogamente, anche il fenomeno della corruzione non risulta emergere in modo rilevante all'interno del contesto analizzato[385]. Nonostante alcune indicazioni ipotetiche circa possibili influenze esterne o complicità istituzionali, le indagini non hanno restituito elementi probatori solidi che confermino il ricorso a pratiche corruttive, sebbene questa apparente assenza possa anche ricondursi alla natura e all'orientamento delle attività investigative, le quali si sono concentrate prevalentemente sulla dimensione tecnico-operativa dei reati informatici, tralasciando in parte l'approfondimento di aspetti collaterali quali la violenza e la corruzione sistemica. Ciò evidenzia la necessità di ampliare il perimetro analitico, al fine di cogliere con maggiore completezza le possibili connessioni tra criminalità digitale e forme di potere coercitivo o corruttivo più tradizionali[386].

In generale, emerge chiaramente che la natura del crimine informatico si discosta profondamente dalle pratiche tradizionali del crimine organizzato, come quelle tipiche delle mafie. In particolare, la dinamica dell'estorsione, che nel crimine tradizionale si traduce in minacce fisiche e intimidazioni sul terreno, non trova riscontro nel cyberspazio. Al posto della violenza fisica, il crimine informatico si avvale di forme di intimidazione più sottili ma altrettanto efficaci, quali minacce psicologiche, emotive, e, soprattutto, attacchi informatici: le modalità di estorsione online, ad esempio, come nel caso del *ransomware*, permettono ai criminali di esercitare un potere simile a quello delle pratiche fisiche, ma in una forma digitale, manipolando e minacciando le vittime attraverso la rete[387].

---

[385] Cfr. LEUKFELDT R.E., LAVORGNA A., KLEEMANS R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., pp. 294.

[386] *Ibidem*.

[387] Cfr. MINNAAR A., *Organised Crime And The 'New More Sophisticated' Criminals Within The Cybercrime Environment: How 'Organised' Are They In The Traditional Sense?,* cit., pp. 128 ss.

2.6. La suddivisione dei ruoli all'interno del gruppo

I gruppi criminali organizzati nel cyberspazio operano con una struttura interna ben definita, molto simile a quella di un'azienda tradizionale. All'interno di questi gruppi, ogni membro ha compiti specifici e ruoli ben delineati, a seconda del tipo di attività illecita da portare a termine: si tratta di vere e proprie "imprese del crimine", dove il lavoro è suddiviso tra esperti tecnici, addetti al supporto, operatori logistici e persino figure incaricate di gestire i flussi finanziari, spesso incaricate di ricevere, smistare o riciclare i proventi delle attività illecite[388].

I ruoli interni variano quindi in base al tipo di reato cibernetico e alla natura delle attività offline eventualmente necessarie per il compimento dell'illecito. Quando il crimine richiede competenze specifiche o particolari strumenti tecnologici, il gruppo può ingaggiare professionisti esterni per portare a termine operazioni complesse. Ad esempio, nei casi di alcuni reati informatici, come l'abuso o lo sfruttamento sessuale online di minori, ogni fase del crimine è gestita da persone con ruoli specifici e compiti precisi, spesso supportati da tecnologie e piattaforme digitali: i compiti sono distribuiti tra chi individua le vittime, chi le adesca e chi produce, scambia o archivia materiale illegale[389].

Diverso è il caso dei gruppi che commettono crimini informatici basati sull'uso intensivo della rete e delle infrastrutture tecnologiche. In questi casi, i ruoli si specializzano attorno agli strumenti e alle competenze digitali necessarie per violare sistemi o rubare dati[390].

Nel panorama della criminalità informatica emergono, dunque, due modelli organizzativi distinti, che riflettono approcci diversi alla gestione delle attività illecite online.

Non può ignorarsi, da un lato, la presenza di network più fluidi e decentralizzati, caratterizzati da una struttura informale e spesso priva di una vera e propria leadership. Questo è il caso di gruppi motivati da ideologie politiche o da intenti discriminatori, come i promotori di crimini d'odio o di attacchi cibernetici con finalità militanti o di protesta. In questi ambienti, l'azione collettiva è guidata da un obiettivo condiviso, ma non esiste

[388] Sul punto, v. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., pp. 9, in cui vengono evidenziati nel dettaglio alcuni ruoli che possono rivestire i membri del gruppo cybercriminale.
[389] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 18-19.
[390] *Ibidem*.

un comando centrale: i membri agiscono in maniera autonoma, coordinandosi in modo orizzontale e flessibile, spesso tramite piattaforme digitali e canali di comunicazione temporanei o anonimi[391].

Dall'altro lato, si osserva la presenza di gruppi strutturati in modo gerarchico, con una catena di comando ben definita e ruoli rigidamente assegnati. Un esempio tipico è rappresentato da alcuni forum online specializzati nello scambio di beni e servizi illegali, dove l'organizzazione interna ricorda quella di un'impresa criminale tradizionale. In questi contesti, esistono figure apicali che gestiscono le operazioni, controllano l'accesso dei membri, impongono regole e sanzioni, e coordinano le attività in modo centralizzato[392].

Tra le figure chiave in questi gruppi troviamo, ad esempio: il programmatore, ovvero un tecnico che sviluppa software dannosi, o strumenti su misura per penetrare i sistemi informatici, incaricato di creare malware personalizzati su richiesta; l'hacker, che si occupa di identificare e sfruttare falle di sicurezza in reti, applicazioni e infrastrutture informatiche; il tecnico di supporto, per fornire assistenza continua al gruppo, occupandosi del corretto funzionamento delle infrastrutture digitali, della manutenzione dei server, della risoluzione dei problemi tecnici e dell'aggiornamento degli strumenti di attacco; l'host, incaricato di offrire o gestire spazi fisici o digitali dove vengono condotte le attività criminali[393].

Questo modello rappresenta una struttura teorica e non implica necessariamente l'esistenza di un'organizzazione rigida o formalmente costituita. In molti casi, infatti, alcune funzioni operative possono essere affidate a soggetti esterni al gruppo principale. È il caso, ad esempio, del gruppo Koobface, di cui si parlerà più avanti, che ricorre proprio ad un "outsourcing criminale" per svolgere determinate attività[394].

Infine, è bene specificare che all'interno delle organizzazioni criminali cibernetiche, esistono anche ruoli di natura temporanea, ricoperti da individui che vengono coinvolti solo per brevi periodi e per compiti specifici. Una volta raggiunto l'obiettivo per cui sono

---

[391] Cfr. MCGUIRE M., *Organised Crime in the Digital Age*, John Grieve Centre for Policing and Security, Londra, 2012.
[392] Cfr. LUSTHAUS J., *How organised is organised cybercrime?*, cit., pp. 52-60.
[393] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 18**;** BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cybercrime: an analysis of the nature of groups engaged in cyber crime*, cit., pp. 9-10.
[394] *Ibidem*.

stati ingaggiati, questi soggetti vengono solitamente esclusi o abbandonati dal gruppo. Si tratta, dunque, di figure generalmente considerate usa e getta all'interno del sistema criminale, soprattutto se agiscono in modo inconsapevole[395].

Un esempio emblematico è quello dei già menzionati "*money mule*", ovvero persone reclutate — spesso tramite annunci ingannevoli online o false offerte di lavoro — per utilizzare i propri conti bancari (o aprirne di nuovi) al fine di ricevere, movimentare o trasferire somme di denaro di origine illecita[396].

3. Classificazione teleologica dei cybercriminali

Una classificazione particolarmente utile per comprendere le caratteristiche e le modalità operative dei gruppi criminali cibernetici, che verranno analizzati nei paragrafi successivi, è quella proposta da Van der Hulst e Neve[397].

Gli autori distinguono tre principali profili di cybercriminali, basandosi sulle motivazioni che li spingono ad agire. Questa suddivisione permette non solo di leggere le azioni dei singoli cybercriminali, ma anche di interpretare la composizione e le finalità dei gruppi di cui fanno parte.

La prima categoria è costituita da giovani maschi, spesso adolescenti o appena entrati nell'età adulta, che si avvicinano al mondo dell'hacking per gioco, curiosità, sfida personale o desiderio di affermazione sociale. Questi soggetti non sono necessariamente motivati da intenti criminali in senso stretto, ma piuttosto da un bisogno di riconoscimento e appartenenza, o dal fascino per la tecnologia; le loro azioni possono però avere conseguenze anche gravi, soprattutto quando, per inesperienza o sottovalutazione del rischio, violano sistemi sensibili o accedono a dati riservati. In molti casi, questi individui agiscono in reti informali, prive di una vera struttura gerarchica, e vengono cooptati in gruppi più organizzati solo successivamente, una volta dimostrate le proprie capacità[398].

---

[395] *Ibidem***.**
[396] *Ibidem***;** in proposito si veda anche United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 18; cfr. anche LEUKFELDT R.E., LAVORGNA A., KLEEMANS R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., pp. 290 ss
[397] VAN DER HULST R.C., NEVE R.J.M., *High-tech crime*, *Soorten Criminaliteit En hun daders*, *Een literatuurinventarisatie*, The Hague: WODC, 2008, pp. 106 e 107, richiamato da KOOPS B., *The Internet and its Opportunities for Cybercrime,* in *Tilburg Law School Legal Studies Research Paper Series*, 9, 2011, pp. 742 ss.
[398] *Ibidem.*

Il caso *Dreamboard* rappresenta un esempio paradigmatico di gruppo criminale cibernetico in cui le attività illecite si intrecciano con dinamiche di gioco, appartenenza e desiderio di affermazione sociale. All'interno di tale comunità online, chiusa e fortemente strutturata, i membri non erano mossi unicamente da fini economici o predatori, ma anche dalla ricerca di status all'interno di una gerarchia interna, costruita sulla base della partecipazione attiva e della quantità di contenuti condivisi. Il mantenimento dell'accesso alla piattaforma richiedeva, infatti, un coinvolgimento costante, e i partecipanti acquisivano visibilità e riconoscimento attraverso un sistema interno di livelli e ruoli[399].

La rete era caratterizzata da un'elevata attenzione alla sicurezza e all'anonimato: gli utenti operavano sotto pseudonimo, utilizzavano connessioni criptate e accedevano alla piattaforma tramite server proxy, strumenti finalizzati a oscurare la reale posizione geografica degli utenti e a rendere complesso il tracciamento delle attività da parte delle autorità; le regole di partecipazione e condotta erano redatte in più lingue a testimonianza dell'estensione internazionale del fenomeno. I server erano localizzati negli Stati Uniti, mentre alcuni degli amministratori principali risultavano operare da Paesi come la Francia e il Canada[400].

Nel 2009, a seguito di attività investigative coordinate, ha preso avvio l'Operazione Delego, un'importante iniziativa condotta dall'U.S. Immigration and Customs Enforcement (ICE) e dalla Child Exploitation and Obscenity Section (CEOS) del Dipartimento di Giustizia degli Stati Uniti, con la collaborazione di numerose autorità giudiziarie e forze di polizia internazionali. Tale operazione ha portato allo smantellamento della rete Dreamboard, con l'incriminazione di 72 persone in 14 Paesi distribuiti su cinque continenti. Al momento della conclusione delle indagini, risultavano arrestate 55 persone, sia negli Stati Uniti che all'estero[401].

Le prove raccolte nel corso dell'indagine hanno messo in luce il grave impatto delle attività criminali del gruppo, che aveva coinvolto un numero significativo di minori in condizioni di particolare vulnerabilità[402].

---

[399] Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cybercrime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 13; anche United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16; SANDOIU A., *Combating organised crime: The analysis, effects, and control of crimes committed by means of the emerging Dark Net*, Ambassadeurs de la Jeunesse, 2019, p. 8.
[400] *Ibidem.*
[401] *Ibidem.*
[402] *Ibidem.*

La seconda tipologia di cyber criminali include quelli "ideologicamente o politicamente motivati", che si distinguono per un elevato livello di intelligenza, un'intensa motivazione all'apprendimento e, spesso, un forte orientamento identitario[403].

In questo gruppo rientrano gli hacktivisti, che utilizzano le competenze informatiche per promuovere cause politiche, sociali o culturali, talvolta operando in opposizione a governi, istituzioni o grandi corporation. Le loro azioni possono spaziare dalla semplice diffusione di informazioni all'interno di campagne di sensibilizzazione, fino ad attacchi informatici su larga scala, come i DDoS o la manipolazione di dati. Non mancano comunque, all'interno di questa categoria, soggetti ossessivi o antisociali, spinti da una profonda sfiducia nelle autorità o da sentimenti di alienazione, che possono trasformare il loro attivismo in forme di cyberterrorismo[404]. Tali hacker operano spesso in gruppi decentralizzati, dove la leadership è condivisa o assente, e le azioni si coordinano intorno a obiettivi comuni, più che tramite una gerarchia formale[405].

A questo proposito, vale la pena menzionare il collettivo *Anonymous*, che nasce nel 2003 all'interno della piattaforma imageboard *4Chan*, in origine come un'aggregazione informale e fluida di individui accomunati da interessi comuni nel mondo digitale, quali l'anonimato, il gusto per la provocazione e una particolare inclinazione alla trasgressione. In questa fase embrionale, dunque, il gruppo si configurava come una rete di *hackers* e *pranksters*, privo di una struttura gerarchica formale, ma che vedeva emergere figure che, in modo spontaneo, assumevano ruoli di coordinamento nelle operazioni, dando luogo a una forma di organizzazione distribuita[406].

---

[403] Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cybercrime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 13; sul punto, anche NURSE J., BADA M., *The Group element of cybercrime: types, dynamics and criminal operations*, in *The Oxford handbook of cyberpsychology*, DOI: 10.1093/oxfordhb/9780198812746.013.36, 2018, p. 6.

[404] Cfr. ROMAGNA M., RUTGER LEUKFELDTB E., *Hacktivism: From Loners to Formal Organizations? Assessing the Social Organization of Hacktivist Networks,* in *Deviant Behavior*, 2024, in cui gli Autori mostrano come tali gruppi si caratterizzino per piccoli team ben organizzati, con compiti e ruoli distinti, pur mantenendo un panorama complessivamente eterogeneo; l'analisi evidenzia inoltre l'importanza delle azioni individuali, dell'affiliazione con soggetti affini, dell'esistenza di regole interne e delle competenze di hacking quali fattori determinanti dell'influenza all'interno del gruppo..

[405] *Ibidem*; cfr. anche CHOO K.R., SMITH R.G., *Criminal Exploitation of Online Systems by Organised Crime Groups,* cit., p. 42.

[406] Cfr. MC GOVERN V., FORTIN F., *The Anonymous Collective: Operations and Gender Differences*, in *Women and Criminal Justice*, 30, 2, 2019, pp. 91-105; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16; WALL D., *Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, in *The European Review of Organized Crime*, 2, 2, 2015, pp. 82-83; MINNAAR A., *Organised Crime And The 'New More Sophisticated' Criminals Within The Cybercrime Environment: How 'Organised' Are They In The Traditional Sense?,* cit. p. 139.

A partire dal 2008, Anonymous inizia a orientare le proprie azioni verso finalità più chiaramente politiche, avviando una progressiva transizione da fenomeno ludico e provocatorio a forma di attivismo digitale strutturato (*hacktivism*). L'azione contro la Chiesa di Scientology, nota come *Project Chanology*, segna un primo momento di forte visibilità pubblica; in tale occasione, furono utilizzati attacchi *Distributed Denial of Service* (DDoS) per contrastare le pratiche ritenute opache e autoritarie dell'organizzazione religiosa[407].

Il 2010 rappresenta un punto di svolta per Anonymous, con l'operazione in difesa di *WikiLeaks* e del suo fondatore Julian Assange, in seguito alla decisione di alcune piattaforme finanziarie — tra cui PayPal, Visa e MasterCard — di bloccare le donazioni al sito. In risposta, il collettivo ha lanciato una campagna di attacchi informatici volta a sabotare i portali web di tali enti, rafforzando così la propria immagine di attore impegnato nella tutela della libertà di informazione e della trasparenza istituzionale. Questo episodio ha segnato il passaggio definitivo del gruppo a una dimensione di militanza politica, posizionandolo tra i principali protagonisti della resistenza digitale globale[408].

A seguire, negli anni successivi, Anonymous ha ampliato il proprio campo d'azione con una serie di operazioni contro gruppi estremisti, istituzioni autoritarie e soggetti ritenuti responsabili di ingiustizie sociali. Tra le campagne più rilevanti si annoverano l'azione contro i responsabili dell'attacco alla redazione del periodico satirico *Charlie Hebdo*, l'*Operation Ice ISIS* — finalizzata a interrompere le attività online di reclutamento dell'organizzazione jihadista — e l'*Operation KKK*, durante la quale sono stati resi pubblici i nominativi di presunti affiliati al Ku Klux Klan[409].

Guardando, infine, alla terza categoria di cyber criminali, si individuano i gruppi criminali mossi invece da interessi economici, una delle componenti più rilevanti nel panorama del *cybercrime* contemporaneo.

Questi individui possono avere provenienze e competenze molto diverse, ma condividono l'obiettivo di ottenere un profitto diretto dalle loro attività illegali: alcuni possiedono un alto livello di specializzazione tecnica e sono in grado di sviluppare

---

[407] *Ibidem.*
[408] Cfr. Mc Govern V., Fortin F., *The Anonymous Collective: Operations and Gender Differences*, in *Women and Criminal Justice*, 30, 2, 2019, pp. 91-105.
[409] *Ibidem*.

strumenti sofisticati come *malware*, *ransomware* o *exploit* su misura; altri invece agiscono come "esecutori" o intermediari all'interno di organizzazioni più ampie, svolgendo compiti specifici (ad esempio, riciclaggio di denaro, logistica o phishing). Spesso operano in gruppi strutturati gerarchicamente, che si comportano come vere e proprie imprese criminali, con divisione del lavoro, ruoli ben definiti e sistemi di comunicazione cifrata. È proprio in questi contesti che si osservano forme di collaborazione transnazionale, con reti che sfruttano la globalizzazione e l'anonimato della rete per operare su vasta scala[410].

Koobface rappresenta uno degli esempi più noti di *malware* concepito esplicitamente per fini economici. Si tratta di un *worm*[411] che ha colpito principalmente i social network dell'era Web 2.0, in particolare Facebook — da cui deriva il nome stesso, costituito come anagramma. Il meccanismo di diffusione prevedeva l'invio automatico di messaggi agli "amici" degli utenti infettati, contenenti un link a un sito fraudolento. A questi utenti veniva suggerito di scaricare un presunto aggiornamento che, in realtà, installava il *malware* sul dispositivo[412].

Una volta attivo, Koobface alterava il comportamento del browser dell'utente, ridirezionando la navigazione verso siti affiliati di natura truffaldina. Tali siti proponevano offerte ingannevoli - come falsi investimenti, software antivirus contraffatti, finti servizi di incontri o contenuti per adulti - il cui unico scopo era quello di generare entrate economiche per gli sviluppatori del malware. Il profitto derivava principalmente da modelli di guadagno basati su pay-per-click e pay-per-install[413], garantendo una rendita significativa ogni qualvolta un utente interagiva con uno di questi contenuti[414].

---

[410] Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 13; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16.

[411] Il "worm" è un programma malevolo che, a differenza del virus, non ha bisogno di essere attaccato ad un file per propagarsi; nel caso di Koobface, ad esempio, il malware si diffondeva attraverso l'invio di link malevoli.

[412] Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 13; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16.

[413] Nei circuiti criminali viene sfruttato il pay-per-click per commettere frodi: bot o malware simulano clic su banner, generando profitti illeciti per chi controlla il traffico; il pay-per-install prevede, in ambito criminale, che diffonde malware (ad esempio tramite phishing o siti pirata) viene pagato per ogni installazione riuscita.

[414] Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 13; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16.

Secondo l'azienda di cybersicurezza Sophos, dietro Koobface vi era un'organizzazione composta da cinque soggetti, attiva tra la Russia e la Repubblica Ceca. Il gruppo, soprannominato "Ali Baba & i 4", si era già precedentemente cimentato in attività digitali borderline, tra cui pornografia online e diffusione di spyware, tentando anche di avviare un'impresa legittima nel settore del software mobile. Nonostante i ripetuti tentativi di neutralizzazione da parte di grandi piattaforme come Facebook e Google, Koobface ha dimostrato una notevole resilienza, riuscendo a sopravvivere grazie alla costante evoluzione delle sue componenti e a un sofisticato sistema di gestione del traffico verso i siti affiliati[415].

Le stime ricavate dai server di comando e controllo del malware indicano guadagni annuali pari a circa 2 milioni di dollari, confermando come l'intero progetto fosse orientato primariamente al profitto economico[416].

4. Principali attività dei cybercriminali

Come già approfondito nei capitoli precedenti, nel panorama della criminalità contemporanea di tipo informatico, che contraddistingue i gruppi di tipo I e di tipo II, il ruolo delle tecnologie digitali non si limita a un mero strumento accessorio, ma costituisce spesso l'essenza stessa dell'azione criminosa.

La criminalità informatica si sviluppa, infatti, a partire da una profonda interconnessione tra l'evoluzione tecnologica e le nuove modalità di progettazione e realizzazione dei reati. In particolare, la natura dei cosiddetti crimini cyber-dipendenti evidenzia chiaramente come tali illeciti non possano esistere al di fuori dell'ambiente digitale: è bene ricordare, infatti, che si tratta di reati che prendono forma e significato unicamente grazie all'impiego delle tecnologie dell'informazione e della comunicazione, le quali non solo facilitano la realizzazione dell'illecito, ma ne costituiscono altresì il fondamento strutturale[417].

---

[415] *Ibidem.*
[416] *Ibidem.*
[417] Si veda sui cyber-dependent crimes, KRANENBARG M., *Cyber-Dependent Crime Versus Traditional Crime*, in *Kranenbarg, and Leukfeldt, Cybercrime in context: The human factor in victimization, offending, and policing,* cit., pp. 195-216; MCGUIRE M., DOWLING S., *Cybercrime: A Review of the Evidence: Summary of Kedy Findings and Implications*, Home Office, London, UK, 2013.

Questa tipologia di crimini colpisce direttamente i pilastri fondamentali su cui si fondano i sistemi informatici: la riservatezza, ovvero la protezione dell'accesso ai dati da parte di soggetti non autorizzati; l'integrità, che garantisce la correttezza e l'affidabilità delle informazioni trattate; e la disponibilità, intesa come la possibilità di accedere ai sistemi e alle risorse informatiche quando necessario. È proprio attaccando questi tre principi cardine che i cybercriminali riescono a compromettere in maniera significativa la sicurezza dei dati e delle infrastrutture digitali[418].

Avendo già esaminato nei precedenti capitoli la differente categorizzazione dei crimini commessi dalle organizzazioni criminali in base al rapporto con la tecnologia, è ora opportuno soffermarsi in maniera più dettagliata su alcuni dei reati cibernetici più noti e diffusi, così da comprendere concretamente le manifestazioni della criminalità cibernetica.

La criminalità organizzata cibernetica, indipendentemente dal fatto che sia esclusivamente, o solo parzialmente, cibernetica – riferendosi quest'ultima suddivisione, come già detto, alla sola componente organizzativa e non invece alle attività[419] – non si limita alla perpetrazione di crimini cyber-dipendenti, ma si rende spesso responsabile anche di reati tradizionali che la tecnologia contribuisce a facilitare o potenziare. È proprio questa duplice dimensione operativa – esclusivamente digitale da un lato, e digitalmente agevolata dall'altro – a rendere la criminalità informatica particolarmente insidiosa e adattabile.

Saranno quindi analizzate le principali condotte illecite, distinguendo tra quelle che dipendono in modo esclusivo dalla tecnologia e quelle che, pur esistendo anche in forma fisica, trovano nel contesto digitale un terreno fertile per una nuova e più efficace modalità di attuazione.

Uno dei crimini più diffusi in questa categoria è l'accesso illegale ai sistemi informatici, noto comunemente come hacking[420]. Questo fenomeno comprende tutte le attività volte a penetrare nei sistemi informatici senza autorizzazione, oppure a superare

---

[418] Per un'analisi e una classificazione dei *cybercrimes* e dei beni giuridici tutelati, si rinvii a PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in Id., (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova 2004, p. 21 ss

[419] Si rinvia per questa distinzione a sez. I, cap. I, par. 4.2.

[420] Cfr. United Nations Office on Drugs and Crime, Cybercrime Module 2 on General Types of Cybercrime; il termine "hacking", tuttavia, non è incluso nelle leggi multilaterali, regionali e nazionali sulla criminalità informatica. Vengono invece utilizzati i termini "accesso illegale" o "accesso non autorizzato".

i limiti dell'accesso consentito. Come visto, gli hacker possono essere mossi da motivazioni diverse: dal guadagno economico all'attivismo politico, dalla semplice curiosità al desiderio di affermare la propria abilità nel contesto di comunità underground. Una volta ottenuto l'accesso, il cybercriminale può sottrarre, modificare, cancellare o danneggiare informazioni e sistemi, causando danni spesso ingenti sia a privati che a organizzazioni pubbliche e private[421].

Ulteriore attività criminale tipica è l'intercettazione o acquisizione illecita di dati, che consiste nella cattura non autorizzata di informazioni digitali in transito, come email, credenziali di accesso o dati bancari[422]. A questa si aggiunge l'interferenza nei dati e nei sistemi, ovvero l'alterazione, la cancellazione, l'inserimento o il deterioramento di dati, così come l'ostruzione del funzionamento dei sistemi informatici[423]. Questi attacchi compromettono direttamente la funzionalità e l'affidabilità delle infrastrutture digitali, con ripercussioni che possono estendersi alla sicurezza nazionale, specialmente quando colpiscono settori strategici come sanità, energia o trasporti.

Di particolare rilevanza è anche il possesso e l'utilizzo improprio di dispositivi informatici[424], come *malware*, *spyware*, *keylogger* o *trojan*, progettati appositamente per compromettere i sistemi, eludere i controlli di sicurezza o acquisire informazioni sensibili. Questi strumenti sono spesso commercializzati nei circuiti del dark web, e possono essere personalizzati in base agli obiettivi specifici dei criminali.

---

[421] Cfr. art. 2, Convenzione del Consiglio d'Europa sulla criminalità informatica, che include il termine "accesso illegale", definito come l'intenzionale "*accesso senza diritto alla totalità o a una parte di un sistema informatico*"; cfr, anche nel nostro ordinamento l'art. 615 ter c.p.

[422] Cfr. nel nostro ordinamento art. 167 ter codice della privacy – "Acquisizione fraudolenta di dati personali"; v. anche nell'art. 3 della Convenzione del Consiglio d'Europa l'"intercettazione illegale" è definita come "*l'intercettazione intenzionale senza diritto, effettuata con mezzi tecnici, di trasmissioni non pubbliche di dati informatici verso, da o all'interno di un sistema informatico, comprese le emissioni elettromagnetiche provenienti da un sistema informatico che trasporta tali dati informatici*".

[423] Cfr. nel nostro ordinamento l'art. 635 *bis* c.p. "Danneggiamento di informazioni, dati e programmi informatici"; vedi anche Cfr. United Nations Office on Drugs and Crime, Cybercrime Module 2 on General Types of Cybercrime**;** l'art. 4 della Convenzione del Consiglio d'Europa sulla criminalità informatica, l'interferenza nei dati è considerata reato quando è "*commessa intenzionalmente*" e comporta il "*danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici senza diritto*" e, inoltre, l'art. 5 della stessa Convenzione spiega che l'interferenza nel sistema è considerata illegale quando è commessa intenzionalmente e ostacola gravemente e senza diritto il funzionamento di un sistema informatico inserendo, trasmettendo, danneggiando, cancellando, deteriorando, alterando o sopprimendo dati informatici.

[424] Articolo 6, paragrafo 1 a, della Convenzione del Consiglio d'Europa sulla criminalità informatica.

Parallelamente ai crimini cyber-dipendenti, si ravvisa la commissione di crimini informatici in senso più ampio, ovvero quei reati tradizionali che si avvalgono delle tecnologie ICT per essere commessi con maggiore efficacia o su scala globale.

Tra questi, le frodi e le falsificazioni informatiche rappresentano una delle minacce più frequenti. La frode può consistere nella manipolazione di sistemi o dati digitali con lo scopo di ottenere un indebito guadagno economico, come avviene nei casi di *phishing*, *smishing*, truffe online o frodi telefoniche (es. SIM box fraud)[425]. La falsificazione, invece, riguarda l'alterazione di dati con l'intento di renderli apparentemente autentici[426].

Un'altra forma grave di criminalità digitale è costituita dai reati contro l'identità, che comprendono il furto e l'uso illecito di identità digitali per realizzare truffe, frodi o altri reati. I dati personali rubati – come numeri di carte di credito, password, indirizzi email o documenti d'identità – vengono spesso rivenduti nei mercati clandestini online e rappresentano una merce di grande valore economico[427]. A questi si affiancano i crimini legati alla contraffazione di beni e documenti, illegalmente rivenduti sia nel mondo fisico che in quello virtuale, spesso per finanziare organizzazioni criminali più ampie[428].

Tra le pratiche più pericolose rientrano poi la cyberestorsione[429] e il *ransomware*[430], tecniche attraverso le quali i criminali minacciano di diffondere dati sensibili o bloccano l'accesso a sistemi informatici, richiedendo un riscatto in cambio della restituzione delle funzionalità. Forme particolarmente gravi di ricatto digitale sono la *sextortion*, in cui si minaccia la pubblicazione di contenuti intimi, e le truffe di riscatto, in cui le vittime vengono ingannate da falsi agenti di polizia, banche o avvocati[431]. Infine, non possono non menzionarsi i crimini legati allo sfruttamento sessuale di minori, alla tratta di esseri umani e al traffico di migranti, fenomeni che si avvalgono delle tecnologie per adescare,

---

[425] Articolo 8 della Convenzione del Consiglio d'Europa sulla criminalità informatica

[426] Articolo 7 della Convenzione del Consiglio d'Europa sulla criminalità informatica.

[427] Vedi anche United Nations Office on Drugs and Crime, Cybercrime Module 2 on General Types of Cybercrime, "Reati informatici".

[428] Cfr. ALBANESE J., *Cybercrime as an Essential Element in Transnational Counterfeiting Schemes. Presentation at International Academic Conference: Linking Organized Crime and Cybercrime*, UNODC, 2018.

[429] Individui, gruppi, organizzazioni private, organizzazioni non governative e agenzie governative sono obiettivi comuni dell'estorsione. Quando l'estorsione è facilitata tramite le ICT, si parla di cyberestorsione.

[430] Come detto, il ransomware rappresenta una delle forme più dannose di malware, in quanto combina il blocco o la cifratura dei dati con l'estorsione economica. La sua diffusione su scala globale, evidenziata anche nel rapporto *Internet Organised Crime Threat Assessment 2020* di Europol, dimostra come non siano solo i singoli utenti a essere colpiti, ma anche aziende e istituzioni pubbliche, rendendolo una minaccia trasversale e persistente.

[431] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 47.

controllare, pubblicizzare e coordinare le attività criminali. I social network, le chat room e le piattaforme di annunci vengono spesso utilizzati per ingannare le vittime, nascondere le identità degli autori e aggirare i controlli delle forze dell'ordine[432].

Nel 2023, gli attacchi ransomware, lo sfruttamento sessuale dei minori (CSE) e le frodi online hanno continuato a rappresentare le manifestazioni più minacciose della criminalità informatica nell'Unione Europea (UE)[433].

5. Le associazioni a delinquere esclusivamente cibernetiche o gruppi di tipo I

5.1. Le due diverse configurazioni dei gruppi dei cybercriminali: swarms e hubs

Nel modello di suddivisione e scomposizione dei gruppi di McGuire, i gruppi di tipo I, che operano principalmente online, sono classificati in due categorie principali: *swarms* e *hubs*. Questa distinzione evidenzia una doppia ramificazione nella struttura e nelle modalità operative di tali gruppi[434].

Gli *sciami* sono gruppi temporanei, decentralizzati e privi di una struttura di comando rigida, composti da individui che si uniscono per un periodo limitato con l'obiettivo di compiere un crimine informatico specifico[435].

La loro caratteristica principale è, pertanto, la fluidità e la mancanza di continuità, in quanto il gruppo si costituisce per il raggiungimento dell'obiettivo comune e si dissolve una volta raggiunto, e alcuni o tutti i membri possono separarsi per unirsi ad altri sciami in futuro. Ciò si spiega se si osservano le motivazioni che spingono alla commissione dei crimini: questi gruppi si formano principalmente attorno a motivazioni ideologiche, come il desiderio di esprimere una protesta o diffondere una causa, piuttosto che per ottenere un guadagno materiale[436].

---

[432] *Ibidem*.
[433] Europol, *Internet Organised Crime Threat Assessment*, IOCTA, 2024, Publications Office of the European Union, Luxembourg.
[434] Cfr. MCGUIRE M., *Organized Crime in the Digital Age*, cit.
[435] United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., pp. 15-16; Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 7; Cfr. DI NICOLA A., *Towards digital organized crime and digital sociology of organized crim*e, cit., pp.10-11.
[436] *Ibidem.*

Accanto alla temporanea partecipazione dei membri, si rileva altresì una struttura organizzativa generalmente minimale, con una leadership che può emergere in modo informale, ma che non è rigidamente definita[437].

Gli sciami operano in modo autonomo, con ogni membro che svolge un ruolo relativamente indipendente, senza un sistema complesso di comando o gerarchie tradizionali[438].

Un esempio di sciame è il gruppo *hacktivista* Anonymous, che, pur non avendo un leader formale, presenta comunque una certa organizzazione interna, con alcuni membri che prendono l'iniziativa di organizzare, pianificare e decidere le azioni collettive[439].

Nonostante la natura temporanea e meno strutturata degli sciami, questi gruppi sono comunque in grado di organizzare e realizzare attacchi informatici complessi. Tuttavia, nella maggior parte delle giurisdizioni, gli sciami non vengono considerati gruppi criminali organizzati, a meno che non perseguano un obiettivo di natura materialistica.

In sostanza, gli sciami rappresentano una forma di crimine informatico che sfida le tradizionali definizioni di crimine organizzato, in quanto la loro natura temporanea e decentralizzata non rispecchia i modelli convenzionali di criminalità organizzata[440].

D'altro canto, invece, un *hub* ("centro di potere") è un gruppo criminale altamente strutturato, caratterizzato dalla presenza di un nucleo centrale di criminali che gestiscono direttamente le operazioni, mentre i membri periferici svolgono compiti più specifici sotto il controllo di questo nucleo[441].

La struttura di comando degli *hub* è gerarchica e definita, con una divisione chiara dei ruoli: i membri di livello più alto prendono le decisioni e dirigono le attività più articolate, mentre quelli di livello inferiore sono responsabili di eseguire compiti meno complessi, come la distribuzione del materiale illecito o l'attuazione di attacchi informatici. Questo sistema gerarchico garantisce che le operazioni vengano condotte in modo ordinato,

---

[437] *Ibidem.*
[438] *Ibidem.*
[439] *Ibidem.*
[440] Vedi United Nations Office on Drugs and Crime, Mod. 13, *Criminal groups engaging in cyber organized crime*.
[441] In proposito, United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., pp. 15-16; Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 7; Cfr. DI NICOLA A., *Towards digital organized crime and digital sociology of organized crim*e, cit., pp.10-11.

minimizzando il rischio di disorganizzazione e mantenendo un controllo centralizzato su tutte le attività criminali[442].

La struttura rigida consente, inoltre, di suddividere i membri nell'ambito di diversi gruppi che dispongono di accessi e responsabilità differenziate, poiché i membri di livello superiore godono di maggiori vantaggi, come l'accesso a risorse più esclusive o informazioni riservate. Questo sistema di incentivi e punizioni, tipico delle organizzazioni gerarchiche, favorisce la cooperazione e la fedeltà all'interno del gruppo[443].

Un esempio emblematico di questo tipo di struttura è Dreamboard, una rete criminale che distribuiva materiale pedopornografico esclusivamente tra i suoi membri. All'interno di Dreamboard, i membri erano suddivisi in categorie diverse: a differenza dei membri VIP, infatti, i SuperVIP, avevano accesso a contenuti e materiale più esclusivo e producevano il proprio materiale. Inoltre, trattandosi di un *hub*, i membri di Dreamboard dovevano rispettare regole precise per rimanere all'interno del gruppo, con penalità severe per chi non rispettava gli obblighi[444].

5.2. Le comunità online di pedofili: struttura, tecniche operative e capacità di adattamento

Con l'espansione di internet, anche il fenomeno della pedofilia ha subito una trasformazione radicale. Se prima dell'era digitale i soggetti con tendenze pedofiliche operavano in ambienti isolati, basati su un'alta selettività e su un'intensa fiducia interpersonale, oggi la rete ha favorito la nascita di vere e proprie comunità virtuali, in cui questi soggetti possono connettersi, riconoscersi e collaborare. Tali spazi digitali non sono soltanto luoghi di condivisione di materiale pedopornografico, ma anche ambienti in cui si consolidano dinamiche collettive di sostegno reciproco, razionalizzazione ideologica e scambio di competenze operative.

Le piattaforme utilizzate sono molteplici e comprendono newsgroup, social network, bulletin board, reti peer-to-peer, chat room e applicazioni di messaggistica istantanea[445]. L'ambiente digitale fornisce agli utenti un senso di anonimato che non solo favorisce

[442] *Ibidem*.
[443] *Ibidem*.
[444] Su Dreamboard v. *United States of America v. John Doe #1, Edward Odewaldt, et al*., Case n.. 10-CR-00319, (W.D. Louisiana, 16 March 2011).
[445] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 77.

l'interazione, ma abbassa drasticamente le barriere all'azione, rendendo pratiche, altrimenti stigmatizzate, socialmente più "accessibili" e "sicure"[446].

La condivisione di contenuti illeciti avviene oggi anche attraverso canali crittografati, spesso in modalità uno-a-uno o all'interno di gruppi ristretti, specialmente su app largamente diffuse come WhatsApp[447].

L'analisi di inchieste giudiziarie condotte su comunità pedofile ne rivela svariati tratti comuni.

Tali reti hanno frequentemente una portata transnazionale, resa possibile dalla natura globale del cyberspazio. La regola dell'anonimato è imprescindibile: gli utenti nascondono la propria identità e l'interazione è limitata al solo ambito virtuale. La condivisione imprudente di dati personali può mettere in pericolo l'intera rete, motivo per cui comportamenti sospetti vengono spesso sanzionati con l'espulsione[448].

Non di rado, queste comunità contengono sezioni specifiche dedicate a insegnare come adescare minori, come evitare la sorveglianza e come produrre contenuti pedopornografici. Accanto a questi scopi operativi, trovano spazio anche *thread* dedicati alla giustificazione morale delle proprie condotte e alla condivisione di manuali per la sicurezza digitale[449]. In parallelo, Europol segnala la pubblicazione ricorrente di materiali informativi e di sintesi sulle operazioni delle forze dell'ordine, con l'obiettivo di migliorare la sicurezza collettiva[450].

Le comunità differiscono notevolmente per dimensioni e grado di strutturazione. Alcune appaiono come gruppi informali, accessibili dal web di superficie e con scarsa regolamentazione interna. Altre operano nel dark web, sono altamente strutturate e impongono severe regole di accesso, rigidi codici di condotta, divisione dei compiti e gerarchie interne simili a quelle di vere organizzazioni criminali[451].

L'affiliazione è selettiva e l'avanzamento di rango è correlato al contributo offerto alla comunità — come la produzione e la diffusione di contenuti, l'incoraggiamento all'abuso o il supporto tecnico agli altri membri[452].

---

[446] Sul punto, PICARELLA L., *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, cit., 2025.
[447] Cfr. Europol, *Internet organized crime threat assessment*, IOCTA, 2020, p. 38.
[448] Sul punto, PICARELLA L., *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, cit., 2025.
[449] *Ibidem*.
[450] Cfr. Europol, *Internet organized crime threat assessment*, IOCTA, 2020, p. 38.
[451] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 77.
[452] Cfr. Europol, *Internet organized crime threat assessment*, IOCTA, 2020, p. 38.

Le strategie di occultamento si sono evolute parallelamente alla crescita dell'offerta tecnologica. Si registra un'intensificazione nell'uso di canali crittografati, non solo su Tor, ma anche su piattaforme più comuni, rendendo sempre più complesso il lavoro delle autorità investigative[453].

Un ulteriore livello di sofisticazione è rappresentato dalla tendenza di questi soggetti a formare comunità chiuse e ristrette, talvolta accessibili solo tramite invito, considerate più sicure rispetto ai forum pubblici del dark web. In alcuni casi, si infiltrano in gruppi già esistenti frequentati da minori, creando nuovi sottogruppi misti composti da adulti e bambini[454]. Le comunità più coese si dimostrano estremamente resilienti: reagiscono alla chiusura di piattaforme o all'arresto di membri con la creazione di nuovi spazi, la migrazione verso tecnologie alternative o la resurrezione di forum precedenti[455].

L'analisi della struttura organizzativa di queste comunità e la valutazione della loro possibile riconducibilità alla nozione penalistica di "associazione per delinquere", ai sensi dell'art. 416 c.p., costituirà oggetto di approfondimento nel capitolo successivo.

5.3. Le organizzazioni di hacktivisti

Nel dibattito contemporaneo sulla sicurezza informatica, è fondamentale distinguere tra le figure dell'hacker, del cracker e dell'hacktivista, poiché ciascuna incarna motivazioni, metodi e implicazioni etiche differenti. Il termine "hacker", sebbene comunemente associato a pratiche illegali, ha origini meno negative: inizialmente designava individui dotati di un alto livello di competenza tecnica, spinti da curiosità intellettuale e desiderio di esplorare i sistemi informatici per comprenderne il funzionamento[456]. Questa accezione, tuttora riconosciuta in ambienti tecnici e accademici, si contrappone alla visione più popolare che equipara l'hacker a un criminale informatico.

Di contro, il termine "cracker" si è consolidato per indicare coloro che, pur possedendo competenze simili, agiscono con intento malevolo, come violare la sicurezza dei sistemi,

---

[453] *Ibidem*.
[454] *Ibidem*.
[455] *Ibidem*.
[456] DITTRICH D., HIMMA K.E., *Hackers, Crackers, and Computer Criminals*, in *Handbook of Information Security, Information Warfare, Social, Legal, and and International Issues and Security Foundations*, edito da Bidgoli H., 2, 2006, p. 154 ss.

sottrarre dati o danneggiare infrastrutture digitali. In questa distinzione, i cracker sono considerati gli attori principali delle attività informatiche illecite, spesso mossi da interessi personali, economici o da una volontà di sopraffazione[457].

Ne consegue, pertanto, che mentre l'hacker, nella sua accezione più classica e originaria, è animato da una logica esplorativa e creativa, il cracker, invece, si appropria delle medesime competenze tecniche per fini distruttivi o personali, come il sabotaggio, il furto di dati o l'estorsione, guidato dall'interesse individuale, dal profitto economico o dalla volontà di causare danni, collocandosi così in contrasto diretto con l'etica hacker[458].

La comunità informatica, in particolare nei primi anni della cultura hacker, ha sempre cercato di tracciare una linea distintiva tra l'hacking come pratica intellettuale e creativa e il cracking come comportamento antisociale o criminoso. Tuttavia, tale distinzione è spesso difficile da mantenere al di fuori di contesti specializzati, dove prevale una percezione semplificata e sensazionalistica del fenomeno.

All'interno di queste dinamiche, assume rilievo anche la figura dell'hacktivista, una categoria che unisce le tecniche dell'hacking con motivazioni politiche o ideologiche. Gli hacktivisti impiegano strumenti informatici per protestare, diffondere messaggi o destabilizzare infrastrutture percepite come oppressive, spesso attraverso azioni simboliche, come il *defacement* di siti web istituzionali, o azioni più intrusive come il rilascio di documenti riservati[459].

Ne consegue, pertanto, che nel contesto della sicurezza informatica, la distinzione tra hacker, cracker e hacktivisti non può prescindere da un'attenta analisi delle motivazioni che guidano le loro azioni. Se da un lato esistono sovrapposizioni nei mezzi tecnici impiegati, dall'altro lato, è proprio l'intenzione sottesa all'attività di intrusione o manipolazione dei sistemi informatici a costituire la chiave interpretativa più significativa per comprendere la differenza tra queste figure. Inoltre, le motivazioni non solo contribuiscono a distinguere il lecito dall'illecito, ma chiariscono anche il ruolo sociotecnico che tali soggetti rivestono nella rete globale.

---

[457] *Ibidem*.
[458] *Ibidem*.
[459] *Ibidem*; in proposito si veda altresì ROMAGNA M., RUTGER LEUKFELDTB E., *Hacktivism: From Loners to Formal Organizations? Assessing the Social Organization of Hacktivist Networks,* in *Deviant Behavior*, 2024; anche ROMAGNA M., VAN DEN HOUT N.J., *Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats*, Virus Bullettin Conference October, Madrid, 2017.

Tra le motivazioni principali, emerge innanzitutto la curiosità intellettuale: molti hacker agiscono mossi dal desiderio di comprendere a fondo il funzionamento interno di sistemi complessi, spinti da un impulso esplorativo più che distruttivo. Si tratta spesso di individui altamente qualificati dal punto di vista tecnico, che considerano la penetrazione nei sistemi non autorizzati come una sfida personale, un esercizio di abilità logica e creativa. In questi casi, l'atto dell'hacking assume una dimensione quasi ludica, simile a un gioco mentale, in cui il superamento di barriere di sicurezza rappresenta un traguardo in sé, indipendentemente da ogni intenzione di arrecare danno. Questa motivazione è alla base dell'hacking "etico", dove l'intrusione è volta a segnalare vulnerabilità e migliorare la sicurezza dei sistemi[460].

Altri attori, però, sono spinti da motivazioni economiche, e qui il confine etico si fa più netto. I cosiddetti cracker entrano nei sistemi informatici per trarne profitto personale, attraverso attività come il furto di dati sensibili, le frodi con carte di credito, l'accesso a conti bancari o la distribuzione di *ransomware* per estorcere denaro. In questi casi, l'interesse economico è il motore principale dell'azione, e la tecnologia diventa uno strumento per la realizzazione di obiettivi illeciti. Tali attività, pur richiedendo competenze tecniche avanzate, si distinguono per l'intento deliberatamente criminale e l'assenza di qualsiasi giustificazione etica o sociale[461].

Una motivazione distinta, ma sempre più rilevante, è quella ideologica o politica, che dà origine alla figura dell'hacktivista.

Gli hacktivisti, come accennato, operano nella convinzione che l'informatica possa essere un mezzo di lotta contro ingiustizie sociali, abusi di potere o politiche oppressive. A differenza dei cracker, il loro obiettivo non è il guadagno personale, ma la diffusione di un messaggio o la difesa di una causa. Le loro azioni includono il *defacement* di siti istituzionali, la pubblicazione di documenti riservati o l'organizzazione di attacchi distribuiti contro organizzazioni percepite come dannose. Le motivazioni qui sono fortemente ideologizzate e inserite in una cornice etica, che giustifica la violazione delle leggi in nome di una giustizia percepita come superiore. In questo senso, l'hacktivismo si avvicina ad altre forme di disobbedienza civile digitale, dove la legittimità dell'atto è rivendicata sulla base della legittimità della causa[462].

---

[460] *Ibidem*.
[461] *Ibidem*.
[462] *Ibidem*.

Pur nascendo da motivazioni individuali fortemente ideologizzate – come il desiderio di giustizia sociale, la lotta alla censura, la difesa della libertà d'informazione o l'opposizione a governi autoritari e multinazionali – l'azione degli hacktivisti non si esaurisce nella dimensione soggettiva del dissenso digitale. Al contrario, per avere un impatto concreto e visibile, questi attori tendono ad aggregarsi in forme collettive di mobilitazione che, pur mantenendo una natura informale e fluida, assumono nel tempo le caratteristiche di vere e proprie entità organizzate. È in questo passaggio – dalla spinta motivazionale individuale all'azione coordinata su larga scala – che l'hacktivismo evolve, in alcuni casi, verso configurazioni strutturate riconducibili a forme di criminalità organizzata[463].

Questa transizione dal singolo alla rete non implica necessariamente un'adesione esplicita o formale a un'organizzazione: al contrario, una delle peculiarità dell'hacktivismo contemporaneo risiede proprio nella capacità di agire collettivamente senza una struttura gerarchica rigida o una leadership visibile[464].

Non a caso, uno degli elementi più caratteristici delle organizzazioni hacktiviste, che le distingue profondamente dalle tradizionali strutture criminali organizzate, è la loro architettura orizzontale e decentralizzata. A differenza delle mafie, dei cartelli o di altri gruppi del crimine organizzato, che si basano su una gerarchia rigida, con ruoli ben definiti e un comando centralizzato, i gruppi hacktivisti si configurano spesso come reti fluide, distribuite e in larga parte anonime, prive di un'autorità formale riconosciuta e con una leadership variabile, effimera o addirittura del tutto assente[465]. Questa struttura non gerarchica è uno degli aspetti più innovativi e, al contempo, più elusivi di tali gruppi, che possono apparire disorganizzati dall'esterno, ma che in realtà si basano su logiche operative altamente adattive e resilienti.

In questi contesti, il potere decisionale è generalmente distribuito tra nodi della rete che assumono ruoli sulla base della loro competenza tecnica, carisma digitale o capacità di influenza nel canale comunicativo utilizzato (come forum, chat IRC, Telegram, piattaforme del dark web o social network). Non esiste una catena di comando fissa: le

[463] *Ibidem*.
[464] Sulla struttura dei gruppi criminali di hacktivisti v. ROMAGNA M., RUTGER LEUKFELDTB E., *Hacktivism: From Loners to Formal Organizations? Assessing the Social Organization of Hacktivist Networks,* cit., p. 5; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16.
[465] *Ibidem*.

azioni vengono proposte, discusse e approvate attraverso un processo informale di consenso, spesso in spazi digitali criptati o chiusi, dove il contributo è volontario e la partecipazione può essere anonima o pseudonima. In alcuni casi, emerge una leadership situazionale, legata più alla capacità di iniziativa o al successo di un'azione che a un mandato strutturato[466].

Questa assenza di *leadership* formale non rappresenta una debolezza, ma al contrario costituisce uno dei punti di forza degli hacktivisti, soprattutto in ottica di resistenza alla repressione. Senza vertici identificabili, il gruppo non può essere smantellato attraverso arresti mirati, poiché, anche qualora alcuni membri vengano individuati o perseguiti, la rete tende a rigenerarsi rapidamente, mantenendo intatti gli obiettivi e le capacità operative. La dimensione reticolare favorisce, inoltre, una forma di intelligence collettiva: le informazioni, le competenze e le risorse sono condivise orizzontalmente, potenziando la capacità del gruppo di adattarsi e reagire in tempo reale alle evoluzioni del contesto[467].

Questa configurazione presenta, tuttavia, anche implicazioni giuridiche complesse.

In assenza di una catena di comando chiaramente identificabile, è difficile applicare le tradizionali categorie giuridiche relative all'associazione a delinquere, che presuppongono elementi come la stabilità dell'organizzazione, la suddivisione dei ruoli e l'esistenza di un fine criminoso comune. L'apparente spontaneità e informalità dei gruppi hacktivisti rende ardua anche la distinzione tra partecipanti attivi, simpatizzanti e semplici osservatori, complicando ulteriormente le indagini e la possibilità di configurare responsabilità penali individuali.

Nel caso di Anonymous, ad esempio – uno dei gruppi hacktivisti più noti e iconici – l'assenza di un'identità unica e definita è diventata un elemento distintivo: chiunque può prendere parte ad "Anonymous", purché aderisca temporaneamente a una causa o a un'azione. Il gruppo funziona quindi come un brand ideologico aperto, a cui si può accedere senza affiliazione formale, con una modalità di azione che privilegia l'efficacia simbolica e l'impatto mediatico, piuttosto che la continuità organizzativa[468].

---

[466] Cfr. ROMAGNA M., RUTGER LEUKFELDTB E., *Hacktivism: From Loners to Formal Organizations? Assessing the Social Organization of Hacktivist Networks,* cit., p. 5.
[467] Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., pp. 22 ss.
[468] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16.

6. Le associazioni a delinquere parzialmente cibernetiche o gruppi di tipo II

6.1. Le due diverse configurazioni dei gruppi ibridi dei cybercriminali: clustered ed extended

Come già visto, nel contesto della criminalità informatica organizzata, si stanno consolidando sempre più frequentemente modelli di associazioni ibride, ossia gruppi criminali in grado di operare con continuità e coerenza, tanto nel mondo digitale, quanto in quello fisico. Queste organizzazioni non si limitano a utilizzare strumenti informatici per potenziare reati tradizionali, ma manifestano una vera e propria integrazione tra dimensione online e offline, tanto sul piano operativo quanto su quello strutturale.

Appare evidente, dunque, che il concetto di "ibrido" può essere declinato secondo due assi analitici differenti ma complementari: da un lato, la struttura organizzativa[469]; dall'altro, la natura mista delle condotte criminali[470]. Questa duplice lettura consente di meglio comprendere la fluidità e complessità delle organizzazioni criminali nell'era digitale, le quali si sottraggono sempre più frequentemente alle categorie giuridiche tradizionali, richiedendo un ripensamento concettuale e normativo alla luce della smaterializzazione delle attività criminali e della destrutturazione delle catene di comando.

Picarella analizza la natura ibrida delle associazioni cibernetiche a partire non tanto dalle attività criminali poste in essere, quanto dalla collocazione della struttura organizzativa. Secondo l'autore, si deve parlare di associazioni esclusivamente cibernetiche quando sia la componente organizzativa sia il programma criminoso sono integralmente situate nel cyberspazio. Al contrario, le associazioni parzialmente cibernetiche si caratterizzano per una organizzazione ancora radicata nel mondo fisico, mentre le attività criminali possono estendersi anche nel contesto digitale. È dunque la topologia della struttura organizzativa, più che la natura dell'illecito, a determinare il grado di "ibridismo" di una data associazione[471].

---

[469] Cfr. PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, in *Meridiana*, 106, 2023, p. 164.
[470] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 17; BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 9.
[471] Cfr. PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, cit., p. 164.

Diversa è invece la prospettiva di Broadhurst e di altri autori[472], che hanno sviluppato una classificazione centrata maggiormente sulla natura delle attività criminali piuttosto che sulla loro struttura organizzativa. Nel cosiddetto Cybercrime Digest, viene proposta una distinzione tra gruppi di tipo I e gruppi di tipo II, dove questi ultimi sono definiti come "ibridi" in quanto combinano condotte illecite online e offline[473]. I gruppi di tipo II si suddividono a loro volta in due sottocategorie.

I *clustered hybrids* (ibridi raggruppati) sono formazioni criminali generalmente compatte, composte da un numero ristretto di soggetti, la cui attività si concentra su specifici metodi o tipologie di reato. Tali gruppi presentano una struttura simile agli *hub*, ma con la peculiarità di muoversi agevolmente tra la sfera fisica e quella digitale. Un esempio tipico è rappresentato dalle bande dedite allo *skimming*: i dati delle carte di credito vengono raccolti mediante dispositivi fisici installati su bancomat, e successivamente utilizzati per acquisti online o rivenduti su forum e circuiti di "carding" nel dark web[474].

Gli *extended hybrids* (ibridi estesi), invece, mantengono modalità operative analoghe ai *clustered hybrids*, ma si distinguono per una maggiore dispersione organizzativa. Si tratta di reti più ampie, meno centralizzate, composte da affiliati, sottogruppi e attori diversi che, pur operando in modo semi-autonomo, coordinano le proprie azioni all'interno di ecosistemi criminali condivisi, spesso attivati attraverso piattaforme digitali. Tali reti presentano una notevole eterogeneità funzionale e territoriale, ma conservano un sufficiente livello di coerenza e interconnessione da garantire la realizzazione di obiettivi comuni[475].

Un esempio paradigmatico di ibrido esteso, di cui si dirà a breve nel dettaglio, è costituito dai marketplace del dark web, come Silk Road, AlphaBay e Dream Market, i quali aggregano una molteplicità di soggetti – dagli amministratori centrali ai venditori e clienti finali – collegati da logiche di mercato e anonimato criptografico, piuttosto che da un vincolo associativo formale[476].

---

[472] In particolare, si veda BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 9; MCGUIRE M., *Organized Crime in the Digital Age*, cit..
[473] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 17.
[474] *Ibidem*.
[475] *Ibidem*
[476] *Ibidem*.

6.2. Le associazioni dedite alle truffe online

Tra le associazioni per delinquere cibernetiche ibride rientrano le organizzazioni criminali dedite alle truffe online. Si tratta di sodalizi che operano con modalità particolarmente sofisticate, sfruttando sia il cyberspazio che il mondo fisico, creando un legame tra elementi puramente digitali e strutture organizzative territoriali. Questi gruppi criminali sono capaci di mettere in atto operazioni fraudolente molto complesse, che implicano l'impiego di tecnologie avanzate per ingannare le vittime e ottenere accesso a informazioni sensibili, ma la cui esecuzione richiede anche un coordinamento fisico, con attività logistiche e finanziarie che avvengono al di fuori del cyberspazio[477].

La principale caratteristica di queste organizzazioni è la loro capacità di operare a livello globale, spesso con una suddivisione dei compiti che supera i confini nazionali, facendo sì che le attività criminali si integrino perfettamente in una rete criminale transnazionale[478].

L'attività principale di queste organizzazioni è il *phishing*, una tecnica di *social engineering* che mira ad ingannare le vittime inducendole a rivelare informazioni sensibili, come numeri di carte di credito, credenziali bancarie, o accessi a conti online. I *phisher*, in sostanza, impersonano entità affidabili, come istituti bancari, enti governativi, o altre figure di autorità, al fine di convincere le vittime a fornire i propri dati. Questi messaggi, che spesso si presentano sotto forma di email, SMS o comunicazioni su social network, sono altamente credibili e appositamente progettati per sfruttare la psicologia del destinatario, creando un senso di urgenza o preoccupazione che spinge la vittima a reagire senza pensare. Una volta ottenute le credenziali delle vittime, i truffatori possono accedere ai loro conti bancari o effettuare acquisti online a loro nome, dando così avvio al processo di trasferimento e movimentazione dei fondi[479].

---

[477] Sull'argomento si veda PICARELLA L., *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, cit..

[478] Sul punto cfr. PRUZELIUS G., GYLLNER T., *Phishing in the workplace: organizational practices, culture and phishing vulnerability*, in *Diva Portal*, 2025.

[479] *Ibidem*; sul phishing v. in particolare DI PAOLO E., *Cyber crime. Il Phishing: prospettive di un delitto*, in Arch. pen., 2, 2017, p. 1.

Le organizzazioni dedite al *phishing* si avvalgono di una struttura logistica complessa, che funge da supporto fisico per l'esecuzione dei crimini. Questa struttura è composta da diverse figure chiave, ognuna delle quali svolge compiti specifici[480].

Al vertice ci sono i capi area, che coordinano l'intera operazione in una determinata zona geografica, responsabili del reclutamento e del monitoraggio delle attività. A loro sottostanno i capigruppo, che gestiscono autonomamente i reclutatori, veri e propri intermediari che operano sul territorio per individuare e reclutare i cosiddetti prestaconto. Questi ultimi sono persone che, spesso inconsapevoli della truffa, vengono coinvolte nelle operazioni fraudolente, mettendo a disposizione conti bancari, carte prepagate o altri strumenti finanziari che consentono ai *phisher* di trasferire i soldi rubati[481].

La struttura logistica si occupa anche di supervisionare i prestaconto, per evitare che possano sottrarsi con i fondi che hanno prelevato. Inoltre, all'interno di queste organizzazioni c'è una gerarchia ben definita, che prevede anche la possibilità di avanzamenti, come nel caso di un reclutatore che può essere promosso a capogruppo[482].

La struttura transnazionale delle organizzazioni dedite al *phishing* è caratterizzata da un forte legame tra le operazioni cibernetiche e le attività di persone fisiche. In molti casi, infatti, gli attacchi informatici vengono progettati in un paese, ma l'esecuzione delle operazioni, come il trasferimento dei fondi rubati o il prelievo dai conti bancari, avviene in un altro, tramite una rete di agenti finanziari o muli di denaro, che si occupano di spostare i fondi ottenuti verso conti esteri o altre destinazioni[483].

Il trasferimento dei fondi può avvenire anche tramite servizi di pagamento elettronico, che permettono di spostare denaro in modo rapido e difficile da tracciare.

È in questa fase che la logistica gioca un ruolo fondamentale: i capo area e i capigruppo mantengono stretti contatti con gli agenti di attacco e gli intermediari, per assicurarsi che i trasferimenti di denaro avvengano senza intoppi. Inoltre, è frequente che queste organizzazioni criminali impieghino pratiche di *money laundering*, ovvero di riciclaggio

---

[480] Sempre PRUZELIUS G., GYLLNER T., *Phishing in the workplace: organizational practices, culture and phishing vulnerability*, cit., parla di "*division of labor that promotes role differentiation and specialization*"; sul punto, PICARELLA L., *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, cit.

[481] Sul punto v., BIRK D., GAJEK S., GROBART F., SADEGHI A., *Phishing Phishers: observing and tracing Organized cybercrime*, in Second International Conference on Internet Monitoring and Protection, 2007.

[482] Sempre PRUZELIUS G., GYLLNER T., *Phishing in the workplace: organizational practices, culture and phishing vulnerability*, cit., parla di "*structured network of relationships designed to accomplish tasks"*.

[483] *Ibidem*.

dei fondi ottenuti in modo illecito, che vengono "ripuliti" tramite la stratificazione digitale, rendendo più difficile individuare la provenienza del denaro[484].

Non a caso, le metodologie utilizzate dai *phisher* sono analoghe a quelle tradizionali di riciclaggio di denaro: diverse figure sono coinvolte in ogni fase del processo, dalla raccolta delle credenziali (tipicamente effettuata da agenti di hosting, che creano siti web fraudolenti o compromettono quelli esistenti) al *layering*, in cui i fondi vengono trasferiti su conti bancari esteri o su piattaforme di pagamento online. Il processo di *placement* avviene quando i fondi vengono messi a disposizione degli agenti finanziari, che si occupano di spostarli verso altre destinazioni. Tuttavia, in molte operazioni di *phishing*, non si verifica una divisione fisica dei fondi, come accade nel riciclaggio tradizionale. Questo può essere dovuto al fatto che, a differenza dei metodi tradizionali, i *phisher* non sempre dispongono di una rete di agenti di *layering* sufficientemente estesa per separare ulteriormente i fondi, o che i server compromessi siano già saturi di credenziali da utilizzare[485].

In ogni caso, l'elemento cruciale in queste operazioni è la reclusione dei fondi attraverso l'utilizzo di strumenti finanziari digitali. Questi possono includere denaro elettronico, criptovalute, o beni digitali come oggetti nei videogiochi online, che vengono trasferiti da un conto all'altro senza necessità di un'interazione fisica. L'analogia con il riciclaggio di denaro fisico si estende dunque nel mondo digitale, ma con un grado di sofisticazione tale che rende queste operazioni sempre più difficili da fermare[486].

6.3. Le comunità criminali operanti nei mercati online illegali

Nel contesto della criminalità digitale, una delle forme più complesse e insidiose è rappresentata dalle comunità criminali operanti nei mercati online illegali presenti nel dark web, come *Silk Road*, *Silk Road 2.0*, *Dream Market* e *AlphaBay*.

---

[484] *Ibidem*.
[485] Sul punto v., BIRK D., GAJEK S., GROBART F., SADEGHI A., *Phishing Phishers: observing and tracing Organized cybercrime*, cit.; anche PRUZELIUS G., GYLLNER T., *Phishing in the workplace: organizational practices, culture and phishing vulnerability*, cit., secondo cui "*some security procedures may lack personalization or clarity, leading to risk"*.
[486] *Ibidem*.

Queste piattaforme, accessibili esclusivamente tramite reti di anonimizzazione come Tor, hanno dato vita a vere e proprie associazioni cibernetiche ibride, ossia organizzazioni criminali che operano simultaneamente nel cyberspazio e nel mondo reale[487].

A differenza delle forme più tradizionali di criminalità organizzata, queste comunità non si basano su un'organizzazione verticistica classica, ma si articolano secondo strutture reticolari e decentralizzate, all'interno delle quali agiscono soggetti con ruoli funzionalmente distinti: amministratori, moderatori, venditori, clienti, fornitori e affiliati.

Le attività illecite promosse da tali mercati comprendono la vendita di droghe, armi, dati rubati, malware, documenti falsi e servizi di hacking, con transazioni gestite in criptovaluta per garantire l'anonimato. L'infrastruttura digitale funge da catalizzatore per attività che restano, in larga parte, radicate nel mondo fisico: produzione, distribuzione, logistica, riciclaggio. In tal modo, queste comunità si configurano come ibridi estesi, capaci di muoversi tra il virtuale e il reale, sfruttando le potenzialità della tecnologia per organizzare reati comuni su scala transnazionale[488].

Un caso particolarmente rappresentativo di questo modello è quello di Dream Market, oggetto di indagine nel procedimento penale avviato contro Gal Vallerius negli Stati Uniti.

Dream Market era un marketplace attivo nel dark web che consentiva agli utenti di pubblicare annunci per la vendita di sostanze stupefacenti, ai quali altri membri potevano rispondere per concludere l'acquisto[489]. Le transazioni venivano effettuate in criptovalute, principalmente Bitcoin, per garantire l'anonimato degli utenti[490].

All'interno di Dream Market operava Gal Vallerius con lo pseudonimo di OxyMonster. Egli ricopriva un duplice ruolo: da un lato, amministratore e moderatore del sito, fornendo supporto e consulenza agli altri utenti; dall'altro, venditore diretto di sostanze stupefacenti, che riceveva i pagamenti attraverso un "Bitcoin tip jar", ovvero un deposito elettronico. La struttura del mercato prevedeva, quindi, funzioni gestionali e operative

---

[487] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 17.
[488] *Ibidem*.
[489] United States District Court, *United States of America v. Gal Vallerius* (2018), United States District Court Southern District Of Florida Case n. 17-Cr-20648-Scola/Torres United States Of America, Plaintiff, V. Gal Vallerius, Defendant *Report And Recommendation On Defendant's Motion To Suppress*: *The website allows individuals to create online advertisements offering various narcotics for sale, to which other members can respond and seek to purchase the drugs for a price set by the offering member"*, p. 2.
[490] Ivi: "*Payment for the illicit purchases are made through the use of Bitcoin and other cryptocurrencies, which add an additional layer of anonymity…"*, p. 2.

che contribuivano al mantenimento della piattaforma e allo svolgimento delle attività illecite.

L'anonimato garantito dalla rete Tor e dalle criptovalute era, tuttavia, solo parziale. Gli investigatori statunitensi sono riusciti a collegare l'identità digitale di OxyMonster a quella reale di Vallerius attraverso l'analisi incrociata dei wallet Bitcoin e lo studio comparato dello stile linguistico dei post pubblicati nel forum con i contenuti delle sue attività sui social network[491].

Il caso dimostra chiaramente come il Dream Market operasse secondo una logica di organizzazione criminale ibrida: le operazioni digitali (gestione della piattaforma, transazioni criptate, pubblicazione di annunci, anonimato degli utenti) erano strettamente collegate a condotte materiali (vendita e spedizione fisica delle droghe, gestione dei proventi, identificazione dei soggetti coinvolti), realizzando quella perfetta integrazione tra attività online e offline che caratterizza le associazioni cibernetiche ibride di tipo esteso.

Altro esempio emblematico è Silk Road, attivo tra il 2011 e il 2013, e considerato il primo grande marketplace criminale del dark web. Fondato da Ross Ulbricht**,** alias *Dread Pirate Roberts*, Silk Road operava interamente sulla rete Tor, rendendo estremamente difficile rintracciare gli utenti[492]. Il sito consentiva la compravendita di sostanze stupefacenti, documenti falsi e software per il *cybercrime*[493], con pagamenti effettuati esclusivamente in Bitcoin[494].

La piattaforma offriva poi strumenti di comunicazione interna, come un sistema di messaggistica privata, un forum pubblico e una wiki, utili a facilitare le transazioni e l'assistenza tra utenti e amministratori[495]. Gli acquirenti potevano contattare direttamente

---

[491] *Ivi*, *"Agents tracked… deposits from the tip jar to various 'wallets' controlled by Vallerius… Authorities determined that the writing style and syntax… matched those written by Defendant on his social media accounts"*, p. 3.

[492] Cfr. United States Court Of Appeals For The Second Circuit August Term, 2016 (Argued: October 6, 2016 Decided: May 31, 2017) No. 15-1815 United States Of America, Appellee, — V. — Ross William Ulbricht, A/K/A Dread Pirate Roberts, A/K/A Silk Road, A/K/A Sealed Defendant 1, A/K/A Dpr, Defendant-Appellant, *"Silk Road was a massive, anonymous criminal marketplace that operated using the Tor Network, which renders Internet traffic through the Tor browser extremely difficult to trace"*, p. 3.

[493] *Ivi*, *Silk Road users principally bought and sold drugs, false identification documents, and computer hacking software"*, p. 3.

[494] *Ivi*, *"Transactions on Silk Road exclusively used Bitcoins, an anonymous but traceable digital currency"*, p. 3.

[495] *Ivi*, "*The site also contained a private message system, a public forum... and a 'wiki' which users could access to receive advice"*, p. 3.

i venditori e lasciare recensioni, contribuendo a un sistema di reputazione simile a quello delle piattaforme legittime. D'altro canto, Silk Road fungeva altresì da piattaforma logistica indiretta, in cui i venditori spedivano fisicamente le droghe ai clienti, spesso con packaging anonimo o occultato.

Ross Ulbricht non era solo il fondatore, ma anche l'amministratore tecnico e ideologico del sito. Gestiva l'infrastruttura, interagiva con gli utenti, decideva le regole interne e manteneva un diario delle sue attività criminali[496]. Nel corso dell'indagine, le autorità statunitensi hanno sequestrato il suo laptop e scoperto al suo interno file crittografati, log delle chat con collaboratori, la struttura dei server e transazioni per un valore di circa 18 milioni di dollari in Bitcoin[497].

Ulbricht fu arrestato nel 2013, mentre stava amministrando il sito da un computer portatile in una biblioteca pubblica. In quel momento, era connesso come *Dread Pirate Roberts* alla sezione "staff chat", riservata ai gestori del marketplace[498].

7. Conclusioni

In questo capitolo si è proposta un'analisi descrittiva delle associazioni criminali di tipo cibernetico, con l'obiettivo di ricostruirne le principali caratteristiche strutturali e operative. Si è evidenziato come tali organizzazioni rappresentino una nuova e pervasiva forma di criminalità organizzata, capace di adattarsi alle logiche e agli strumenti del contesto digitale. A differenza delle strutture tradizionali, queste entità operano spesso in modo decentralizzato, sfruttando le tecnologie informatiche per coordinarsi, comunicare e realizzare attività illecite su scala globale. Le attività di riferimento – tra cui il traffico di dati, l'estorsione tramite ransomware, le frodi online, l'intermediazione di servizi criminali nel dark web – mostrano un livello crescente di specializzazione e professionalizzazione, che rende particolarmente difficile la loro individuazione e il loro contrasto attraverso i canali investigativi convenzionali.

---

[496] *Ivi*, "*Ulbricht created Silk Road in 2011 and continued to operate the site... by maintaining its computer infrastructure, interacting with vendors, crafting policies for site users...*", p. 14.
[497] *Ivi*, *"The government seized approximately $18 million worth of Bitcoins from the wallet on Ulbricht's laptop..."*, p. 16.
[498] *Ivi*, *"Ulbricht was arrested… and incident to that arrest agents seized his laptop. The same chat… was open on Ulbricht's screen"*, p. 12.

Oltre alla complessità strutturale e operativa, è fondamentale sottolineare come il dilagare di queste organizzazioni stia generando un crescente allarme sociale.

La percezione di insicurezza legata alla vulnerabilità dei dati personali, delle infrastrutture critiche e dei sistemi economico-finanziari ha portato l'opinione pubblica, i media e le istituzioni a considerare la criminalità cibernetica come una delle principali minacce del nostro tempo. Questo senso diffuso di esposizione al rischio, alimentato anche da episodi sempre più frequenti di attacchi su larga scala, ha prodotto una domanda pressante di risposte efficaci e tempestive da parte dei sistemi giuridici e delle autorità competenti, sia a livello nazionale che internazionale.

Alla luce di quanto emerso, questo capitolo rappresenta un passaggio preliminare e propedeutico per un'analisi giuridica del fenomeno. Si rifletterà, in particolare, sull'adeguatezza dell'attuale impianto normativo nell'inquadrare queste nuove forme associative, sulle problematiche relative alla qualificazione giuridica delle condotte, nonché sulle prospettive di evoluzione del diritto penale e internazionale per fronteggiare con maggiore efficacia una criminalità che opera oltre i confini fisici e giuridici tradizionali. Solo a partire da una chiara comprensione delle dinamiche organizzative e operative del *cyber-organised crime* sarà infatti possibile proporre soluzioni normative coerenti, capaci di rispondere alle esigenze di tutela e di sicurezza della società contemporanea.

CAPITOLO VI

Il *cyber-organised crime* tra inquadramento definitorio e ricostruzione giurisprudenziale

1. Premessa – **2.** Il dibattito dottrinale sull'inquadramento dei gruppi cibernetici nell'alveo dell' "*organised crime*" – **3.** Il reato di associazione per delinquere: gli elementi costitutivi e le questioni interpretative – **3.1.** Struttura organizzativa, vincolo associativo e programma criminoso – **3.2.** L'individuazione dei ruoli nel sodalizio criminoso: profili giurisprudenziali e dottrinali – **3.3.** La condotta di partecipazione all'associazione a delinquere: profili controversi in dottrina e giurisprudenza **– 3.4.** L'elemento soggettivo dell'associazione a delinquere: l'*affectio societatis* – **4.** L'inquadramento giurisprudenziale delle associazioni per delinquere di tipo cibernetico – **4.1.** La dimensione associativa nelle comunità online dedite allo scambio di materiale pedopornografico – **4.2.** Le comunità di hacktivisti operanti nel cyberspace: il caso Anonymous – **4.3.** Un'analisi comparativa delle comunità virtuali alla luce dell'evoluzione giurisprudenziale – **4.4.** La giurisprudenza sulle associazioni cibernetiche ibride dedite alle truffe online – **5.** Conclusioni

1. Premessa

Quanto agli aspetti giuridici relativi al *cyber-organised crime*, diversamente da quanto avvenuto con riferimento alla criminalità organizzata tradizionale, rispetto alla quale la ricerca si è focalizzata sull'analisi delle problematiche giuridiche e degli strumenti di contrasto, la ricerca delle principali questioni giuridiche sul *cyber-organised crime* si muove lungo un piano differente, compiendo un passo indietro per affrontare una questione preliminare di natura concettuale e definitoria, relativa all'inquadramento stesso del fenomeno del *cyber-organised crime*.

Ciò in quanto, a differenza del modello di criminalità precedentemente esaminato, la tecnologia, oltre ad essere strumento per la commissione dei crimini, è altresì parte intrinseca dell'attività del gruppo criminale e ne influenza i connotati teleologici e strutturali.

Come si è anticipato, infatti, gli strumenti digitali vengono impiegati per la prevalente commissione di crimini cibernetici, conseguendone, pertanto, una divergenza nei "reati fine" tipici del tradizionale crimine organizzato. D'altro canto, poi, dalla più alta presenza

della componente tecnologica deriva una notevole semplificazione nell'organizzazione del gruppo criminale, la cui struttura, come si è detto, diviene fluida e flessibile. Diversamente dalle mafie o dalle associazioni a delinquere tradizionali, infatti, queste realtà digitali presentano come visto strutture fluide, decentralizzate, prive di gerarchie stabili e di un'organizzazione durevole, e perseguono finalità legate a reati tipicamente informatici piuttosto che ai delitti tradizionalmente associati alla criminalità organizzata.

Per queste ragioni, da vari studi sulla criminalità organizzata cibernetica emerge la maggioritaria considerazione che l'attribuzione dell'etichetta di "*organised crime*" non sia empiricamente giustificata, ma che sia, piuttosto, conferita al solo fine di creare sensazionalismo o, ancora, allo scopo di perseguire delle politiche securitarie di contrasto alla criminalità organizzata.

Sul punto, la presente analisi non si limiterà a richiamare le principali linee teoriche sviluppate dalla letteratura criminologica, ma prenderà in esame i casi più noti di *cyber-organised crime* per verificare se tali gruppi possano realisticamente ricondursi nell'alveo applicativo dell'art. 416 c.p. o se piuttosto si tratti di un inquadramento forzato, motivato più da esigenze politico-criminali o mediatiche che da una effettiva compatibilità giuridica.

A tal fine, l'indagine si soffermerà sull'esame dei principali casi concreti e della giurisprudenza esistente, al fine di valutare se i requisiti strutturali richiesti dal reato associativo – stabilità del vincolo, programma delittuoso, organizzazione – siano effettivamente riscontrabili in tali formazioni digitali, oppure se si renda necessaria una revisione normativa che dia conto delle peculiarità di una criminalità tecnologicamente sofisticata ma dai tratti atipici.

2. Il dibattito dottrinale sull'inquadramento dei gruppi cibernetici nell'alveo dell' "*organised crime*"

Negli ultimi anni, la letteratura criminologica ha rivolto una crescente attenzione allo studio delle caratteristiche dei gruppi criminali operanti nel cyberspazio, interrogandosi sulla loro possibile riconducibilità all'interno della categoria di criminalità organizzata.

Il tema ha assunto particolare rilievo soprattutto nell'ultimo decennio, parallelamente al progressivo incremento dei reati informatici, alla diffusione di pratiche criminali

altamente sofisticate e alla percezione che la dimensione digitale rappresenta non soltanto un nuovo terreno di azione per la devianza, ma un contesto in grado di trasformare la natura stessa delle organizzazioni criminali.

Il dibattito che ne è derivato si colloca in un alveo prettamente criminologico e si caratterizza per una significativa polarizzazione.

Da una parte, un filone di studi che sostiene la possibilità di leggere le formazioni cybercriminali come nuove espressioni della criminalità organizzata, non solo concentrandosi sull'individuazione di tratti comuni alle associazioni criminali tradizionali, ma anche ipotizzando una progressiva evoluzione o addirittura compenetrazione tra la criminalità organizzata tradizionale e quella cibernetica.

Dall'altra parte, un secondo orientamento dottrinale ha assunto invece un atteggiamento più prudente, se non apertamente critico, rispetto a tale assimilazione, ritenendo che le caratteristiche proprie delle realtà criminali operanti nel cyberspazio impediscano una piena sovrapponibilità con la nozione di criminalità organizzata così come tradizionalmente elaborata ed evidenziando, inoltre, i limiti ed i rischi connessi ad un'estensione troppo ampia di tale etichetta.

In questa cornice, l'analisi dei due filoni dottrinali rappresenta un passaggio necessario per comprendere le implicazioni teoriche e pratiche che derivano dalla qualificazione dei gruppi dediti al *cybercrime*.

In particolare, muovendo in primo luogo dall'esame del filone critico, mancherebbero sufficienti evidenze empiriche per sostenere l'assimilazione tra gruppi criminali dediti al *cybercrime* e criminalità organizzata, non essendo emersi riscontri circa l'adozione di pratiche che caratterizzano storicamente le organizzazioni criminali tradizionali, quali l'esercizio stabile del potere su un determinato contesto socioeconomico, o il ricorso alla violenza come strumento di regolazione e controllo.

Indubbiamente la complessità di rintracciare tra i cybercriminali le caratteristiche tipiche dei gruppi organizzati tradizionali complica la questione. Come già detto, appaiono difficilmente trasferibili nell'ambiente digitale il controllo del territorio o l'uso sistematico della violenza[499].

---

[499] Nell'ambito dell'orientamento critico, si vedano LUSTHAUS J., *How organised is organised cybercrime?*, in *Global Crime Journal*, 14, 1, 2013; WALL D., *Internet mafias? The dis-organisation of crime on the internet*, in S. Canappele – F. Calderoni (a cura di), *Organized crime, Corruption and crime prevention*, Springer, Cham, 2014; LAVORGNA A., SERGI A., *Serious, therefore organised? A critique of*

La violenza fisica costituisce da sempre lo strumento cardine attraverso il quale i gruppi di criminalità organizzata esercitano controllo e regolazione sui mercati illeciti; nel cyberspazio non esiste un'equivalente diretto, poiché pratiche come l'esclusione da comunità online o attacchi DDos possono assumere una funzione coercitiva, ma difficilmente raggiungono il livello di deterrenza e di efficacia che caratterizza le tipiche manifestazioni di violenza fisica delle organizzazioni criminali[500].

Risultano problematiche anche le dinamiche interne al gruppo poiché, al contrario del contesto offline dove le relazioni criminali si fondano su regole interne e strumenti di coercizione, in ambito *cyber* tali strumenti non sono facilmente applicabili, influendo negativamente sulla stabilità dei rapporti e sulla resistenza delle alleanze[501].

In secondo luogo, una delle principali critiche sollevate rispetto alla riconducibilità dei cybercriminali all'interno della categoria dell'"*organised crime*" attiene all'uso dell'etichetta di "*organised crime*" come "*umbrella concept*", che rischia di inglobare indistintamente qualsiasi forma di cooperazione criminale, oscurando la specificità concettuale del fenomeno[502].

L'etichetta di "*organised crime*", infatti, è stata impiegata in maniera estensiva per includere fenomeni criminali molto eterogenei, generando ambiguità definitorie e rischi di *mislabeling*.

Il concetto di "*organised crime*" opera come un contenitore ampio che ingloba condotte e gruppi molto diversi ed assume una funzione più evocativa che descrittiva: sotto la medesima etichetta vengono infatti ricondotti tanto gruppi mafiosi consolidati, quanto aggregazioni frammentarie e temporanee di soggetti operanti nel cyberspazio.

Se è vero che, a livello internazionale, il riferimento rimane la Convenzione ONU del 2000[503] contro la criminalità organizzata transnazionale che, all'interno dell'articolo 2 lett.

---

the emerging "Cyber-organised crime" rhetoric in the United Kingdom, in *International Journal of Cyber criminology*, 10, 2, 2016; LEUKFELDT, E. R., LAVORGNA A., KLEEMANS E. R., *Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit.

[500] Sull'utilizzo della violenza e della corruzione da parte dei gruppi di cybercriminali si veda LEUKFELDT, E. R., LAVORGNA A., KLEEMANS E. R., *Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., p. 294.

[501] *Ibidem*; sul punto cfr. anche. LUSTHAUS J., *How organised is organised cybercrime?*, cit.

[502] Sul concetto di "umbrella concept" cfr. LAVORGNA A., *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?,* cit., p. 193.

[503] Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, dottata dall'Assemblea Generale delle Nazioni Unite con ris. n. 55/25 del 15 novembre 2000, aperta alla firma a

c, chiarisce che per "gruppo strutturato" non è necessario né un'organizzazione formale né la continuità dei membri, è altrettanto vero che questa definizione volutamente ampia, se da un lato consente di adattarsi a diversi contesti giuridici, dall'altro lato abbassa notevolmente la soglia di riconoscibilità e rischia di rendere l'espressione "*organised crime*" un concetto vuoto[504].

Non a caso, l'estensione indiscriminata dell'etichetta diventa particolarmente problematica in ambito *cyber*, venendo applicata a forme criminali debolmente organizzate, spesso caratterizzate da reti piatte e temporanee. Il fatto che finisca per costituire una categoria onnicomprensiva implica la perdita di un'importante distinzione tra gruppi che operano esclusivamente online, e altri che invece sono radicati in mercati offline che utilizzano gli strumenti digitali semplicemente in maniera complementare al proprio *core business*[505].

Infine, a rafforzare questa deriva contribuisce il fatto che il dibattito intorno all'ampiezza dell'etichetta di *organised crime* non rimane confinato al piano puramente teorico e speculativo, ma assume una rilevanza pratica di primaria importanza, trovando crescente applicazione anche nelle politiche securitarie e nel linguaggio politico istituzionale. Parrebbe infatti, nel parere di questa dottrina, che se da un lato, in ambito accademico, si fatica ancora a definire con precisione la natura delle organizzazioni criminali nel cyberspazio, dall'altro lato invece le agenzie di sicurezza e le istituzioni adottano la retorica dell'"OC" per attuare politiche securitarie, con conseguenze significative in termini di allocazione di risorse e definizione delle strategie operative. Sovrastimare il coinvolgimento della criminalità organizzata in un determinato reato può tradursi nell'ottenimento di risorse supplementari, nell'attribuzione di poteri legali ulteriori e, al contempo, nel consolidamento del sostegno da parte della classe politica, dell'opinione pubblica e dei mezzi di comunicazione[506].

Inoltre, l'invocazione di tale etichetta come spiegazione di reati complessi costituisce una chiave di lettura più immediata e rassicurante.

Palermo il 12-15 dicembre 2000, entrata in vigore il 29 settembre 2003, in G.U. n. 85 dell'11 aprile 2006 (legge di ratifica 16 marzo 2006, n. 146).

[504] *Ibidem*.

[505] *Ibidem*.

[506] Circa le conseguenze, in termini pratici, derivanti dall'applicazione dell'etichetta di "organised crime" si veda LAVORGNA A., *Cyber-organised crime. A case of moral panic?,* in *Trends in Organized Crime*, 4, 2019, p. 358.

Tuttavia, tale approccio non è esente da criticità, in quanto rischia di produrre una distribuzione inefficiente delle risorse, un'interferenza sproporzionata nei confronti dei diritti degli indagati e un'attenzione erroneamente concentrata sulla criminalità organizzata a discapito di strategie preventive e investigative potenzialmente più efficaci[507].

La narrazione spesso impiegata dalle politiche pubbliche tende, secondo parte della dottrina, a postulare una convergenza tra criminalità organizzata e *cybercrime* nonostante la scarsità di evidenze empiriche solide, basandosi piuttosto sul cosiddetto "paradigma della gravità" che accosta in modo talvolta ingiustificato la serietà delle attività criminali alla natura organizzata dai criminali stessi[508]. Il "paradigma della serietà", infatti, implica l'assunzione implicita che vi sia sempre una corrispondenza diretta tra gravità del crimine e livello di organizzazione. In altre parole, nelle politiche pubbliche spesso si tende a considerare i crimini gravi come intrinsecamente organizzati e, viceversa, a etichettare come gravi solo le attività chiaramente organizzate. Tuttavia, parte della dottrina insiste nel criticare tale paradigma, ritenendo che tale connessione non trovi sempre riscontro nella realtà empirica: esistono infatti crimini gravi compiuti da individui isolati o da gruppi poco strutturati, così come attività criminali organizzate che non comportano danni sociali significativi. L'applicazione, dunque, di tale paradigma produrrebbe una distorsione analitica, enfatizzando la pericolosità di certi gruppi sulla base di un presupposto teorico, piuttosto che su evidenze concrete[509].

Si suggerisce, in questo senso, di ripensare alle modalità con cui si concettualizza e si misura la criminalità organizzata, specialmente nel contesto del cyberspazio: in particolare, sarebbe opportuno operare una separazione critica tra gravità e organizzazione, in base al caso concreto e, al posto di usare l'elemento organizzativo

---

[507] *Ibidem;* sempre LAVORGNA, A. *Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology.* in *Trends in Organised Crime,* 2023.

[508] Cfr. LEUKFELDT, E. R., LAVORGNA A., KLEEMANS E. R., *Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., pp. 287-300

[509] Sul paradigma della "seriousness" vedi: SERGI A., *Divergent mind-sets, convergent policies. Policing models against organised crime in Italy and in England within international frameworks*, in *European Journal of Criminology*, 12, 6, 2015, pp. 658– 680; LAVORGNA A., SERGI A., *Serious, therefore Organised? A Critique of the Emerging "Cyber-Organised Crime" Rhetoric in the United Kingdom,* cit., p. 171.

come “proxy” di pericolosità, occorrerebbe analizzare caso per caso il danno concreto, gli effetti sistemici e le minacce reali per la società[510].

Ciò non equivale a negare la dimensione collettiva e, in taluni casi, organizzata del *cybercrime*, bensì induce ad un approccio improntato ad una maggiore cautela, che privilegia l'analisi critica e la produzione di nuove ricerche empiriche prima di giungere a conclusioni definitive sull’opportunità di collocare tali gruppi entro la cornice della criminalità organizzata[511].

Muovendo adesso ad analizzare il secondo filone dottrinale a favore dell’inquadramento dei gruppi dediti al *cybercrime* nell’alveo della criminalità organizzata, è opportuno precisare come alcuni contributi appartenenti a questa corrente abbiano carattere eminentemente speculativo, anche in ragione del fatto che risalgono a un periodo relativamente remoto rispetto alla rapida evoluzione tecnologica degli ultimi anni.

In quest’ottica, si colloca il contributo di Brenner il quale, con una riflessione di carattere puramente speculativo, ipotizza una possibile compenetrazione tra criminalità organizzata e fenomeni di *cybercrime*[512].

L'autore propone un'analisi teorica dell'evoluzione della criminalità organizzata nel mondo reale, dalla comparsa delle prime gang fino alle strutture gerarchiche complesse del ventesimo secolo, e riflette su come l'integrazione del cyberspazio nelle attività illecite possa generare nuove forme organizzative, radicalmente differenti da quelle tradizionali.

Secondo la sua visione, le gang e le strutture gerarchiche complesse, nate e consolidate in un contesto fisico e territoriale, risultano ormai inadatte a essere trasposte nel contesto digitale senza che vi siano delle profonde trasformazioni: entrambe le strutture, infatti, perdono gran parte della loro funzionalità in un ambiente in cui i processi possono essere automatizzati e la cooperazione temporanea tra individui può sostituire la concentrazione stabile di sforzi fisici. Si ipotizza, pertanto, una criminalità online dalle forme fluide,

---

[510] Cfr. LEUKFELDT, E. R., LAVORGNA A., KLEEMANS E. R., *Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, cit., p. 297, dove gli Autori, in sede di conclusioni, sottolineano la necessità di analisi più precise di danno, rischio e minaccia per i singoli cybercrimini e mettono in guardia contro la narrativa della “cyber-OC”, che rischia di distogliere attenzione e risorse dalle misure di sicurezza.

[511] Sul punto, v. anche PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, cit., p. 159.

[512] Cfr. Brenner S.W., *Organized cybercrime? How cyberspace may affect the structure of criminal relationships*, cit., pp. 1-50.

reticolari e temporanee, un modello definito evocativamente come "Mafia del momento" o "*cartel of the day*", che seppur radicalmente diverso dai modelli tradizionali permette comunque di perseguire finalità tipiche della criminalità organizzata. Si tratta, dunque, di un contributo innovativo che non concepisce la compenetrazione tra criminalità organizzata e *cybercrime* come un semplice trasferimento dei modelli tradizionali nell'ambiente digitale, ma ipotizza la nascita di nuove modalità di organizzazione criminale, in cui la flessibilità e l'adattabilità sostituiscono progressivamente gli elementi di stabilità, gerarchia e presenza fisica propri delle organizzazioni consolidate[513].

All'interno dello stesso filone dottrinale si collocano contributi che sostengono la potenziale riconoscibilità dei gruppi dediti al *cybercrime* nell'alveo della criminalità organizzata considerando l'assenza di una definizione circoscritta e universalmente accettata di quest'ultima.

Si evidenzia come il concetto di "criminalità organizzata" non sia specificamente definito: come osserva Klaus von Lampe[514], già in precedenza menzionato, esistono svariate definizioni di criminalità organizzata, ciascuna con sfumature e criteri differenti.

Le concezioni classiche, ispirate al cosiddetto "modello mafioso", descrivevano organizzazioni monolitiche, gerarchicamente strutturate e basate su legami stabili. Tuttavia, già dagli anni '90, studi empirici hanno evidenziato che gran parte dell'attività criminale non è il frutto di strutture durevoli, ma di coalizioni temporanee flessibili, di reti di piccoli gruppi che si aggregano per realizzare specifiche operazioni. Proprio questo mutamento di prospettiva ha fatto sì che l'idea di imprese verticalmente integrate cedesse il passo alla metafora delle reti, oggi a fondamento del pensiero contemporaneo sulle interrelazioni all'interno dei gruppi criminali organizzati e tra singoli gruppi. Pertanto, secondo questa linea di pensiero, gli sviluppi nelle organizzazioni criminali sono progrediti rapidamente negli ultimi anni, rendendo alcune definizioni di criminalità organizzata troppo ristrette e vincolate dall'ideologia[515].

---

[513] *Ibidem*.

[514] Cfr. VON LAMPE K., *A Systematic Overview of Definitions of Organized Crime*, in *Organized Crime: Analyzing illegal activities, criminal structures, and extra-legal governance*, cit., pp. 27-30, secondo il quale la nozione di criminalità organizzata risulta priva di una definizione univoca, riflettendo non solo la complessità del fenomeno ma anche la sua costruzione sociale e politica. Le definizioni disponibili, infatti, variano in base a interessi pratici o scelte ideologiche.

[515] *Ibidem*.

Non è detto infatti che l'inquadramento di criminalità organizzata debba basarsi esclusivamente su un movente economico, individuandosi comunque delle organizzazioni criminali che aspirano al raggiungimento di valori non monetari; così come non è necessariamente vero che le attività organizzate debbano necessariamente fondarsi su gerarchie rigide o su affiliazioni permanenti[516].

Sulla stessa scia, altra dottrina[517], pur ammettendo l'esistenza di differenze evidenti tra i gruppi di cybercriminali e la criminalità organizzata tradizionale, suggerisce di concepire la criminalità organizzata non più come un concetto rigido e statico, ma come una categoria elastica, capace di includere anche le formazioni criminali digitali che replicano, in chiave tecnologica, molte delle dinamiche già osservabili nelle associazioni a delinquere tradizionali. In particolare, tra i vari elementi di contaminazione tra vecchi e nuovi modelli organizzativi, si osserva talvolta la presenza in taluni gruppi criminali di nuclei stabili di membri, che collaborano in maniera duratura e non episodica, in modo da assicurare la continuità del vincolo associativo, anche se non sorretta da forme di affiliazione esplicita o da rituali di ingresso tipici delle mafie[518].

Un secondo punto di contatto riguarda la divisione funzionale delle competenze: così come nelle organizzazioni criminali tradizionali vi è una ripartizione di ruoli, anche nelle formazioni *cyber* è possibile individuare ruoli distinti (sviluppatori di malware, fornitori di infrastrutture, operatori di mercati neri digitali, riciclatori di denaro, figure con capacità di intermediazione); questa specializzazione interna è funzionale all'aumento di efficienza e riproduce, seppur con strumenti tecnologici diversi, la logica imprenditoriale propria delle grandi organizzazioni criminali[519].

Ancora, ulteriore elemento di comunanza viene rintracciato nella propensione transnazionale[520]: se le mafie e i cartelli hanno da tempo assunto dimensioni globali, sfruttando canali finanziari e logistici per superare i confini nazionali, le reti dei

---

[516] Cfr. BROADHURST R., GRABOSKY P., ALAZAB M., CHON S., *Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime*, cit., pp. 2-3.
[517] cfr. NURSE J., BADA M., *The Group element of cybercrime: types, dynamics and criminal operations*, cit., p. 14.
[518] *Ibidem*.
[519] *Ivi*, p. 14: sulla specializzazione e sulla divisione dei ruoli vedi anche BROADHURST R., GRABOSKY P., ALAZAB M., CHON S., *Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime*, cit.
[520] *Ivi*, pp. 5-6.

cybercriminali beneficiano, sin dalla loro origine, della natura intrinsecamente senza frontiere del cyberspazio.

Infine, analogamente alla criminalità organizzata tradizionale, storicamente caratterizzato da processi di professionalizzazione e da una crescente capacità di adattarsi ai cambiamenti tecnologici e sociali, anche nel *cybercrime* si assiste alla "*professionalization of computer crimes*" da parte dei gruppi di cybercriminali, che tendono a strutturarsi secondo le logiche di mercato[521].

D'altro canto, evidenzia altra dottrina, altro elemento che rafforza l'ipotesi di una crescente compenetrazione tra criminalità organizzata e *cybercrime* è rappresentato dalle motivazioni economiche che muovono entrambi i fenomeni[522]. Così come le mafie e i cartelli hanno storicamente basato la propria sopravvivenza sulla capacità di infiltrarsi nei circuiti economici legali e di sfruttare i canali finanziari transnazionali, allo stesso modo, i gruppi cybercriminali orientano la propria attività anche verso reati a scopo di lucro come frodi informatiche, estorsioni digitali, *phishing*[523].

Accanto a chi sostiene che la definizione di criminalità organizzata sia talmente estesa da poter ricomprendere anche i gruppi dediti al *cybercrime*, c'è dottrina che invece ritiene più opportuno che venga aggiornata l'attuale definizione di crimine organizzato, affinché essa rifletta le profonde trasformazioni indotte dalla rivoluzione digitale.

In tale prospettiva, si colloca il pensiero di Di Nicola, il quale sottolinea come le definizioni criminologiche tradizionali si rivelino oggi incapaci di inglobare le nuove configurazioni criminali operanti nella società digitale. Secondo l'autore, i paradigmi del passato appaiono parzialmente obsoleti perché, come più volte illustrato, presuppongono un'organizzazione criminale stabile, territoriale e rigidamente strutturata[524].

---

[521] *Ivi*, p. 11.

[522] Sui gruppi criminali mossi invece da interessi economici, una delle componenti più rilevanti nel panorama del *cybercrime* contemporaneo, si consulti Cfr. BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 13; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16.

[523] Cfr. CHOO K.R., SMITH R.G., *Criminal exploitation of online systems by organised crime groups*, cit., pp. 37-59.

[524] Cfr. DI NICOLA A., *Towards digital organized crime and digital sociology of organized crime*, cit., 2022, in cui l'Autore evidenzia come attori umani e non umani (dispositivi, software, dati, oggetti digitali) siano sempre più interconnessi e interdipendenti, fino a costituire ciò che la teoria dell'Actor-Network definisce "assemblaggi sociotecnici". Tali assemblaggi non rappresentano semplici strumenti di supporto, ma diventano elementi fondamentali che plasmano attività sociali, pratiche quotidiane e persino identità individuali e collettive.

Per tale ragione, la criminalità organizzata non può essere considerata unicamente un fenomeno confinato entro le categorie del "modello tradizionale", ma dovrebbe rappresentare un *continuum* che abbraccia un'ampia gamma di comportamenti e di assetti organizzativi. Le attività criminali, infatti, sono sempre più caratterizzate da un passaggio bidirezionale tra l'online e l'offline: il cyberspazio non rappresenta più un'alternativa al mondo reale, bensì un'estensione dello stesso, con l'effetto che la distinzione tra reale e virtuale, così come tra *cybercrime* e criminalità organizzata tradizionale, tende a sfumare, generando forme ibride di interazione tra attori umani e non umani, secondo logiche descritte dall'autore come "assemblaggi socio-tecnici"[525].

Pertanto, di fronte a questa complessità egli ritiene non più sostenibile mantenere una concezione rigida del fenomeno, che rischierebbe di escludere dal campo definitorio una parte significativa e crescente delle manifestazioni criminali contemporanee.

Occorre, dunque, una ridefinizione criminologica di criminalità organizzata, capace di abbracciare anche le innovazioni introdotte dalla digitalizzazione, includendo tanto i gruppi che operano esclusivamente online quanto quelle organizzazioni tradizionali che si avvalgono della rete per espandere, diversificare e rafforzare le proprie attività illecite. Questa nuova definizione dovrà comunque mantenere come denominatore comune l'elemento dell'organizzazione della professionalità criminale, ma dovrà declinare tali elementi alla luce di strutture più elastiche, dinamiche tecnologicamente integrate[526].

3. Il reato di associazione per delinquere: gli elementi costitutivi e le questioni interpretative

A fronte del vivace dibattito dottrinale intorno alla riconducibilità dei gruppi dediti al cybercrime nell'alveo della criminalità organizzata, il presente lavoro si propone ora di affiancare all'analisi teorica una ricognizione del materiale giudiziario disponibile, al fine di verificare come e in che misura taluni sodalizi criminali operanti nel contesto digitale siano stati in concreto sussunti entro la fattispecie incriminatrice dell'associazione delinquere prevista dall'articolo 416 c.p.

[525] *Ibidem*.
[526] *Ibidem*.

Per perseguire tale obiettivo, appare necessario procedere preliminarmente a un inquadramento della figura dell'associazione per delinquere, con particolare attenzione ai suoi elementi costitutivi e alle modalità con cui la dottrina e la giurisprudenza ne hanno delineato i contorni applicativi. Solo attraverso questo quadro sarà possibile comprendere in che modo la giurisprudenza si sia concretamente confrontata con i principali gruppi di cybercriminali, valutando le soluzioni interpretative adottate e le eventuali criticità emerse nel ricondurli entro la fattispecie di associazione per delinquere.

3.1. Struttura organizzativa, vincolo associativo e programma criminoso

Il primo profilo che occorre considerare è quello del bene giuridico tutelato, giacché dalla sua individuazione discende la funzione preventiva della norma e si comprende la ragione per cui il legislatore abbia deciso di anticipare la soglia di punibilità alla mera esistenza di un'associazione a prescindere dalla realizzazione dei reati fine.

L'esistenza di un'associazione a delinquere costituisce, di per sé sola e a prescindere dalla commissione dei singoli reati fine, un fattore idoneo a suscitare allarme nella collettività e a determinare un perturbamento dell'ordine pubblico. Quest'ultimo non va inteso - secondo l'ormai superata concezione di ordine "ideale" - come mera osservanza dell'ordinamento giuridico, bensì in senso materiale, ossia come regolare assetto e buon andamento del vivere civile, come percezione sociale di tranquillità e di sicurezza[527].

È in questa chiave che la giurisprudenza di legittimità ha costantemente ribadito la centralità del pericolo insito nel vincolo associativo: il delitto di cui all'articolo 416 c.p. non richiede per la sua configurazione la consumazione effettiva dei delitti fine, in quanto

[527] Data la genericità del concetto di ordine pubblico e il fatto che la legislazione d'emergenza ha indistintamente raggruppato varie tipologie di reati per motivi simbolici ed ideologici sotto l'etichetta di "reati contro l'ordine pubblico", l'individuazione esatta del concetto di "ordine pubblico" ha da sempre suscitato ampio dibattito nel pensiero giuridico italiano. Da un lato, l'accezione di ordine pubblico in senso materiale, inteso come situazione di pacifica convivenza e di sicurezza collettiva, risultava la tesi accolta dalla dottrina prevalente poiché più aderente ad una visione costituzionalmente orientata di bene giuridico, trattandosi di un'entità empiricamente più afferrabile (FIANDACA G., *Il «bene giuridico» come problema teorico e come criterio di politica criminale, in Riv. it. dir. proc. e pen.*, 1, 1982, pp. 42 ss.). Dall'altro lato, la concezione di ordine pubblico ideale o normativo, inteso come insieme di principi e istituzioni fondamentali alla base di un ordinamento giuridico, si esponeva a rilevi ai critici a causa dell'astrattezza del concetto e del rischio di manipolazioni interpretative (FIORE C., voce *Ordine Pubblico (penale*), in Enc. Dir., Vol. XXX, 1980, (online.leggiditalia.it), p. 3.). Occorre infine menzionare la posizione della Corte costituzionale che ha definito l'ordine pubblico costituzionale come l'"insieme di principi fondamentali, che riassumono l'ordine legale di una convivenza sociale ispirata ai valori costituzionali" (Corte cost., 8 luglio 1971, n. 168).

ciò che rileva è la potenzialità destabilizzante dell'accordo criminoso che lega più individui in modo stabile ed organizzato[528]. Da ciò emerge, dunque, la funzione tipicamente preventiva della fattispecie, che si colloca in quella linea politica criminale volta ad anticipare la soglia di tutela, colpendo non solo le condotte che già hanno prodotto l'offesa, ma anche quelle che, per loro natura, moltiplicano esponenzialmente il rischio della commissione futura di reati.

Quanto agli elementi costitutivi di natura oggettiva del reato, la giurisprudenza di legittimità richiede l'esistenza di un vincolo associativo stabile, di un programma indeterminato di delitti e di una struttura organizzativa, la quale, seppur minima, deve risultare idonea e adeguata a realizzare gli obiettivi criminosi perseguiti[529].

La formulazione della fattispecie incriminatrice è stata a lungo oggetto di scrutinio critico da parte della dottrina, poiché caratterizzata da una latitudine di applicazione che, se non opportunamente interpretata, rischia di determinare un significativo deficit di tipicità[530].

Tale criticità è accentuata dalla vaghezza dei termini mediante i quali vengono individuate le condotte e il bene giuridico tutelato determinando una congeniale indeterminatezza della fattispecie associativa.

Primo elemento costitutivo dell'associazione per delinquere è il programma indeterminato di delitti, che segna la distanza ontologica e funzionale tra la fattispecie associativa e il concorso di persone nel reato. Secondo l'orientamento maggioritario giurisprudenziale, infatti, nell'associazione per delinquere l'accordo è permanentemente diretto alla realizzazione di una serie indeterminata di delitti, mentre nel concorso di persone è contingente e mirato alla commissione di uno o più reati determinati[531].

---

[528] Si vedano, sul punto, Cass. pen., sez. I, n. 1440 del 1986; Cass. pen., sez. III, 7 luglio 1992, n. 8539; *a fortiori*, si aggiunga che l'esistenza del reato associativo permane sia in caso di *abolitio criminis* di taluno die reati-fine (Cass. pen, sez. IV, 27 novembre 2003, n. 7187), sia a seguito dell'intervenuta estinzione degli stessi (*Cass., I, n. 9307/1985*), nonché per effetto dell'assoluzione del partecipe dall'accusa relativa a taluni reati-fine (Cass. pen.,, sez. IV, 28 gennaio 2014, n. 8092).

[529] Cfr. sul punto Cass. pen., sez VI, 14 giugno 1995, n. 11413, Montani; in senso conforme anche Cass. pen., sez. II, 17 gennaio 2013, n. 16339, Burgio.

[530] Cfr. FIANDACA G., MUSCO E., *Diritto penale, Parte Speciale*, vol. I, IV ed., Bologna, 2012, p. 486.

[531] Sul *discrimen* tra reato associativo e concorso di persone nel reato si vedano Cass. pen., sez. I, 24 marzo 1992, n. 3402; Cass. pen., sez. I, 14 luglio 1998, n. 10107; Cass. pen., sez. VI, 13 maggio 2014, n. 36131.

Non a caso, secondo la giurisprudenza, l'accordo non riguarda la commissione di reati specificamente individuati, ma si connota per l'indeterminatezza numerica, cronologica e modale dei delitti programmati[532].

In tale prospettiva, si è osservato efficacemente che l'associazione non produce reati bensì opportunità criminose, essendo il reato associativo caratterizzato da un potenziale criminale che trascende i singoli episodi delittuosi; questi ultimi costituiscono soltanto un epifenomeno del sodalizio, non ne esauriscono la pericolosità, che permane anche oltre e dopo la loro consumazione, a giustificazione del maggior disvalore attribuito alla fattispecie dall'ordinamento[533].

L'elemento dell'indeterminatezza si coglie appieno se posto in raffronto con la disciplina del vincolo della continuazione di cui all'articolo 81 co. 2 c.p., che richiede l'unicità del disegno criminoso e, quindi, la concezione e la volontà originaria delle azioni delittuose nei loro tratti essenziali. Al contrario, nell'associazione per delinquere, i singoli reati scaturiscono da determinazioni autonome e successive, essendo accomunati soltanto dall'esistenza di un progetto generico e indefinito di attività criminale[534]. Ciò implica che il programma criminoso dell'associazione rimane indeterminato in relazione al numero e alla qualità dei reati da commettere, ma non per questo appare privo di contenuto, potendo infatti circoscriversi ad un determinato arco temporale o ad uno specifico settore di attività[535].

La Suprema Corte ha altresì chiarito che l'indeterminatezza del programma criminoso non viene meno nel caso in cui l'attività del sodalizio sia rivolta esclusivamente alla commissione di reati della medesima natura; come si è detto, infatti, l'indeterminatezza non riguarda la qualificazione giuridica dei delitti, bensì il loro numero, le modalità, i tempi e gli obiettivi concreti delle condotte delittuose. In questo senso, l'individuazione di un preciso ambito di attività, nel quale il gruppo si propone di commettere una pluralità

---

[532] Cfr. Cass. pen., sez. I, 13 marzo 1968, n. 434.

[533] Cfr. IACOVIELLO F.M., *Ordine pubblico e associazione per delinquere*, in *Giustizia Penale*, 1990, II, p. 51 ss.; IDEM, *L'organizzazione criminogena prevista dall'art. 416 c.p.*, in *Cass. pen.*, 1994, p. 577, in cui l'autore propone una lettura innovativa dell'ordine pubblico materiale in chiave empirico-criminologica, inteso come equilibrio dinamico del sistema sociale in rapporto inverso con il disordine criminale, misurabile attraverso i tassi di criminalità e le opportunità delittuose. Ne consegue che la tutela penale di tale bene giuridico viene giustificata con la riduzione, rilevabile in termini statistici, delle occasioni criminali connesse ai reati-fine delle associazioni per delinquere.

[534] Cfr. Cass. pen., sez. III, 25 giugno 2024, n. 39478; Cass. pen, sez. 1, 8 gennaio 2016, n. 15955; Cass. pen., sez. I, 26 febbraio 2014, n. 39222, Rv. 260896; Cass. pen., sez. I, 13 dicembre 1995, n. 6553.

[535] Sul programma criminoso dell'associazione si veda Cass. pen., sez. VI, 11 luglio 2018, n. 38524.

indeterminata di reati, costituisce un indizio significativo dell'esistenza del vincolo associativo[536].

Per la configurazione dell'associazione, la giurisprudenza è costante nel sottolineare l'esigenza di un minimo di organizzazione stabile e adeguata, anche se rudimentale e mancante di una precisa distribuzione gerarchica di funzioni e purché idonea al perseguimento del programma criminoso[537].

È altresì ammesso l'impiego di una struttura preesistente, originariamente destinata a scopi leciti, purché effettivamente piegata al perseguimento di finalità criminose. Non è dunque necessario creare *ex novo* un'organizzazione, ma è sufficiente l'utilizzo di un apparato già operativo, a condizione che vi sia un collegamento funzionale tra la struttura e il programma criminoso[538].

Si rende dunque necessaria una puntuale indagine sulla struttura organizzativa del sodalizio criminoso. In particolare, si richiede un grado di adeguatezza tale da consentire il perseguimento effettivo degli obiettivi delittuosi programmati: la verifica dell'idoneità dell'apparato organizzativo è indispensabile ai fini del rispetto del principio di offensività, in quanto in mancanza di tale accertamento la pericolosità dell'associazione finirebbe per essere desunta dalla mera esistenza di un accordo criminoso[539].

Pertanto, l'adeguatezza della struttura viene valutata in relazione alla capacità di realizzare i reati scopo e di mantenere l'efficienza operativa dell'associazione, articolandosi in ruoli esecutivi e strumentali, quali l'approvvigionamento di mezzi, il coordinamento e il controllo delle attività[540].

Nella medesima prospettiva, deve essere altresì valorizzato il requisito della stabilità, che si concretizza nell'attitudine dell'organizzazione a perdurare nel tempo e ad essere

---

[536] Cfr. Cass. pen., sez. II, 17 gennaio 2013, n. 16339: "proprio l'individuazione di un settore di attività verso il quale gli indagati rivolgono le loro attenzioni criminali per commettere, in quell'ambito delimitato, una serie indeterminata di delitti fine, rappresenta un sintomo significativo idoneo a rivelare, in presenza degli altri elementi di seguito elencati, l'esistenza di un sodalizio criminoso finalizzato appunto alla realizzazione di più delitti delle specie indicate".

[537] Cfr, ANTOLISEI F., *Manuale di diritto penale*, *Parte Speciale*, vol. II, XVI ed, 2016, p. 248; MANZINI V., *Trattato di diritto penale italiano,* V ed., vol. VI, 1987, pp. 196-197; in giurisprudenza Cass. pen., sez. VI, 7 novembre 2011, n. 3886; Cass. pen., sez. VI, 28 febbraio 2017, n. 15573.

[538] Cfr. Cass. pen., sez. I, 28 settembre 2005, n. 39757; Cass. pen., sez. VI, 30 gennaio 2013, n. 34489.

[539] In proposito si veda DE FRANCESCO G., *Associazione per delinquere e associazione di tipo mafioso*, in *Digesto penale*, I, Torino, 1987, p. 289.

[540] Cfr. Cass. pen., sez. II, 3 aprile 2013, n. 20451; Cass. pen., sez. VI, 7 novembre 2011, n. 3886; Cass. pen., sez. V, 5 maggio 2009, n. 31149.

riutilizzata anche dopo la commissione dei singoli reati, configurandosi come entità autonoma rispetto agli episodi delittuosi[541].

Il connotato di stabilità è accostato altresì al vincolo associativo e postula l'esistenza di un'unione permanente, la cui durata, indeterminata o meno, deve risultare sufficiente allo svolgimento di un programma delinquenziale, restando irrilevante, a tal fine, sia la sua precoce interruzione per effetto della scoperta da parte dell'autorità, sia la realizzazione o meno del programma criminoso stesso. Infatti, secondo la giurisprudenza di legittimità, ai fini della configurabilità del reato di associazione per delinquere, non è necessario che il vincolo assuma carattere di assoluta stabilità, essendo sufficiente che esso non sia *ab origine* circoscritto alla commissione di uno o più delitti predeterminati, dal momento che l'elemento temporale che connota la nozione stessa di "stabilità" non implica il necessario protrarsi del legame criminale, potendo ritenersi sufficienti anche forme di partecipazione di brevi periodi[542].

Possono dunque rilevare forme di partecipazione concepite *ab origine* come temporalmente circoscritte e dirette al perseguimento di vantaggi personali ulteriori rispetto a quelli dell'organizzazione, trattandosi comunque di modalità partecipative che non vanno a scalfire il contributo causale fornito dal soggetto all'efficienza e alla persistenza dell'associazione[543].

Quanto alla prova dell'accordo associativo, la giurisprudenza di legittimità ha chiarito che essa non richiede necessariamente la dimostrazione di un patto espresso o formalizzato tra i sodali, potente emergere anche da una serie di *facta concludentia*. Tra questi assumono rilievo la continuità, la frequenza e l'intensità dei rapporti tra i soggetti, l'interdipendenza delle loro condotte, la predisposizione di mezzi finanziari e l'efficienza dell'organizzazione criminale[544].

Segnatamente, la Corte ha sottolineato come i delitti programmati ed effettivamente realizzati possano costituire un significativo indice probatorio quando il contesto in cui maturano e le modalità esecutive ne rivelino la riconducibilità ad un vincolo associativo: sebbene sia pacifico che la sola commissione di uno o più reati non basti di per sé a

---

[541] *Ibidem*.
[542] Cfr. Cass. pen., sez. II, 15 gennaio 2013, n. 19917; per precedenti pronunce giurisprudenziali in senso conforme cfr. Cass. pen., sez. I, 18 marzo 2011, n. 31845; Cass. pen., sez. V, 28 giugno 2000, n. 12525.
[543] Sulle forme di partecipazione all'associazione temporalmente circoscritte cfr. Cass. pen., sez. II, 24 marzo 2011, n. 16606.
[544] Cass. pen., sez. VI, 10 aprile 1987, n. 7789.

dimostrare l'adesione all'associazione[545], è tuttavia ammesso che da tali condotte il giudice possa inferire elementi quali la stabilità del vincolo e l'indeterminatezza del programma criminoso, laddove le condotte si susseguano in modo "ininterrotto e frenetico, per un ampio lasso temporale" e siano poste in essere da soggetti stabilmente collegati nel perseguimento delle finalità del sodalizio[546].

Tale orientamento trova una conferma paradigmatica in materia di traffico di stupefacenti, ambito in cui la Corte ha ribadito che non è necessaria la prova di un patto espresso, ma è sufficiente desumere l'esistenza del vincolo associativo dalle modalità esecutive dei reati fine, dalla loro ripetitività, dalla natura dei rapporti intercorrenti tra gli autori, nonché dalla divisione di compiti e ruoli funzionali al perseguimento dell'obiettivo comune[547]. In questa prospettiva, sono stati considerati indici rivelatori i contatti frequenti fra gli spacciatori, i ripetuti viaggi per il fornimento della droga, l'esistenza di basi logistiche, e le modalità organizzative adottate, anche sotto forma di una divisione parcellizzata dei compiti[548].

Un chiarimento di particolare rilievo, offerto dalla giurisprudenza di legittimità in tema di associazione per delinquere, riguarda l'illecita degli scopi perseguiti dal sodalizio.

Tale precisazione, oltre a consentire di definire i contorni dogmatici della fattispecie, si rivelerà altresì funzionale alla comprensione delle più recenti elaborazioni giurisprudenziali in materia di criminalità organizzata cibernetica. In questo senso, infatti, la libertà di forme che caratterizza l'associazione per delinquere consente di cogliere l'essenza del fenomeno associativo anche al di là di schemi formali. La centralità del consenso criminoso, quale fondamento della tipicità, si presta ad illuminare con chiarezza il modo in cui la giurisprudenza affronterà in seguito la configurabilità delle associazioni criminali operanti nel cyberspazio, giacché la mancanza di forme tradizionali di organizzazione, l'assenza di un radicamento territoriale, tipici di tali associazioni, rendono ancor più evidente la necessità di riconoscere l'associazione, non sulla base di elementi

---

[545] Cass. pen, sez. III, 6 novembre 2015, n. 9459, *Venere.*
[546] Cass. pen., sez. II, 4 ottobre 2016, n. 53000.
[547] Cass. pen., sez. VI, 24 settembre 2012, n. 9061, *Cecconi,* la cui massima recita come segue: "Ai fini della configurabilità dell'associazione finalizzata al traffico illecito di sostanze stupefacenti, non è richiesto un patto espresso fra gli associati, potendo desumersi la prova del vincolo dalle modalità esecutive dei reati-fine e dalla loro ripetitività, dalla natura dei rapporti tra i loro autori, dalla ripartizione di compiti e ruoli fra i vari soggetti in vista del raggiungimento del comune obiettivo di effettuare attività di commercio di stupefacenti".
[548] Nello stesso senso e sempre in tema di associazione per delinquere dedita al traffico di stupefacenti, Cass. pen., sez. III, 11 giugno 2021, n. 47291, *Esposito.*

esteriori e formali, ma in virtù della convergenza teleologica e dell'operatività effettiva del vincolo criminoso.

Sul punto, in particolare, il generico connotato dell'illiceità degli scopi rappresenta la ragione essenziale della riconosciuta libertà di forme e della conseguente possibilità di affermare l'esistenza del sodalizio anche in assenza di atti costitutivi, statuti, regolamenti, discipline interne o cariche formalizzate[549].

La giurisprudenza di legittimità, infatti, ha più volte ribadito che il nucleo strutturale del delitto associativo si concretizza nell'accordo di volontà tra i soggetti, al quale si aggiunge la predisposizione di mezzi funzionali alla commissione dei delitti fine: ciò che assume rilevanza, dunque, non è la formalizzazione dell'accordo in un atto di costituzione o in manifestazioni rituali di adesione, bensì la circostanza che, in conseguenza della volontà convergente degli associati, si realizzi di fatto la struttura criminosa prevista dalla legge[550].

A nulla rilevano, pertanto, ai fini della sussistenza del reato, numerosi fattori accidentali, quali la materiale riunione degli associati, l'identità di residenza, la reciproca conoscenza dei membri, il subentro di nuovi membri o il recesso di altri, l'identificazione nominativa di tutti i partecipi da parte dell'autorità, il possesso di armi, o la partecipazione congiunta dei membri ad ogni singolo reato[551].

3.2. L'individuazione dei ruoli nel sodalizio criminoso: profili giurisprudenziali e dottrinali

L'individuazione dei ruoli apicali all'interno del sodalizio criminoso è stata oggetto di elaborazione giurisprudenziale stratificata e di attenzione costante da parte della dottrina. La ricostruzione giurisprudenziale consente di delineare le figure apicali come soggetti che, pur in forme diverse – direttive, propulsive o organizzative - sono indispensabili all'esistenza della *societas sceleris*.

La Suprema Corte ha, in primo luogo precisato, che la qualifica di capo non si esaurisce nella mera posizione formale di vertice, ma implica il concreto esercizio di un potere di

[549] Cfr, ANTOLISEI F., *Manuale di diritto penale*, *Parte Speciale*, vol. II, XVI ed, 2016, p. 249; MANZINI V., *Trattato di diritto penale italiano,* V ed., vol. VI, 1987, pp. 196.
[550] Sul punto si veda Cass. pen., sez. I, 22 aprile 1985, n. 7462; conformi Cass. pen., sez. I, 27 febbraio 1993, n. 5343; , 27.2.1993.
[551] Cfr. Cass. pen., 13 febbraio 1970, n. 345.

direzione e comando tale da collocare il soggetto in una posizione di supremazia gerarchica sugli altri consociati, essenziale ed infungibile[552].

Accanto al capo, la figura del promotore è stata delineata come quella di colui che non solo ha avuto un ruolo genetico nella costituzione del sodalizio, ma si è altresì adoperato per consolidarne la stabilità e per accrescerne la pericolosità[553]. Con la figura dell'organizzatore o "coordinatore", infine, si fa riferimento a colui che in piena autonomia si adopera per il reperimento dei mezzi, per l'impiego razionale delle strutture associative e per la gestione complessiva delle risorse necessarie alla realizzazione del programma criminoso: tale ruolo non si esaurisce, dunque, in una funzione meramente esecutiva ma implica un contributo essenziale nell'attività di promuovere nuove adesioni, di sovraintendere la gestione complessiva del gruppo e di assumere decisioni strategiche per il *pactum sceleris*[554].

La prova dell'effettivo svolgimento di ruoli apicali - capo, promotore e organizzatore - non può tuttavia desumersi in via automatica dalla sola appartenenza ad un sodalizio di struttura gerarchica, dovendo il giudice in concreto verificare l'esistenza di condotte sintomatiche dell'esercizio di poteri direttivi o propulsivi[555].

Sul punto, la Corte ha valorizzato diversi indicatori fattuali: la convergenza delle dichiarazioni di collaboratori di giustizia; la partecipazione a riunioni di rilevanza strategica per la vita del sodalizio; il ruolo di arbitro nelle controversie che insorgono tra i sodali; la gestione delle risorse economiche e la natura fiduciaria dei rapporti verso altri criminali esterni[556].

Quanto alla distribuzione dei ruoli nell'organizzazione, la giurisprudenza di legittimità ha poi costantemente precisato che, per l'integrazione del delitto di associazione per delinquere, non è necessaria la presenza di una struttura interna rigidamente organizzata né che vi sia una formale distinzione di ruoli tra i sodali. La norma, del resto, configura la presenza di promotori, costitutori o organizzatori come una evenienza eventuale e non

[552] Cfr. Cass. pen., sez. II, 12 febbraio 2021, n.7839.
[553] Cfr. Cass. pen., sez. II, 27 settembre 2016, n. 52316.
[554] Cfr. Cass. pen., sez. VI, 10 maggio 1994, n. 11446.
[555] Cass. pen., sez. VI, 15 giugno 2011, n. 25698, secondo la quale "per poter affermare la qualità di "promotore" od "organizzatore" è necessaria la prova del ruolo in concreto svolto da coloro cui tale qualifica viene attribuita, atteso che i compartecipi di un'associazione priva di una struttura gerarchica non possono, per ciò stesso ed in modo automatico, essere ritenuti "promotori" od "organizzatori"".
[556] Cfr. Cass. pen., sez. V, 24 ottobre 2018, n.15041.

necessaria, idonea ad integrare un'autonoma ipotesi criminosa con un più elevato disvalore, ma non indispensabile ai fini della sussistenza dell'accordo associativo[557].

Ne consegue che i compartecipi di un sodalizio privo di articolazioni gerarchiche non possono essere automaticamente qualificati come promotori o organizzatori in mancanza di una specifica contestazione e di una puntuale dimostrazione del ruolo concretamente svolto nell'associazione[558].

Questo principio vale, pertanto, anche per le forme associative atipiche, avendo la giurisprudenza, come si illustrerà nel prosieguo, più volte ritenuto configurabile il delitto di cui all'articolo 416 c.p. in presenza di gruppi operanti esclusivamente in rete, privi di un vertice individuabile o di una direzione centralizzata[559]. La Corte, per far valere tale estensione, richiamava, in particolare, le proprie statuizioni in materia di associazione sovversiva con finalità di terrorismo internazionale, dove si ribadiva che il requisito dell'organizzazione non implica necessariamente il riferimento a modelli ordinari di aggregazione criminale, a strutture tradizionali di comando o coordinamento[560].

Questo orientamento giurisprudenziale, che valorizza la dimensione funzionale dell'accordo criminoso, privilegiando la capacità operativa dell'organizzazione rispetto alla normale distribuzione dei compiti, agevolerà, come di seguito si dirà nel dettaglio, l'inclusione entro l'ambito applicativo dell'articolo 416 c.p. di manifestazione associative che presentano schemi più fluidi, orizzontali e reticolari.

3.3. La condotta di partecipazione all'associazione a delinquere: profili controversi in dottrina e giurisprudenza

La condotta di partecipazione all'associazione per delinquere non è univocamente definita nei suoi contorni oggettivi, tanto in dottrina quanto in giurisprudenza. In ragione della natura atipica "a forma libera" della condotta, la nozione di partecipazione associativa è stata oggetto nel tempo di lettura eterogenee che hanno portato all'elaborazione di tre modelli interpretativi principali.

---

[557] Sul punto v. Cass. pen., sez. VI, 14 ottobre 2016, n. 52590; Cass. pen., sez. V, 8 febbraio 1983, n. 1768.
[558] Sul punto v. Cass. pen., 10 aprile 2003, n. 17027; analogamente già Cass. pen., sez. VI, 12 aprile 1986, n. 2894.
[559] Cfr. Cass. pen., sez. fer., 12 settembre 2013, n. 50620.
[560] *Ibidem*.

Il modello più risalente di partecipazione, definito "psichico", concepiva la condotta punibile come un mero atteggiamento interiore di adesione al sodalizio mafioso prescindendo dal compimento di attività materiali[561].

Tale impostazione, tuttavia, si è rivelata sin da subito problematica, poiché ancorata a un elemento di natura esclusivamente soggettiva e, in quanto tale, non suscettibile di essere provato empiricamente; inoltre, tale teoria si poneva in evidente frizione con principi cardine del diritto penale, come il principio di personalità della responsabilità penale, il principio di materialità della condotta e quello di offensività[562].

A partire dalla seconda metà degli anni '80 la concezione meramente psichica di partecipazione ha ceduto il passo al modello cosiddetto causale.

Quest'ultimo modello, sviluppatosi a partire dalla sentenza Arslan[563], riconosceva la condotta partecipativa in qualsiasi contributo, anche minimo, purché non insignificante, che il singolo avesse apportato alla vita dell'associazione e al perseguimento dei suoi scopi. Il partecipe è dunque colui che, pur non avendo assunto un ruolo di costituente ed organizzatore, decide di aderire all'associazione, impegnandosi a svolgere attività continuative per il perseguimento degli scopi comuni: ciò implica l'assunzione di compiti, anche marginali, in una posizione funzionalmente subordinata rispetto a chi dirige, e la disponibilità ad operare in via esecutiva per la realizzazione del programma criminoso[564].

---

[561] Si veda, sul punto, PIOLETTI U., voce *Associazione per delinquere*, in *Enc. forense*, 1958, vol. I, p. 472, secondo cui i partecipanti sono coloro che aderiscono non solo all'idea e all'organizzazione criminale, ma che accettano anche di porsi sotto la direzione dei capi.

[562] Sul punto, si osserva che ricondurre la fattispecie oggettiva della partecipazione associativa alla sola manifestazione di volontà di adesione al sodalizio comporta rilevanti criticità sul piano sistematico: in particolare, si è evidenziato come tale impostazione finisca per generare il rischio che ciascuno associato venga chiamato a rispondere non già per il proprio concreto contributo, bensì per i risultati complessivamente prodotti dall'organizzazione criminale nel suo insieme. In proposito cfr. FIANDACA G., *Criminalità organizzata e controllo penale*, in *Ind. pen.*, 1991, p. 17; anche GUERINI T., INSOLERA G., *Diritto penale e criminalità organizzata*, Giappichelli, 2019, p. 47.

[563] Cfr. Cass. pen., sez. I, 22 aprile 1985, n. 7462, la cui massima recita come segue: "Il delitto di partecipazione ad associazione per delinquere si configura certamente come reato a forma libera, nel senso che qualsiasi Azione, con qualsiasi modalità eseguita - purché, ovviamente, causale rispetto all'evento tipico, cioè idonea a cagionarlo - è costitutiva della materialità del fatto di tale delitto. Ma ciò non significa che nell'ambito della distribuzione dei compiti caratterizzante ogni struttura associativa finalizzata ad uno scopo - e costituente il quadro di riferimento della condotta tipica - non si debba concretamente individuare e specificare la "parte" svolta dal "compartecipe" o, se si preferisce, il "tassello", sia pure mobile e sostituibile, del "mosaico" concreto, il contributo, cioè, minimo ma non insignificante dal singolo apportato alla vita della struttura ed in vista del perseguimento del suo scopo. Se così non fosse, la previsione normativa del "solo fatto di partecipare all'associazione" sfuggirebbe completamente ad ogni possibilità di tipizzazione della condotta punibile e la stessa, per tal modo, non si sottrarrebbe a fondati rilievi di costituzionalità per l'assoluta carenza di tassatività del dato normativo".

[564] In proposito, v. VALIANTE M., *Natura plurisoggettiva della partecipazione all'associazione criminale*, in *Riv. it. dir. e proc. pen*., 1, 1987, p. 55.

In questo senso, infatti, la giurisprudenza ha sottolineato che per dimostrare la partecipazione all'associazione sarà necessaria la prova chiara e certa della volontà di far parte stabilmente del gruppo e di apportare un contributo concreto alla realizzazione delle finalità associative[565].

Tuttavia, fondare la tipicità della condotta esclusivamente sull'idoneità del contributo al rafforzamento del sodalizio rischia di compromettere la determinatezza della fattispecie, considerato che l'effettivo rafforzamento dell'associazione, nella pratica, risulta difficilmente accertabile e quantificabile in concreto[566].

In secondo luogo, il modello causale rischiava di assorbire e neutralizzare lo spazio applicativo del concorso esterno, trasformando qualsiasi contributo in partecipazione. Si trattava, dunque, di un modello dalla "vocazione onnivora" in quanto, subordinando la rilevanza penale della condotta alla mera dimostrazione di un qualsiasi contributo dotato di efficienza eziologica, finiva per ricomprendere nella nozione di partecipazione anche condotte prive di un effettivo inserimento unico nel sodalizio[567].

Sulla scorta delle critiche dottrinali rivolte ai modelli precedenti, la giurisprudenza elaborava così un nuovo paradigma, noto come "modello organizzatorio", che attribuiva centrale rilievo all'effettivo inserimento del partecipante all'interno della compagine associativa. In particolare, la volontà di aderire al sodalizio doveva trovare riscontro in un atto di accettazione da parte degli altri membri dell'associazione. Secondo tale modello, l'*intraneus* si identificava con un soggetto la cui volontà di operare a favore del gruppo veniva confermata da una decisione univoca e concorde ad inserirlo nell'organizzazione, assegnandogli un ruolo stabile all'interno della struttura[568].

Anche tale modello, tuttavia, non era privo di criticità: in particolare, l'assegnazione di un ruolo stabile non implicava necessariamente l'effettivo adempimento dei compiti ad

---

[565] Cass. pen., sez. I, 21 aprile 1982, n. 1674; Cass. pen., sez. VI, 21 novembre 1989, n. 16164; Cass. pen., sez. I, 9 dicembre 1993, n. 11307; Cass. pen., sez. II, 26 gennaio 2005, n. 2350; Cass. pen., sez. II, 11 febbraio 2010, n. 5424; Cass. pen., sez. III, 25 gennaio 2012, n. 8024; Cass. pen., sez. I, 18 dicembre 2015, n. 1911.

[566] Cfr. DE FRANCESCO G., *Dogmatica e Politica criminale nei rapporti tra concorso di persone ed interventi normativi contro il crimine organizzato*, in *RIDPP*, 1994, p. 1281; INGROIA A., *L'associazione di tipo mafioso*, Giuffrè, 1993, p. 41.

[567] Cfr. MAIELLO V., *Il concorso esterno tra indeterminatezza legislativa e tipizzazione giurisprudenziale. Raccolta di scritti,* Torino, 2014, pp. 102 e 106.

[568] Sul punto, v. DE FRANCESCO G., *Gli articoli 416, 416-bis, 416-ter, 417, 418 c.p.,* in *Mafia e criminalità organizzata*, I, Torino, 1995, p.34; IDEM, voce *Associazione per delinquere e associazione di tipo mafioso*, in *Dig. disc. pen*., vol. I, 1987, p. 295; INGROIA A., *L'associazione di tipo mafioso*, cit., p. 40; Cass., Sez. feriale, 1 settembre 1994, Graci, in *Cass. pen*., 1995, p. 539.

esso connessi determinando il rischio di una nozione formale e soggettivistica di partecipazione[569].

La constatazione dei limiti dei modelli causale e organizzatorio ha spinto la giurisprudenza ad elaborare un terzo modello, oggi largamente prevalente, che armonizza i due approcci precedenti. Si tratta del cosiddetto "modello misto" che tenta di combinare, da un lato, l'esigenza strutturale di verificare che il soggetto sia effettivamente inserito nel sodalizio e riconosciuto dai membri come parte stabile dell'organizzazione e, dall'altro, la dimensione causale che richiede di accertare un contributo concreto e funzionale del partecipe al rafforzamento del gruppo criminale[570].

Nel tempo, il modello misto è stato declinato con accentuazioni diverse, dal momento che alcune interpretazioni privilegiano la componente causale, altre quella strutturale.

La questione interpretativa è stata definitivamente affrontata dalle Sezioni Unite con la sentenza Mannino *bis* del 2005 che hanno delineato una versione "sincretistica-additiva" del modello misto. Secondo tale prospettiva la partecipazione associativa si configura come una combinazione coerente degli elementi del modello organizzatorio e di quelli del modello causale, in quanto la condotta partecipativa non si esaurisce nell'aver acquisito uno status formale all'interno dell'associazione, ma richiede altresì che il soggetto compia atti concreti e continuativi che esprimono il ruolo assegnatogli e contribuiscano agli obiettivi del sodalizio[571].

Quanto al tipo di contributo causale, la giurisprudenza di legittimità ha affermato che non occorre un contributo indispensabile, essendo sufficiente anche un rapporto minimo, purché apprezzabile in concreto, tale da contribuire all'esistenza e al rafforzamento dell'associazione[572].

Si è inoltre riconosciuta la configurabilità della condotta partecipativa anche quando il soggetto agisca perseguendo un proprio tornaconto personale, nella misura in cui il suo operato concorra, seppur indirettamente, alla realizzazione degli scopi del sodalizio[573].

---

[569] Cfr. CAVALIERE A., *I reati associativi tra teoria, prassi e prospettive di riforma*, in FIANDACA G., VISCONTI C. (a cura di), *Scenari di mafia. Orizzonte criminologico e innovazioni normative*, Giappichelli, 2010, p. 151.
[570] In dottrina sul punto v. VALIANTE M., *Il reato associativo*, Giuffrè, 1990, pp. 82-83.
[571] Cfr. Mannino bis, Cass. pen., Sez. VI, 12 luglio 2005, n. 33748.
[572] Cfr. Cass. pen., sez. II, 22 gennaio 2010, n. 5424; precedente confome v. Cass. pen., sez. VI, 2 novembre 1998, n. 1472.
[573] Cfr. Cass. pen., sez. II, 8 novembre 2013, n. 46989.

Resta in ogni caso indispensabile individuare in concreto il contributo fornito dal singolo, anche se è secondario, per evitare che la previsione normativa del partecipare resti priva di contenuto determinato.

È stato infine chiarito che la partecipazione non presuppone necessariamente un vincolo di durata indeterminata né una dedizione esclusiva al sodalizio: sono punibili anche le forme di adesione destinate, *ab origine*, ad una durata limitata, purché caratterizzate da un apporto concreto all'organizzazione, a nulla rilevando che il soggetto persegua parallelamente vantaggi personali ulteriori e autonomi rispetto agli scopi del gruppo[574].

La continuità associativa e la condivisione del progetto criminale comune sono i principi alla base dell'ingresso e del recesso dei membri dell'associazione.

Sul punto, la giurisprudenza della Corte di Cassazione ha chiarito come l'associazione non venga concepita come un vincolo rigido ed immutabile, ma come un accordo tendenzialmente aperto all'adesione di terzi, carattere quest'ultimo che costituisce un sintomo della stabilità stessa dell'organizzazione, che si mantiene intatta in caso di variazione degli associati[575]. In particolare, l'ingresso nella rete associativa è stato definito come una "adesione in progress", cioè una partecipazione che si realizza attraverso un accordo plurilaterale che comporta la condivisione del progetto criminale comune e l'accettazione delle regole interne[576].

La variazione della compagine associativa, sia per l'adesione di nuovi membri sia per il recesso di alcuni, non incide sulla permanenza dell'associazione e non interrompe le attività criminali o l'ampliamento sul territorio[577]. Eventuali modifiche nel ruolo di un partecipante o nelle sue attività non rilevano ai fini degli equilibri interni

[574] Cfr. Cass. pen., sez. II, 24 novembre 2016, n. 52005; Cass. pen., sez. V, 8 ottobre 2014, n. 18756.
[575] Sul punto v. Cass. pen., sez. VI, 16 dicembre 2011, n. 9117, nella specie la struttura associativa si era formata attraverso la cooptazione, da parte di un assessore regionale alla sanità e del suo più stretto collaboratore, di una serie di soggetti che, nominati in posti strategici dell'organizzazione sanitaria, provvedevano a loro volta a nominare funzionari e primari con l'obiettivo finale di controllare illegittimamente appalti e forniture delle Asl regionali.
[576] *Ibidem*.
[577] Cfr. Cass. pen., sez. II, 26 ottobre 2021, n.1688, dove la Corte ha precisato che, per affermare che ad un'associazione ne segua una diversa, occorre la prova che la seconda sia scaturita da un diverso patto criminale oppure che quella originaria abbia definitivamente cessato di esistere a causa di un evento traumatico, generatore di discontinuità nel programma associativo, come in caso di faide o scissioni.

dell'associazione, salvo, ad esempio, non vi sia stato un trasferimento ad altra organizzazione criminale[578].

Il recesso dell'associato, ovvero la volontaria cessazione del vincolo con l'organizzazione, deve essere valutato caso per caso ed è rilevato sulla base di una condotta esplicita, coerente ed univoca, e non semplicemente attraverso la mancanza di comportamenti ulteriori conformi agli scopi dell'associazione.[579]

Anche in assenza di una dichiarazione formale, il giudice può accertare l'allontanamento effettivo e irreversibile del soggetto dal gruppo criminale in presenza di elementi probatori concreti, oggettivi e sintomatici, non essendo invece sufficienti indizi o circostanze generiche come l'età dell'individuo, il subingresso di altri vertici nel gruppo, il trasferimento in un'altra residenza o in un luogo in cui si assume che l'associazione non operi[580].

3.4. L'elemento soggettivo dell'associazione per delinquere: l'affectio societatis

Sul piano soggettivo, il reato di associazione per delinquere trova il suo fondamento nella *affectio societatis*, intesa come consapevole adesione del soggetto al vincolo criminoso che lo lega stabilmente ad un'organizzazione criminale strutturata. Non è sufficiente, infatti, la mera partecipazione occasionale a singole condotte delittuose, né tantomeno la contiguità ambientale o la vicinanza personale con taluni sodali; ciò che rileva è la coscienza e volontà di inserirsi in una trama organizzativa destinata alla realizzazione di una pluralità indeterminata di delitti, con un impegno che, sebbene non debba protrarsi permanentemente nel tempo, deve però superare la dimensione di un contributo contingente[581].

La giurisprudenza di legittimità ha più volte sottolineato come tale atteggiamento psichico possa essere desunto anche da fatti concludenti, ossia da comportamenti

---

[578] Cfr. Cass. pen., sez. V, 15 luglio 2021, n. 32767 secondo la corte ci sono altre situazioni che occorre verificare: "*che le condotte sono successive all'archiviazione o che il soggetto sia passato ad una diversa organizzazione criminale ovvero che si sia verificata una successione nelle attività criminali tra organismi diversi, sia pure con lo stesso nome ed operanti nello stesso territorio".*

[579] Sul recesso dell'associato si vedano Cass. pen., sez. VI, 30 settembre 2020, n. 28821; Cass. pen., sez. II, 12 febbraio 2021, n.7837.

[580] Sull'accertamento del giudice sull'avvenuto recesso v. Cass. pen., sez. VI, 21 maggio 1998, n. 3089.

[581] Sull'elemento soggettivo si veda Cass. pen., sez. I, 1 febbraio 1991, n. 1332; analogamente, più di recente, Cass. pen.,sez. V, 1 dicembre 2000, n. 12525.

oggettivi che rivelano la stabile compartecipazione al sodalizio. L'adesione al sodalizio, infatti, non necessita di manifestazioni formali o dichiarazioni espresse, potendo invece risultare da elementi fattuali come la reiterazione di contatti con altri membri, la partecipazione alla gestione delle risorse del gruppo, l'esecuzione di compiti funzionali alla sopravvivenza e al rafforzamento della struttura organizzativa[582].

Proprio in questa prospettiva, la giurisprudenza ha chiarito che la mera commissione di uno o più delitti riconducibili al programma criminoso non costituisce di per sé prova automatica della partecipazione, ma assume valore di indizio qualificato quando le modalità esecutive e il contesto consentono di ricollegare tali attività all'esistenza di un vincolo associativo[583].

Rappresentano poi indicatori di grande rilevanza, poiché denotano l'inserimento stabile del soggetto nel circuito criminale, la pluralità delle condotte delittuose, la loro frequenza e la continuità dei rapporti con gli altri associati[584]. Altrettanto significativo, inoltre, è che la mancata conoscenza personale tra tutti i componenti non incide sulla configurabilità dell'associazione[585].

Anche la partecipazione ad un singolo episodio criminoso può in astratto costituire elementi indiziante dell'appartenenza all'associazione: tuttavia, in tale ipotesi, il valore probatorio risulta attenuato, poiché occorre che da quella condotta si possa desumere non solo la compartecipazione materiale all'episodio, ma anche la volontà di aderire al progetto collettivo e di condividerne le finalità[586].

Infine, occorre precisare che il dolo del delitto di associazione per delinquere non si sovrappone al dolo dei reati fine, i quali devono essere oggetto di prova autonoma[587].

Come osservato in dottrina, infatti, il dolo associativo si caratterizza per la rappresentazione e l'accettazione di un ruolo organizzativo finalizzato alla realizzazione di un programma comune di delitti, individuabili per tipologie ma non ancora specificati negli elementi concreti. Il dolo dei reati fine, al contrario, si configura con riferimento ad

---

[582] *Ibidem*; sui singoli elementi indizianti si vedano anche Cass. pen., sez. VI, 17 novembre 1994, n. 11446; in senso conforme, più di recente, Cass. pen., sez. I, 5 agosto 2003, n. 33033.
[583] Cfr. Cass. pen., sez. VI, 16 dicembre 2011, n. 9117.
[584] Cfr. Cass. pen., sez. VI, 17 novembre 1994, n.11446.
[585] Sul punto, v. Cass. pen., sez. VI, 16 dicembre 2011, n. 9117.
[586] Cfr. Cass. pen., sez. VI, 17 novembre 1994, n.11446; in senso conforme, più di recente, v. Cass. pen., sez. I, 55 agosto 2003, n. 33033.
[587] Sulla differenza tra dolo associativo e dolo dei reati-scopo si veda Cass. Pen., sez. III, 4 marzo 2015, n. 26724.

un singolo fatto di reato, connotato da determinate coordinate temporali, spaziali e modali che lo rendono unico. Sussiste, dunque, una vera e propria discontinuità psicologica tra la programmazione generale della serie criminosa e la realizzazione di un episodio specifico[588].

4. L'inquadramento giurisprudenziale delle associazioni per delinquere di tipo cibernetico

A fronte dell'analisi degli elementi costitutivi dell'associazione per delinquere, la ricerca si concentrerà ora sui principali gruppi criminali attivi nel cyberspazio, nei confronti dei quali è stata contestata tale fattispecie incriminatrice.

L'obiettivo non sarà soltanto ricostruire l'inquadramento giuridico delle condotte poste in essere, ma di evidenziare il modo in cui la giurisprudenza ha individuato e adattato i requisiti tipici dell'associazione per delinquere all'interno di realtà che, per loro natura, si discostano sensibilmente dal modello tradizionale di criminalità organizzata.

In particolare, verranno esaminati gli arresti giurisprudenziali più significativi, che hanno contribuito a delineare con maggiore precisione i criteri di valutazione degli elementi costitutivi a fronte di condotte associative che, pur essendo morfologicamente atipiche, rivelavano comunque una capacità offensiva e una pericolosità sociale non meno rilevante rispetto alle forme di criminalità tradizionalmente operanti offline.

4.1. La dimensione associativa nelle comunità online dedite allo scambio di materiale pedopornografico

Le comunità virtuali dedite allo scambio di materiale pedopornografico costituiscono aggregazioni eterogenee di soggetti che si avvalgono di strumenti tecnici diversi - forum, gruppi ospitati su piattaforme generaliste, mailing list, newsgroup, reti P2P - per reperire, scambiare, diffondere e talora archiviare materiale pedopornografico.

---

[588] Cfr. DE FRANCESCO G., *Associazione per delinquere e associazione di tipo mafioso*, in *Digesto penale*, I, Torino, 1987, p. 292; INGROIA A., *L'associazione di tipo mafioso*, cit., p. 44.

La questione centrale, su cui si è pronunciata la giurisprudenza, di merito e di legittimità, è se tali gruppi possano integrare i tratti tipici dell'associazione per delinquere di cui all'416 c.p., oppure se rimangano, giuridicamente, solo una somma di condotte concorrenti ma episodiche. Le decisioni giurisprudenziali di seguito esaminate forniscono una risposta sul punto, coerente e per molti versi convergente.

Si ritiene opportuno analizzare, *in primis*, la giurisprudenza di merito che, in maniera più chiara, rispetto alle sentenze di legittimità, ricostruisce in maniera più precisa il funzionamento di comunità online[589] e che, peraltro, rappresenta l'esito dello stesso procedimento su cui la Corte di Cassazione, già nel 2004, si era espressa in fase cautelare.

In particolare, nel caso di specie, la ricostruzione fattuale effettuata dal Tribunale offre una radiografia interna di una comunità virtuale intitolata "Fotodipreteen", creata sfruttando uno spazio web a disposizione degli utenti per acquisire e diffondere fotografie e filmati di carattere pedopornografico.

Gli accertamenti tecnici hanno documentato non solo la presenza di album tematici di contenuto illecito, ma soprattutto l'esistenza di regole per l'ingresso nel gruppo, per il mantenimento del rapporto e sanzioni in caso di trasgressione.

In particolare, al momento del primo accesso il sito presentava il seguente messaggio: "Benvenuti in foto di preteen lasciate che vi dica alcune clausole. A una settimana dall'iscrizione che non metterà materiale verrà espulso tutti possono mettere foto purché le cose ritratte siano sotto i 18 anni potete metterle porno, o nude gay o no basta che siano minorenni se volete mettere video solo formato mpg e ora divertitevi"[590].

L'accesso era ristretto e mediato dall'autorizzazione del gestore - che si presentava come "il padrone" - con messaggi di servizio che imponevano un vero e proprio *enforcement* interno: "a una settimana dall'iscrizione chi non metterà materiale verrà espulso", "ogni settimana eliminerò chi non avrà messo […] almeno una foto", "sono già 20 gli esclusi"[591].

Tale architettura regolativa – si pensi anche solo alla complessa procedura di iscrizione con nickname e autorizzazione del gestore o, ancora, alla procedura di espulsione degli inadempienti – denotava una *governance* stabile del gruppo, destinata a perdurare nel tempo.

---

[589] Tribunale di Siracusa, sent. n. 229 del 19 luglio 2012.
[590] *Ivi*, p. 4.
[591] *Ivi*, pp. 4-5.

Secondo il Tribunale, la "virtualità" del legame non era di ostacolo alla configurabilità dell'associazione – anzi, dalle regole di ammissione e permanenza emergeva chiaramente la natura, la struttura, le finalità e le modalità della partecipazione, realizzando un "caso di scuola" di associazione per delinquere in ambiente digitale[592].

Il reato è stato ritenuto configurabile persino rispetto ai partecipanti che non partecipavano agli "upload": il mancato invio di materiale da parte degli imputati, infatti, non ha avuto alcuna efficacia esimente in quanto il delitto associativo, quale reato di pericolo che si perfeziona con la creazione del vincolo associativo, non richiede l'effettiva commissione da parte di tutti gli associati dei c.d. reati scopo e, a ben vedere, neppure la realizzazione dei reati scopo *tout court*[593].

Sul medesimo caso di associazione per delinquere diretta alla commissione di reati di distribuzione e divulgazione per via telematica di foto pedopornografiche, si era espressa, già nel 2004, la Corte di cassazione in sede cautelare.

Nel valutare la presenza degli elementi oggettivi e soggettivi di cui all'art. 416 c.p., la Corte richiamava quanto già accertato dal Tribunale, secondo cui quanto all'elemento oggettivo, "era stata creata una comunità virtuale, regolata dalle disposizioni dettate dal promotore e gestore C. e quindi dotata di una stabile organizzazione, diretta allo scambio ed alla divulgazione tra tutti i possibili attuali e futuri aderenti di foto pedopornografiche di bambini di età inferiore ai dodici anni"[594]; dall'altro lato, avallava altresì la presenza dell'elemento soggettivo, ritenendo che "tutti gli aderenti erano stati resi edotti dello scopo e delle finalità del gruppo di scambio, che la partecipazione al gruppo era ammessa solo dopo l'esplicita accettazione di tali scopo e finalità nonché dell'impegno di inviare con una certa frequenza foto pedopornografiche, che la permanenza nel gruppo era condizionata dall'invio effettivo di dette foto, e che del resto la fitta rete di regole imposte non consentiva una visita occasionale, per mera curiosità, ma richiedeva la consapevolezza piena del contenuto e dello scopo del gruppo e l'accettazione delle finalità perseguite dalla comunità di cui si entrava a far parte"[595].

[592] *Ivi*, p. 6.
[593] *Ivi*, p. 7.
[594] Cfr. Cass. pen., sez. III, 2 dicembre 2004, n. 8296.
[595] *Ibidem*.

Veniva altresì accertato che i membri della comunità non si erano mai limitati ad una singola sporadica visita sul sito, avendo invece effettivamente compiuto più operazioni di scambio di materiale pedopornografico.

Sulla stessa linea, la giurisprudenza di legittimità si è pronunciata nuovamente nel 2012 sulle associazioni per delinquere dedite allo scambio di materiale pedopornografico, anticipando, peraltro, alcune riflessioni che saranno poi riprese ed ulteriormente sviluppate nelle pronunce successive[596].

Nella richiamata sentenza, la Corte ribadisce che per la configurabilità del reato associativo non è necessario un patto costitutivo espresso "indipendentemente dall'accertamento dell'esistenza di un vero e proprio patto costitutivo dell'associazione, che non è requisito indispensabile per la configurazione del reato"[597]: in questo contesto, deve però valorizzarsi l'*affectio societatis*, che si concretizza nella dimostrazione di un apporto consapevole e continuativo alla vita del sodalizio, non essendo sufficiente un comportamento occasionale, come il mero accesso sporadico ad una chat lo scambio isolato di materiale.

In questo senso, la Corte sottolineava come gli imputati non si limitassero ad accedere ad una piattaforma, ma avessero dato vita ad una vera e propria "struttura telematica organizzata", seppur rudimentale, caratterizzata dalla selezione degli accessi tramite password, dall'uso di software di anonimizzazione per occultare gli indirizzi di connessione e dal collegamento con altri gruppi attivi nel medesimo ambito.

Nella stessa direzione, trattando un caso analogo, si è pronunciata l'anno successivo altra giurisprudenza di legittimità[598].

Nell'occasione, sul piano oggettivo, la Corte ha ribadito un principio consolidato, ossia che l'associazione criminosa si distingue dal mero concorso di persone per la sua struttura e per la capacità di proiettarsi verso la commissione di una pluralità indeterminata di reati. Secondo i giudici, infatti, non sarebbe necessario un'articolata struttura organizzativa, bastando la presenza di un minimo apparato di regole e strumenti funzionali al perseguimento del programma criminoso. Ciò in quanto "quello associativo si qualifica per essere un accordo di carattere 'aperto'. Lo scopo comune, oggetto dell'incontro di volontà, consiste nel programma di commettere – cogliendo le opportunità che, via via,

[596] Cfr. Cass. pen., sez. III, 28 giugno 2012, n. 33563.
[597] *Ivi*, par. 2.3.
[598] Cass pen., sez. III, 14 marzo 2013, n. 20921.

si presentano – una pluralità indefinita di reati, sia pure dello stesso genere, di modo che "è sufficiente una organizzazione minima perché il reato si perfezioni"[599].

Applicando questo principio al caso concreto, la Corte individua l'esistenza di una vera e propria comunità criminale nonostante la sua natura immateriale e virtuale. Gli accertamenti investigativi, infatti, hanno portato alla luce un gruppo composto da oltre 6000 affiliati, suddivisi in sottogruppi nazionali e caratterizzato da "anonimato", "rigida gerarchia", "ferree regole di partecipazione e di esclusione" e, soprattutto, dall'obbligo di contribuire allo scambio di materiale illecito per poter mantenere la propria appartenenza[600].

In tal senso il vincolo associativo si manifestava con chiarezza: la partecipazione non era libera né occasionale, ma subordinata all'accettazione di regole precise: "la partecipazione al gruppo era ammessa solo dopo l'esplicita accettazione di tali scopi e finalità nonché dell'impegno di inviare con una certa frequenza foto pedo-pornografiche. Anche la permanenza nel gruppo era condizionata all'invio effettivo di dette foto"[601].

Questi elementi dimostravano come la struttura associativa fosse non soltanto astrattamente configurabile, ma concretamente operante, tanto da consentire la creazione e la gestione di un'"imponente archivio pedopornografico, il più grande mai rinvenuto, stimato in milioni di files".

Quanto all'elemento soggettivo, la Corte ha posto l'accento sulla necessità che l'adesione al sodalizio fosse avvenuta con la consapevolezza e la volontà stabile di contribuire al perseguimento degli scopi comuni. Non era necessaria un'esplicita manifestazione di intenti, in quanto la volontà poteva desumersi "attraverso comportamenti significativi che si concretino in una attiva e stabile partecipazione"[602].

In altri termini, l'elemento psicologico si riteneva integrato laddove l'agente, accettando le regole del gruppo ed impegnandosi a rispettarle, avesse manifestato una scelta volontaria di adesione al progetto criminale e una disponibilità continuativa a concorrere alla sua realizzazione.

Nel caso di specie, la Suprema Corte ha ritenuto che la condizione stessa di ingresso e di permanenza nel gruppo - ovvero l'invio costante di materiale pedopornografico -

[599] *Ivi*, par. 3.1.
[600] *Ivi*, par. 3.1.
[601] *Ibidem*.
[602] *Ibidem*.

escludesse qualsiasi possibilità di adesione inconsapevole o casuale: "dal momento che tutto ciò non poteva che avvenire con consapevolezza e non in modo casuale, agevoli sono le conseguenze che se ne traggono, sia sul piano soggettivo che per quel che attiene alla configurabilità del reato-fine"[603].

4.2. Le comunità di hacktivisti operanti nel cyberspace: il caso Anonymous

Prima di affrontare le pronunce della giurisprudenza di legittimità in materia di associazioni di hacktivisti e, in particolare, quelle che hanno coinvolto il collettivo Anonymous, appare necessario soffermarsi su un aspetto preliminare relativo alla natura strutturale ed organizzativa di tali formazioni criminali.

La comprensione del funzionamento interno di queste specifiche comunità virtuali rappresenta un presupposto indispensabile per interpretare correttamente le pronunce giurisprudenziali. Solo attraverso questa illustrazione, diventa possibile, infatti, comprendere le ragioni per cui i giudici di legittimità hanno adottato determinate soluzioni giuridiche.

In questa prospettiva, un riferimento imprescindibile è rappresentato dall'analisi dell'*Internet Relay Chat network* (IRC)[604], il principale strumento informatico attraverso cui i membri del collettivo si incontrano virtualmente, discutono, si coordinano e pianificano le proprie iniziative. L'IRC non può essere assimilato ad una comune chat o a un forum presente sul web, poiché presenta caratteristiche peculiari che lo rendono idoneo a costituire la base organizzativa di gruppi criminali privi di una struttura gerarchica e funzionale alla pianificazione delle attività degli stessi.

Tra i tratti distintivi di questa piattaforma si annoverano l'assenza di sistemi di archiviazione dei messaggi - che rende dunque impossibile una consultazione della cronologia delle conversazioni - e l'assenza di suddivisioni tematiche rigide, che lascia ampia libertà di discussione all'interno dei canali. Inoltre, si riscontra come le conversazioni avvengano in tempo reale e il volume di interazioni raggiunga livelli tali da superare di gran lunga le capacità di comunicazione tipiche di altre piattaforme

---

[603] *Ivi*, par. 3.2.

[604] Sul punto, si veda BENJAMIN V., ZHANG B., NUNAMAKER JR., CHEN H., *Examining Hacker ParticipationLength in Cybercriminal Internet-Relay-Chat Communities*, in *Journal of Management Information Systems*, 2016, vol. 33, Is.2, p. 483 (DOI: 10.1080/07421222.2016.1205918).

digitali[605]; a ciò si aggiunge poi l'anonimato garantito dall'utilizzo di nickname e dalla possibilità di creare e frequentare stanze private o pubbliche, dando vita ad una rete dinamica ed estremamente mutevole[606]. In proposito, la distinzione tra stanze segrete - accessibili soltanto a soggetti previamente autorizzati - e stanze pubbliche, accessibili a chiunque possieda le competenze tecniche per accedervi, contribuisce a delineare la complessità di tale fenomeno organizzativo[607].

Proprio tali peculiarità, impongono alla giurisprudenza un approccio interpretativo non meramente formale, ma attento alle concrete modalità di organizzazione e funzionamento di tale comunità.

Sul caso Anonymous, la giurisprudenza di legittimità ha avuto modo di pronunciarsi due volte.

Con una prima sentenza, in sede cautelare, la Corte di Cassazione[608], ha replicato ai motivi di ricorso con cui la difesa sosteneva che nel caso concreto, ove si contestava il reato di associazione per delinquere finalizzata alla realizzazione di una serie di reati informatici[609], difettassero integralmente i tre elementi costitutivi del fatto di associazione per delinquere e che non fosse ravvisabile neppure una condotta di partecipazione dell'imputato, dal momento che ciascun agente, avvalendosi delle proprie competenze tecniche, avrebbe potuto agire autonomamente, senza alcuna consapevolezza del ruolo svolto da altri soggetti.

Di particolare interesse, risulta il percorso argomentativo della Corte sulla ricostruzione della struttura organizzativa delle formazioni criminali in esame, poiché consente di chiarire i presupposti che ne giustificano l'inquadramento nell'alveo dell'art. 416 c.p.

La Corte di Cassazione ha sottolineato come il giudice di merito avesse correttamente evidenziato l'esistenza di una "vera e propria struttura", desumibile sia dallo studio delle

---

[605] *Ibidem*. Sull'*Internet Relay chat*, si veda anche Cfr. HUDSON J., WITT P., *Internet Relay Chat (IRC),* in AA.VV., *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications,* 2007, vol. 3, (a cura di) Bidgoli, John Wiley & Sons Ltd. (DOI: https://doi.org/10.1002/9781118256107.ch57), pp. 890-891.

[606] In proposito, v. BUSSOLATI N., *L'associazione per delinquere "informatica",* in AA. VV., Cybercrime, (a cura di) CADOPPI, CANESTRARI, MANNA, PAPA, 2019, UTET Giuridica, p. 264.

[607] Cfr. HUDSON J., WITT P., *Internet Relay Chat (IRC),* cit., p. 890.

[608] Cass. pen., sez. fer., 29 agosto 2013, n. 46156.

[609] Tra questi, in particolare, la realizzazione di accessi abusivi a sistemi informatici, al danneggiamento di sistemi informatici, alla detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici e all'interruzione illecita di comunicazioni informatiche o telematiche

elaborazioni informatiche riscontrate sul web, sia dall'analisi dei singoli reati accertati a cui con diversi ruoli hanno partecipato gli indagati.

La struttura associativa, secondo quanto accertato, si manifestava attraverso una serie di attività coordinate: "la predisposizione del blog ufficiale dell'organizzazione e del video di propaganda, da diffondere sul blog ufficiale"; "la predisposizione e gestione dei canali di comunicazione IRC privati", che consentivano tanto la comunicazione diretta fra due soggetti quanto il dialogo simultaneo di gruppi più ampi, su scala nazionale e internazionale; "l'organizzazione, in tali canali, delle linee strategiche; la discussione sulla vulnerabilità dei siti da attaccare; la definizione dei testi di rivendicazione poi diffusi mediante siti web e sulle pagine ufficiali"[610].

L'assetto interno del gruppo si fondava unicamente su una ripartizione delle attività in funzione delle competenze tecniche di ciascun membro. Le operazioni di hacking venivano organizzate e coordinate all'interno di due canali IRC privati, ad accesso ristretto, che costituivano il luogo deputato alla pianificazione delle azioni. L'iniziativa concreta degli attacchi era rimessa alla libera determinazione del singolo partecipante, il quale, nel corso dell'esecuzione, poteva richiedere supporto agli altri membri oppure riceverlo spontaneamente.

Parallelamente, il gruppo gestiva anche due canali IRC pubblici, accessibili senza limitazioni, che rappresentavano uno spazio più ampio di aggregazione: in essi prendevano parte numerosi utenti, non necessariamente appartenenti alla compagine hacktivista, e si discuteva di temi di attualità politica e venivano diffuse sia le rivendicazioni sia le attività riconducibili ad Anonymous Italia[611].

Accanto a tali profili di coordinamento, la Corte ha richiamato anche le attività tecniche che denotavano la stabilità e l'efficienza del sodalizio: "il mantenimento dei contatti con i media e con l'organizzazione (…) di livello internazionale; l'effettuazione delle attività di scanning, per verificare la vulnerabilità di possibili siti target, e di exploiting, per accedere abusivamente all'interno dei server che li ospitano; la progettazione, messa a disposizione e condivisione dei c.d. tools di attacco (programmi deputati ad un determinato compito)"[612].

---

[610] Cass. pen., sez. fer., 29 agosto 2013, n. 46156, par. 3.1.
[611] Sul punto, v. anche PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, cit., p. 168.
[612] Cfr. Cass. pen., sez. fer., 29 agosto 2013, n. 46156, par. 3.1.

Tali risultanze, secondo la Corte, non lasciavano dubbi sull'esistenza di un'organizzazione in rete volta all'ideazione, programmazione e realizzazione di reati informatici, data anche la creazione di appositi canali di comunicazione destinati ad operare stabilmente. Non irrilevante, poi, è l'accertata presenza di collegamenti internazionali, mirati al supporto del gruppo italiano con un aiuto internazionale per potenziare gli attacchi.

Infine, la Corte ha evidenziato la ripartizione dei compiti, sebbene priva di una gerarchia verticistica: "sono stati individuati i ruoli ricoperti dai partecipanti all'associazione: ruoli differenziati a seconda delle capacità informatiche individuali ma senza veri e propri capi, essendovi soltanto alcuni soggetti preposti alla cura dei profili organizzativi"[613]. Emblematico è stato, in tal senso, il ruolo dell'indagato, che "si dedicava, unitamente ad altri soggetti, all'ideazione e realizzazione degli attacchi (…) manteneva i contatti tra la cellula italiana e altri gruppi (…) a livello internazionale; partecipava agli attacchi, riuscendo, come nel caso del Banco di Lucca, a carpire anche dati individuali, condivisi con gli altri membri; ha fornito la bozza per il *defacement* relativo all'attacco a Vitrociset S.p.A; ha compiuto operazioni di Sql injection, riuscendo a prelevare dal sito della Guardia costiera dati riservati, che ha condiviso con gli altri membri del gruppo"[614].

In questo senso, la struttura dei canali IRC privati ha determinato di fatto i confini dell'associazione criminale: solo gli utenti con accesso a questi canali privati potevano essere considerati membri del sodalizio. Tanto è vero che l'accusa di associazione per delinquere ex art. 416 c.p. è stata rivolta esclusivamente ai partecipanti dei canali privati, in cui si coordinavano e pianificavano gli attacchi informatici, mentre gli utenti che frequentavano i canali pubblici non sono stati coinvolti nell'imputazione. La caratteristica distintiva dei canali privati risiedeva proprio nell'accesso limitato, riservato a soggetti selezionati, un meccanismo che assicurava il controllo sulla partecipazione e che trovava analogie anche nelle comunità pedopornografiche online, le quali, come visto, si dotavano di criteri precisi per l'ammissione dei nuovi membri[615].

---

[613] *Ibidem*.
[614] *Ibidem*.
[615] Cfr. PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, cit., p. 168; anche United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 44.

La giurisprudenza italiana aveva, infatti, già applicato in passato la fattispecie di associazione per delinquere a gruppi virtuali pedopornografici, ritenendo necessario che esistesse una forma di organizzazione chiusa e riconoscibile.

La sentenza relativa ad Anonymous confermava questa logica: il reato associativo online si configura soltanto quando il gruppo presenta caratteristiche di coesione e stabilità tali da consentire l'identificazione dei partecipanti effettivi[616]. Tale impostazione sembra rispondere alla necessità di contemperare la peculiarità dei gruppi virtuali – fluidi, con confini spesso indefiniti e partecipazioni occasionali – con l'esigenza di non estendere in maniera eccessiva la responsabilità penale, evitando così un'"ipercriminalizzazione" di comportamenti digitali non strettamente collegati al sodalizio criminale[617].

Un'altra vicenda esaminata dalla Corte di Cassazione trae origine dalla presunta partecipazione di un soggetto, nella veste di promotore e organizzatore, a un'associazione per delinquere finalizzata alla commissione di reati informatici, collegata al movimento internazionale Anonymous. Secondo l'accusa, tale sodalizio era finalizzato alla commissione di una serie indeterminata di *cybercrimes*, tra cui accessi abusivi a sistemi informatici, diffusione illecita di codici di accesso, danneggiamento di sistemi e interruzione di comunicazioni telematiche.

Il collegio ha riconosciuto la sussistenza degli elementi costitutivi oggettivi dell'associazione per delinquere.

Anzitutto, in opposizione alla tesi della difesa secondo cui tale organismo, operante nella "realtà virtuale", non potesse sussumersi nel 416 c.p., non essendo mossa da motivi di lucro ma da ispirazioni ideologiche, la Corte affermava che per integrare il reato di associazione per delinquere non fosse necessario né uno scopo di lucro né un'ideologia negativa, né che si potesse escludere la rilevanza penale di quelle azioni se unicamente svolte nello spazio virtuale, avendo comunque gli attacchi informatici degli effetti concreti nel mondo reale, come l'impossibilità anche solo temporanea di utilizzare sistemi informatici essenziali[618].

[616] Cass. pen., sez. fer., 29 agosto 2013, n. 46156, par. 4.
[617] Cfr. United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 16.
[618] Cfr. Cass. pen.. sez. fer., 12 settembre 2013, n. 50620, rv. 258385, p. 8

Dalla pronuncia si ricava un interessante lettura interpretativa concernente la struttura organizzativa di tali comunità, che la difesa reputava invece prive di una gerarchia e di un capo riconoscibile.

La Corte ha però chiarito che non è necessario una struttura rigida, essendo sufficiente un *minimum* organizzativo che può manifestarsi anche attraverso un'organizzazione a cellule, caratterizzata da adesioni progressive e da ruoli diversificati in base alle competenze[619].

In questo senso, i giudici hanno richiamato la giurisprudenza sul terrorismo islamico, non per assimilare i due fenomeni, ma per evidenziare come la giurisprudenza avesse già riconosciuto che gruppi fluidi e decentrati potessero integrare il reato associativo. Nella sentenza richiamata[620], in particolare, si affermava che la necessità di una struttura organizzativa effettiva non implicasse *ex se* il riferimento a schemi organizzativi ordinari, potendo ritenersi sufficiente modelli di aggregazione tra i sodali per l'integrazione del *minimum* organizzativo. Le strutture cellulari, proprie delle associazioni di matrice islamica, sono infatti caratterizzate da estrema flessibilità interna, in grado di rimodularsi di volta in volta in base alle esigenze, e si presentano in condizioni di operare anche contemporaneamente in più stati, in tempi diversi, con sporadicità e arruolando soggetti diversi di volta in volta. Nonostante tali caratteristiche, era stata riconosciuta comunque una struttura associativa saldamente costituita, dalle connotazioni tipiche di una "rete", in grado di mettere in relazione soggetti che condividevano un progetto comune, "catalizzatore" dell'*affectio societatis* e scopo sociale del sodalizio[621].

Pertanto, così come le cellule terroristiche – sebbene morfologicamente eterogenee –, anche le cellule illecite di Anonymous, che di per sé considerate avrebbero potuto anche perseguire delle finalità lecite, potevano dunque inquadrarsi nell'ambito di questo concetto di "rete", e non di certo nell'ambito di un'organizzazione statica.

Nel caso specifico, inoltre, l'esistenza di una struttura organizzativa si ravvisava nel complesso "di elementi strutturali, materiali e immateriali; attrezzature informatiche e patrimonio di conoscenze e competenze tecniche condivise e utilizzate per il compimento dei reati"[622].

---

[619] *Ivi*, pp. 8-9.
[620] Cass. pen., sez. V., 11 giugno 2008, n. 31389.
[621] *Ibidem*
[622] Cfr. Cass. pen.. sez. fer., 12 settembre 2013, n. 50620, rv. 258385, p. 3.

Anche sul piano soggettivo, da ultimo, la Corte ha ritenuto integrata la consapevolezza degli aderenti circa le finalità criminose: l'imputato, in particolare, aveva espresso la volontà di aderire alle iniziative del gruppo e alla sistematicità dei nuovi attacchi pianificati dal gruppo stesso[623].

4.3. Un'analisi comparativa delle comunità virtuali alla luce dell'evoluzione giurisprudenziale

Dall'analisi comparativa delle due tipologie associative sopra considerate – comunità online di pedofili e di hacktivisti - emergono differenze profonde, tali da incidere non solo sul piano fattuale, ma anche sulle giustificazioni date dalla giurisprudenza per inquadrare giuridicamente tali comunità nell'alveo dell'articolo 416 c.p.

Da un lato, infatti, vi sono le comunità pedopornografiche, che, come visto, si caratterizzano per un livello organizzativo elevato, stabile e rigido: l'accesso è sottoposto a controlli severi, la permanenza nel gruppo dipende dal rispetto di regole condivise e le funzioni dei singoli membri risultano chiaramente determinate, con una distinzione netta tra chi partecipa e chi svolge ruoli di direzione o di promozione.

Tale assetto si avvicina al modello classico di associazione per delinquere, adattato al contesto virtuale, in cui la struttura organizzativa e il programma criminoso sono definiti in modo preciso e vincolante per tutti i partecipanti.

Dall'altro lato, il quadro muta di fronte ai gruppi di hacktivisti e, nello specifico, il caso del gruppo Anonymous Italia. Nella specie, la struttura è fluida, priva di una gerarchia stabile fondata su dinamiche di riconoscimento reciproco e di leadership momentanea, spesso legata alle competenze tecniche o alla capacità di influenzare le discussioni. La figura dell'"operatore", che può certamente assumere funzioni assimilabili a quelle del promotore o dell'organizzatore, resta comunque un ruolo instabile, poiché esposto a contestazioni e ad una costante ridefinizione da parte della stessa comunità.

Quanto al programma criminoso, è possibile notare che, nei gruppi criminali dediti alla pedopornografia online, il programma risulti definito in maniera più dettagliata e costante, con regole di funzionamento note e condivise ai membri del gruppo; ciò non

[623] *Ivi*, p. 11.

vale, invece, per i gruppi di hacktivisti, dove il programma non coincide con un'attività univoca, ma si radica nella condivisione di valori ideali ed obiettivi politico sociali, perseguiti attraverso condotte penalmente rilevanti.

Da ultimo, anche il vincolo associativo si configura in maniera diversa: mentre nelle comunità pedopornografiche esso nasce da rapporti di reciprocità e dai meccanismi di scambio di informazioni e materiale illecito, negli hacktivisti il legame principale è rappresentato dal senso di appartenenza a un collettivo e dalla rivendicazione pubblica delle azioni compiute sotto il nome del collettivo stesso.

A fronte di tali differenze strutturali e teleologiche, è inevitabile, pertanto, che la giurisprudenza abbia più facilmente inquadrato le comunità pedopornografiche nei modelli tradizionali di associazioni per delinquere elaborati dalla giurisprudenza precedente e consolidata, e che, invece, sia dovuta ricorrere ad un'interpretazione più elastica ed estensiva per adattare le peculiarità del fenomeno degli hacktivisti alle categorie tipiche del diritto penale associativo.

Non a caso, dall'esame del materiale giudiziario disponibile è possibile individuare due orientamenti interpretativi distinti in materia di associazioni per delinquere operanti esclusivamente online: uno di carattere restrittivo, che ha trovato applicazione soprattutto nei casi riguardanti comunità pedopornografiche connotate da un alto livello di strutturazione; e uno estensivo, formatosi invece a partire dal caso degli hacktivisti di Anonymous Italia[624].

Questa duplicità di approcci riflette l'esigenza, da parte della giurisprudenza, di adattare le categorie del diritto penale associativo a contesti profondamente diversi da quelli tradizionali.

L'orientamento restrittivo richiama, in gran parte, i principi affermati dalla nota sentenza di Cassazione del 2004, che aveva affrontato per la prima volta la questione della qualificazione giuridica di un’associazione criminale operante interamente in rete[625].

In tale pronuncia, come visto, la Corte stabiliva che, per integrare la fattispecie di cui all'articolo 416 c.p., non fosse sufficiente la mera convergenza di più individui verso un obiettivo illecito comune, ma fosse necessario verificare la sussistenza di una struttura organizzativa caratterizzata da stabilità e dotata di specifiche modalità di funzionamento.

---

[624] Cfr. PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, cit., p. 169.
[625] Cfr. Cass. pen., sez. III, 2 dicembre 2004, n. 8296.

Tale orientamento restrittivo individuava, quindi, due requisiti aggiuntivi ritenuti essenziali per la configurabilità dell'associazione cibernetica: da un lato, la predisposizione di meccanismi di selezione degli ingressi, tali da rendere l'aggregazione criminale un gruppo chiuso ad accesso limitato; dall'altro lato, l'esistenza di regole interne concernenti la permanenza dei membri, le modalità di esclusione e le forme di contribuzione alla vita del sodalizio. Entrambi questi elementi presuppongono l'esistenza di un vertice organizzativo incaricato di predisporre e far rispettare delle regole e, dunque, una struttura di tipo gerarchico[626].

In questo modo, la giurisprudenza restrittiva aveva elevato l'asticella del requisito organizzativo ponendosi al di sopra del "minimo livello strutturale" predicato dalla giurisprudenza maggioritaria in tema di associazione per delinquere tradizionale[627].

Secondo questa linea interpretativa, anche l'elemento soggettivo del reato assumeva dei tratti peculiari, non essendo sufficiente la generica consapevolezza di contribuire a un'attività criminosa comune, ma occorrendo che i singoli membri avessero piena cognizione degli obiettivi del gruppo, cognizione che spesso veniva formalizzata al momento dell'affiliazione attraverso dei manifesti programmatici contenenti l'indicazione degli scopi, della struttura, delle regole della piattaforma.

Tale requisito soggettivo, dunque, va oltre la mera *affectio societatis* perché, richiedendo una provata e chiara comprensione del disegno criminoso, accentua il grado di colpevolezza dei partecipanti[628].

Diverso è invece l'approccio dell'orientamento estensivo, che appare più aderente al modello interpretativo "tradizionale" dell'articolo 416 c.p[629].

Anche in questo caso si riconosce la necessità di un minimo di stabilità e di organizzazione, ma non si richiede che l'associazione virtuale sia strutturata in senso gerarchico e che sia governata da un corpus di regole interne elaborate da un vertice. È sufficiente che sussista un'organizzazione rudimentale e stabile, idonea a rendere il gruppo funzionale alla commissione dei reati programmati. Anche per quanto riguarda l'elemento soggettivo l'orientamento estensivo si mostra meno rigoroso, giacché non

---

[626] *Ibidem*.
[627] Sull'organizzazione minima e rudimentale si veda Cass. pen., sez VI, 14 giugno 1995, n. 11413, Montani; in senso conforme anche Cass. pen., sez. II, 17 gennaio 2013, n. 16339, Burgio.
[628] Sull'elemento soggettivo si veda Cass. pen., sez. I, 1 febbraio 1991, n. 1332; analogamente, più di recente, Cass. pen.,sez. V, 1 dicembre 2000, n. 12525.
[629] Si veda per l'orientamento più estensivo Cass. pen., sez. fer., 12 settembre 2013, n. 50620.

ritiene necessaria l'esplicitazione formale degli scopi del funzionamento del gruppo al momento dell'ingresso, né l'esistenza di un manifesto programmatico; si ritiene sufficiente la presenza della *affectio societatis*, intesa come volontà del singolo di contribuire in modo stabile e duraturo alla realizzazione degli obiettivi perseguiti dall'associazione, anche in forma di adesione implicita alle finalità del gruppo, priva di una preventiva dichiarazione o di un atto di investitura formale[630].

La divergenza tra i due orientamenti sembra riflettere la differente base probatoria su cui essi si sono sviluppati[631]: nei casi relativi alle comunità pedopornografiche, la presenza di strutture organizzative rigide basate su regole interne ha indotto i giudici a valorizzare questi aspetti come requisiti necessari, contribuendo alla formazione l'orientamento restrittivo. Viceversa, nei procedimenti riguardanti i gruppi di hacktivisti, l'assenza di elementi così evidenti ha spinto la giurisprudenza a un'interpretazione più flessibile, incentrata su criteri minimi e meno vincolanti. In questo senso, si può parlare di un fenomeno di "*processualizzazione delle categorie sostanziali*", nel quale le caratteristiche probatorie dei singoli casi finiscono per orientare la definizione stessa della fattispecie criminosa[632].

4.4. La giurisprudenza sulle associazioni cibernetiche ibride dedite alle truffe online

Come visto, accanto alle associazioni criminali cibernetiche interamente operanti online, vi sono altre associazioni criminali, di natura ibrida, capaci di integrare dimensione digitale e dimensione fisica, tanto nella struttura quanto nelle condotte[633].

---

[630] *Ivi*, par. 1.1.: "Erano invece presenti: "affectio societatis ed esistenza di un programma teso all'attuazione di una serie indeterminata di reati, ricavabile dal substrato volontaristico destinato ad alimentare la stabile operatività dell'entità collettiva dotata di autonoma identità e destinata a persistere oltre la commissione dei reati - fine; ... attività propedeutiche e successive alle singole operazioni secondo schemi collaudati (individuazione degli obiettivi concordata a seguito di dibattiti svolti negli spazi web adibiti alle discussioni dei sodali sui temi di interesse comune; diffusione dei dati abusivamente estrapolati dai siti target su social network, canali IRC pubblici e privati, blog intestati all'associazione; pubblicazione di messaggi di rivendicazione)."

[631] Cfr. PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, cit., p. 172.

[632] *Ibidem*.

[633] Sulla natura ibrida dei gruppi di cybercriminali v. PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, cit., p. 164; United Nation Office on Drug and Crime, *Digest of cyber organized crime*, cit., p. 17; BROADHUST R.G., GRABOSKY P., CHON S., ALAZAB

Si prenderà, pertanto, in esame anche la giurisprudenza formatasi in materia, con particolare attenzione ai casi riguardanti associazioni dedite alla commissione di truffe online, al fine di comprendere come i giudici abbiano qualificato e affrontato tali fenomeni alla luce degli strumenti giuridici esistenti.

Il fenomeno delle truffe informatiche mediante tecniche di *phishing* ha trovato nella giurisprudenza italiana un primo significativo banco di prova nel procedimento penale conosciuto come "caso Poste Italiane e Banca Intesa"[634]. Tale vicenda giudiziaria ha offerto al giudice l'occasione per applicare la fattispecie dell'associazione per delinquere ad un contesto criminale caratterizzato dall'uso sistematico di strumenti informatici e telematici.

L'inchiesta, condotta dalla Procura di Milano, ha messo in luce l'esistenza di un sodalizio criminoso ben strutturato, composto da più soggetti stabilmente associati con il fine di commettere una pluralità indeterminata di truffe finalizzate all'uso indebito di carte di credito di correntisti di Poste Italiane e Banca Intesa mediante accessi abusivi ai sistemi informatici di *home banking*.

Gli imputati, muovendosi in un contesto transnazionale con base operativa anche in Romania, avevano sviluppato un sistema fraudolento e articolato in più fasi: in primo luogo, venivano predisposte e diffuse, mediante tecniche di *spamming*, email apparentemente provenienti da istituti di credito reali redatte in modo da riprodurre fedelmente i loghi, segni distintivi e modalità comunicative; tali messaggi inducevano il destinatario ignaro a collegarsi a siti web artificiosamente costruiti, i quali riproducevano quasi integralmente l'interfaccia grafica dei portali di Poste Italiane e di Banca Intesa; in tal modo, le vittime erano indotte a inserire le proprie credenziali di accesso ai servizi di *home banking*, inconsapevoli di consegnarle direttamente ai truffatori[635].

Una volta ottenuti i dati sensibili (usarname e password), il gruppo criminale li utilizzava per introdursi abusivamente negli spazi informatici riservati ai correntisti,

---

M., BOUHOURS B., *Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime*, cit., p. 9.

[634] L'associazione a delinquere dedita alle truffe informatiche: il caso "Poste Italiane e Banca Intesa" - G.I.P., Tribunale di Milano, sentenza 10 dicembre 2007, n. 888, pubblicato con il testo della decisione in *Rivista di Giurisprudenza ed Economia d'Azienda*, 4/2008; sul medesimo caso, si è espressa anche la Cassazione penale, 5 novembre 2015 n. 894; sul caso di specie, vedi anche il commento di FLOR R., *Frodi identitarie e diritto penale*, in *Penale.it*, 2008.

[635] *Ibidem*.

eseguendo operazioni di ricarica su carte prepagate; venivano altresì reclutati nuovi individui con il compito di acquistare carte prepagate delle istituzioni coinvolte, poi utilizzate per la realizzazione degli illeciti, o per aprire conti correnti per il medesimo scopo o per far circolare i profitti dei reati posti in essere. Le indagini hanno infatti rivelato un vero e proprio circuito di movimentazione dei fondi, che avveniva attraverso due canali principali: il trasferimento "da conto corrente a postepay" e quello "da postepay a postepay"[636].

La rilevanza del caso, dal punto di vista giuridico, risiede soprattutto nell'accertamento della configurabilità del reato associativo di cui all'art. 416 c.p., di cui la giurisprudenza ha ritenuto integrati tutti i requisiti.

Anzitutto, la compagine criminosa era formata da una pluralità di individui che agivano in modo coordinato e consapevole, ciascuno con compiti distinti, poiché alcuni curavano la predisposizione delle false comunicazioni, altri gestivano i siti clonati, altri ancora si occupavano delle movimentazioni finanziarie. Il carattere continuativo e duraturo del vincolo associativo è stato desunto, poi, dalla reiterazione delle condotte e dalla stabile predisposizione di strumenti tecnici idonei alla realizzazione delle truffe: il gruppo, infatti, non agiva in modo sporadico, bensì aveva costituito un vero e proprio "arsenale telematico", comprensivo di server, domini web e caselle di posta elettronica appositamente creati per la raccolta delle credenziali[637].

Un ulteriore profilo di rilievo era poi rappresentato dalla dimensione transnazionale del fenomeno. Le indagini hanno accertato che una parte significativa della pianificazione e della predisposizione delle attività fraudolente avveniva in Romania, con collegamenti stabili tra i membri dislocati in Italia e quelli operanti all'estero[638].

Accanto al reato associativo, il Gip ha poi confermato la configurabilità di una pluralità di reati fine: la truffa ex art. 640 c.p., quale esito degli artifici e raggiri posti in essere per indurre le vittime a consegnare inconsapevolmente le proprie credenziali; l'accesso abusivo a sistemi informatici ex art. 615-*ter* c.p., realizzato attraverso l'introduzione negli spazi riservati dei correntisti; l'utilizzo indebito di carte di credito e di pagamento ex art. 12 L. 197/1991, concretizzatosi nelle operazioni di ricarica fraudolente; la falsificazione

[636] *Ibidem*.
[637] *Ibidem*.
[638] *Ibidem*.

del contenuto di comunicazioni informatiche ex art. 617-*sexies* c.p., in relazione alla predisposizione di e-mail ingannevoli.

Sulla stessa scia, si ritiene utile analizzare, infine, un'ulteriore pronuncia della giurisprudenza di legittimità, che ha avuto il pregio di consolidare ulteriormente i criteri distintivi tra concorso di persone nel reato e associazione per delinquere, applicati al fenomeno delle truffe online[639].

La vicenda giudiziaria riguardava un gruppo di soggetti dediti in maniera stabile e coordinata alla commissione di frodi informatiche mediante l'uso di conti correnti e carte di credito intestati a prestanome, con attività di adescamento delle vittime attraverso annunci ingannevoli.

Nella specie, la Corte ha sottolineato come la fattispecie di cui all'art. 416 c.p. non si esaurisse nella mera collaborazione estemporanea alla realizzazione di un reato, bensì richiedesse un *quid pluris* rappresentato dall'"attuazione di un più vasto programma criminoso, per la commissione di una serie indeterminata di delitti, con la permanenza di un vincolo associativo tra i partecipanti, anche indipendentemente ed al di fuori dell'effettiva commissione dei singoli reati programmati"[640].

È proprio questa la linea di demarcazione rispetto al concorso di persone nel quale l'accordo criminoso e occasionale è circoscritto ad uno o più reati di determinati.

In questo caso, dalle risultanze processuali, è emerso con chiarezza che il sodalizio oggetto di giudizio possedeva una struttura stabile con una precisa ripartizione dei compiti per ciascuno dei singoli componenti. Ciò implicava, dunque, che i partecipanti non agivano in modo intercambiabile o casuale, ma all'interno di un assetto funzionale predeterminato, volto a garantire l'efficienza del programma criminoso e la replicabilità delle condotte fraudolente.

In particolare, la Corte descriveva l'esistenza di più livelli operativi.

A livello esecutivo di base figuravano soggetti individuati "tramite intermediari, di soggetti ai margini della società che per poche decine di euro si prestavano a fungere da prestanome per aprire conti correnti utilizzati per le azioni delittuose"[641]. Questi individui, facilmente sostituibili e reclutati in ragione della loro marginalità socioeconomica,

[639] Cass. pen., sez. II, 28 aprile 2023, n. 17945.
[640] *Ivi*, par. 3.
[641] *Ivi*, par. 5.

fornivano lo strumento indispensabile per la movimentazione dei capitali illeciti, pur senza accedere direttamente ai profitti principali.

Un secondo gruppo si occupava invece di attività intermedie, come "la pubblicazione degli annunci, la tenuta dei rapporti telefonici con le vittime, [e] il procacciamento dei prestanome"[642]; compiti che richiedevano un contatto diretto con il pubblico e la capacità di rendere credibili le comunicazioni ingannevoli, nonché di ampliare la rete di complici utilizzati per l'intestazione dei conti correnti.

Infine, a livello apicale, la gestione dei proventi e delle carte di credito era concentrata nelle mani dei capi che, secondo la Corte, erano "detentori delle carte di credito [e ai quali] andavano i ricavi dell'attività criminosa"[643]; questi ultimi avevano il controllo delle risorse economiche e gestivano il sodalizio.

La distribuzione dei compiti non solo garantiva la funzionalità del sodalizio, ma permetteva altresì di ridurre i rischi individuali: i prestanome esponevano la propria identità senza avere accesso ai guadagni, mentre i vertici beneficiavano dei profitti senza apparire direttamente in attività rischiose.

La Corte ha inoltre sottolineato la dimensione pluriennale del vincolo associativo: "la permanenza pluriennale del vincolo associativo perlomeno tra gli artefici principali e la predisposizione degli strumenti finalizzati alla ripetizione di schemi criminosi, rimasti immutati nel corso del tempo, fossero diretta espressione del vincolo associativo e non il frutto di un'unione meramente occasionale"[644]. La proiezione temporale dell'accordo criminoso consentiva, dunque, di distinguere l'associazione dal mero concorso, per il quale l'intesa è episodica e si esaurisce con il singolo fatto, mentre nel 416 c.p. l'accordo è "diretto all'attuazione di un più vasto programma criminoso […] per la commissione di una serie indeterminata di delitti, con la permanenza di un vincolo associativo tra i partecipanti"[645]. In tal senso, anche sotto il profilo temporale, l'elemento organizzativo assumeva rilievo sintomatico: la replicazione di identiche modalità di adescamento, la costante canalizzazione dei proventi su conti e carte riconducibili al gruppo, e la continuità delle condotte per un arco di tempo significativo deponevano per la permanenza del sodalizio e non per una compagine estemporanea.

---

[642] *Ibidem*.
[643] *Ibidem*.
[644] *Ibidem*.
[645] *Ibidem*.

5. Conclusioni

L'indagine sviluppata nel corso di questo lavoro consente di trarre alcune considerazioni generali circa l'adeguatezza del concetto tradizionale di criminalità organizzata rispetto al fenomeno della criminalità cibernetica.

È emerso con chiarezza come il trasferimento di tale categoria al contesto digitale non offre sempre risposte soddisfacenti, ma finisce per acuire problemi definitori già presenti nella letteratura criminologica e giuridica.

La nozione di criminalità organizzata, storicamente segnata da una pluralità di significati, si rivela ampia e mutevole per descrivere in modo rigoroso la complessità delle pratiche criminali online. Chiedersi se i gruppi attivi nel cyberspazio siano meno riconducibili alla criminalità organizzata significherebbe restare intrappolati in un dibattito sterile incapace di orientare in modo efficace l'azione di ricerca e di contrasto.

Come visto, si evidenziano notevoli differenze tra i fenomeni analizzati: forum dediti alla diffusione di materiale pedopornografico, gruppi specializzati nel phishing, imprese illegali di streaming, collettivi hacktivisti, Sono tutte realtà eterogenee, non solo nelle finalità perseguite, ma anche nelle forme organizzative, nelle modalità operative, nelle vittime colpite, nella pericolosità sociale.

Sul piano giuridico, la giurisprudenza ha mostrato consapevolezza di tali differenze, elaborando soluzioni che rappresentano un tentativo di adattamento del reato associativo al contesto digitale.

Si è assistito alla definizione di una variante cibernetica dell'associazione per delinquere, nella quale il requisito organizzativo è stato ristretto a forme chiuse, con regole di accesso e selezioni rigorose. Al contempo, è stato adattato anche a configurazioni criminali che, seppur non dotate della medesima stabilità e rigidità strutturale, venivano ritenute altrettanto dannose.

Potrebbe pertanto ipotizzarsi il superamento di un'idea unica ed omnicomprensiva di criminalità organizzata a favore dell'elaborazione di una pluralità di sottocategorie capaci di rappresentare meglio la varietà dei fenomeni. In questo modo si consentirebbe di distinguere meglio tra forme chiuse e gerarchiche, realtà imprenditoriali orientate al profitto, e collettivi politico protestatari, riconoscendo per ciascuna configurazione il tipo

di minaccia prodotta e il livello di pericolosità sociale. Ciò consentirebbe, altresì, di calibrare gli strumenti giuridici ed investigativi in modo mirato, evitando, da un lato, un'eccessiva risposta punitiva e, dall'altro, una sottovalutazione di nuove forme di criminalità emergenti.

Non si tratta di una soluzione meramente classificatoria, ma di un vero e proprio cambio di prospettiva che, per inquadrare un fenomeno nell'ambito della criminalità organizzata, parte dall'analisi delle sue caratteristiche concrete e dei suoi effetti sul piano sociale ed economico.

In quest'ottica, diventa centrale il ricorso a parametri quali il danno, il rischio e la minaccia. Tali indicatori consentono di valutare l'impatto effettivo dei fenomeni criminali, indipendentemente dalla loro forma organizzativa. La pericolosità non sarà più legata esclusivamente alla capacità di strutturarsi stabilmente, ma anche alla possibilità di arrecare danni significativi; in questo modo, la centralità del fattore organizzativo viene ridimensionata, mentre emergono nuovi criteri di valutazione maggiormente aderenti alla realtà contemporanea.

Parallelamente appare indispensabile ampliare l'orizzonte delle politiche di contrasto oltre i confini tradizionali del diritto penale. Il cyberspazio richiede interventi più ampi, capaci di combinare prevenzione e governance delle infrastrutture digitali.

Le riflessioni condotte conducono a una conclusione chiara: il futuro della lotta al *cybercrime* non sta nell'estendere o aggiornare in maniera meramente formale categorie ereditate dal ‘900, ma nel ripensare in profondità gli strumenti analitici e istituzionali disponibili. Occorre definire sottocategorie precise, basare l'analisi su metriche di danno e di minaccia, calibrare le soglie probatorie e costruire un arsenale di strumenti adeguati, non solo di natura repressiva, ma anche preventiva.

CONCLUSIONI

A chiusura dell'analisi sistematica, di tipo sociologico e giuridico, delle due principali categorie di fenomeni criminali organizzati, è possibile ora delineare un quadro articolato.

Da un lato, la criminalità organizzata di matrice "tradizionale", che ha progressivamente adattato le proprie strategie operative al contesto digitale, trasferendo nel cyberspazio logiche, strutture e finalità consolidate nei mercati illeciti fisici.

Dall'altro lato, la criminalità propriamente "cibernetica", che origina e si sviluppa esclusivamente all'interno della dimensione digitale, priva di un legame diretto con forme associative preesistenti nel mondo materiale e caratterizzata da dinamiche più fluide, reticolari e globalizzate.

In primo luogo, la presente ricerca ha indagato in profondità il processo di progressivo adattamento della criminalità organizzata tradizionale alle tecnologie e allo spazio digitale, mettendo in evidenza come tale specifico fenomeno non abbia determinato un mutamento di fini o di obiettivi strategici delle associazioni criminali, bensì una metamorfosi degli strumenti impiegati per il loro perseguimento. Come visto, le organizzazioni criminali tradizionali non hanno modificato la propria essenza: continuano a perseguire il profitto, il controllo territoriale, l'infiltrazione nell'economia e nella politica. Ciò che è cambiato, semmai, è il terreno operativo, la dimensione spazio-temporale e la modalità di esercizio del potere criminale.

In questo senso, si può sostenere che la criminalità organizzata si sia progressivamente adattata alle logiche di un mondo globalizzato, smaterializzato e tecnologicamente avanzato, sfruttando ogni nuova vulnerabilità generata dall'evoluzione digitale. Tale adattamento è stato reso possibile da una caratteristica peculiare delle organizzazioni criminali e, in particolare, delle mafie: la capacità di ibridarsi con contesti sociali, economici e politici mutevoli, senza rinunciare al proprio DNA originario, ma rafforzandolo attraverso la conquista di nuovi spazi.

Come visto, oggi le organizzazioni criminali tradizionali si muovono con disinvoltura tanto nel mercato della droga quanto in quello dei dati digitali, tanto nel riciclaggio tradizionale, quanto nel *cyberlaundering*. La discontinuità rispetto al passato dei mezzi impiegati dalle organizzazioni criminali moderne non deve indurre a concepire la criminalità digitale come entità autonoma e del tutto nuova. Il "vecchio" e il "nuovo"

convivono e si intrecciano, dando vita a una realtà complessa in cui la materialità delle condotte si intreccia con l'immaterialità delle reti digitali.

L'analisi svolta ha mostrato come il diritto processuale penale si trovi dinanzi a una crisi profonda. Le categorie probatorie concepite in epoche precedenti risultano sempre più inadatte a governare fenomeni criminali caratterizzati da volatilità, replicabilità e transnazionalità del dato digitale.

Se da un lato, la prova digitale entra in tensione con le tecniche tradizionali di acquisizione della prova come intercettazioni, sequestri e accertamenti tecnici; dall'altro lato, l'impiego di tecniche come trojan, perquisizioni da remoto, decriptazioni forensi di dati, oltre a non poter essere facilmente compresse entro le rigide e tradizionali categorie probatorie, sollevano perplessità in ordine alla compatibilità con i diritti fondamentali. Da qui discende il rischio del fenomeno della "*tirannia delle categorie desuete*", che non solo ostacola l'efficacia investigativa, ma mina anche le garanzie del giusto processo.

Il rischio è duplice: da un lato, l'uso di strumenti investigativi innovativi rischia di espandersi in assenza di cornici legali chiare, con potenziale compromissione dei diritti fondamentali; dall'altro, l'assenza di tipizzazione normativa rende le prove raccolte vulnerabili a contestazioni di legittimità e incertezza sulla loro utilizzabilità processuale.

Pertanto, un profilo di primaria rilevanza emerso nel corso dell'indagine concerne l'esigenza di un'armonizzazione sovranazionale in materia di acquisizione e circolazione della prova digitale.

L'ordine europeo di indagine, pur rappresentando uno strumento non trascurabile nel percorso di rafforzamento della cooperazione giudiziaria, si rivela tuttavia inadeguato, in quanto ancorato a un principio di mutuo riconoscimento di natura meramente formale, incapace di assicurare che le concrete modalità di acquisizione della prova siano sempre conformi ai canoni del giusto processo previsti dai singoli Stati.

L'orizzonte evolutivo non potrà che orientarsi verso l'elaborazione di uno *ius commune* europeo della prova digitale, capace di contemperare le esigenze di efficienza investigativa con la tutela sostanziale dei diritti fondamentali. Segnatamente, ciò implica, pertanto, la predisposizione di regole comuni in ordine alla catena di custodia di dati, alla tracciabilità delle operazioni di decrittazione, alla conservazione dei dati originari e alle garanzie difensive nelle fasi irripetibili dell'attività probatoria.

La fiducia reciproca tra gli Stati membri non potrà basarsi su meccanismi procedurali automatici, bensì deve fondarsi su presupposti sostanziali e principi condivisi: solo in questo modo, sarà possibile scongiurare il rischio che la cooperazione giudiziaria si traduca in un sistema di "mutua deresponsabilizzazione", nel quale ciascun ordinamento abdichi al proprio controllo di legittimità costituzionale confidando in garanzie altrui mai concretamente verificate.

Il fenomeno dei crypto-asset si impone come una delle innovazioni tecnologiche a più elevato potenziale criminogeno del nuovo millennio. La loro configurazione intrinsecamente decentralizzata, pseudonima e transnazionale li rende strumenti di straordinaria efficacia per finalità illecite, come il riciclaggio di capitali, il finanziamento del terrorismo, la veicolazione di transazioni criminali.

L'Unione europea, come visto, ha intrapreso un percorso regolatorio di indubbio rilievo, volto a introdurre obblighi di autorizzazione, trasparenza e tracciabilità in materia di transazioni crypto.

Nondimeno, permangono significative criticità, imputabili, da un lato, all'eterogeneità applicativa delle discipline interne, dall'altro, a rischio di arbitraggio regolamentare e, più in generale, alla perdurante assenza di un quadro organico di cooperazione internazionale. In tale prospettiva, appare imprescindibile la definizione di un trattato multilaterale in materia di *cyberlaundering*, capace di uniformare gli standard probatori, di disciplinare in modo uniforme gli obblighi gravanti sugli intermediari e di rafforzare i meccanismi di cooperazione giudiziaria transnazionale.

Sul piano penalistico, il legislatore è chiamato ad una scelta dirimente: introdurre nuove figure incriminatrici specificamente destinate ai c.d. cripto-reati, oppure estendere in via ermeneutica le fattispecie incriminatrici già vigenti (riciclaggio, autoriciclaggio, truffa).

La prima soluzione garantirebbe maggiore determinatezza normativa, ma rischierebbe di produrre una proliferazione di disposizioni iper-specialistiche, suscettibili di rapida obsolescenza; la seconda soluzione, più flessibile, esporrebbe però al pericolo di interpretazioni giurisprudenziali eccessivamente creative, con conseguenti margini di incertezza applicativa.

In ogni caso, non appare ulteriormente differibile l'elaborazione di una disciplina puntuale relativa alle misure ablative concernenti wallet digitali o alla responsabilità penale degli intermediari.

Si è rilevato, inoltre, come il contrasto ai cripto reati e, più in generale, alla criminalità digitale, richiedano non soltanto un adeguato apparato normativo, ma anche strumenti investigativi tecnologicamente avanzati e competenze professionali altamente specializzate.

Tecniche come l'analisi delle blockchain, la deanonimizzazione dei wallet, l'infiltrazione nei marketplace del dark web e l'utilizzo controllato di fondi virtuali, si rivelano imprescindibili, ma necessitano di essere rigorosamente inquadrate entro procedure giuridiche rispettose dei principi del giusto processo.

Parimenti essenziale risulta la costituzione di unità investigative dedicate, l'impiego di strumenti di intelligenza artificiale di tipo predittivo per il riconoscimento di pattern e il consolidamento della cooperazione con *exchangers* regolamentati, soprattutto se si concepisce l'investigazione digitale, non solo quale strumento repressivo, ma anche quale presidio preventivo, idoneo ad anticipare le condotte criminali attraverso l'analisi predittiva di dati e la tempestiva individuazione di operazioni sospette.

In conclusione, per il contrasto di un crimine organizzato sempre più digitale, emerge con evidenza che il legislatore e gli operatori del diritto non possono più limitarsi a interventi frammentari o di natura emergenziale, ma devono orientare la propria azione verso una riforma organica, capace di affrontare in chiave sistematica la sfida posta dalla criminalità organizzata digitale.

Ciò è possibile, in primo luogo, attraverso una compiuta sistemazione normativa che tipizzi in maniera chiara e tassativa le tecniche investigative digitali e, parallelamente, tramite la costruzione di uno *ius commune*, fondato su regole sostanziali condivise e su standard comuni di legalità e proporzionalità. Quest'ultimo processo non può però circoscriversi all'ordinamento unionale, poiché la dimensione globale del fenomeno criminale esige il rafforzamento della cooperazione internazionale, al fine di superare le zone grigie giurisdizionali e di impedire che gli spazi normativi più deboli si trasformino in rifugi sicuri per le organizzazioni criminali.

Volgendo ora l'attenzione alla disamina sul crimine organizzato cibernetico, è opportuno restituire una riflessione conclusiva che tenga insieme le molteplici sfaccettature emerse dall'analisi dottrinale, giurisprudenziale e criminologica.

Il percorso d'indagine intrapreso ha messo in evidenza non soltanto l'assenza di una definizione condivisa e cristallizzata di "*cyber organised crime*", ma soprattutto l'esigenza di un approccio critico che sappia bilanciare le narrazioni securitarie, le categorie giuridiche tradizionali e le nuove dinamiche sociali generate dall'avvento della tecnologia digitale.

Una prima considerazione imprescindibile riguarda la problematicità della definizione dell'etichetta di "*organised crime*". Come visto, non si tratta solo di difficoltà puramente semantiche, ma vanno valutati altresì gli effetti concreti che tale etichetta riverbera nella costruzione dell'agenda politica, nell'allocazione delle risorse investigative e nella stessa configurazione giuridica del fenomeno. Peraltro, il rischio di impiegare in maniera eccessivamente estensiva la categoria di crimine organizzato, piegandola alle esigenze contingenti del cyberspazio, è quello di alimentare un paradigma inflazionato, svuotato del proprio potere analitico e incapace di cogliere la specificità delle nuove minacce. In altre parole, l'etichetta di "organizzato" rischia di assumere una funzione prevalentemente retorica, più utile a legittimare misure straordinarie di controllo che a favorire una reale comprensione del fenomeno.

In secondo luogo, lo studio ha messo in luce la tensione tra continuità e discontinuità rispetto al paradigma tradizionale dell'associazione per delinquere. S

e, da un lato, il cyberspazio sembra aver reso più agevole l'accertamento probatorio – si pensi alla pubblicizzazione delle regole interne di taluni sodalizi criminali digitali, che rappresentano una sorta di "statuto costitutivo" del gruppo – dall'altro lato, la fluidità delle relazioni online e l'assenza di confini tangibili pongono sfide inedite al requisito organizzativo della fattispecie.

La giurisprudenza, come dimostrato da recenti pronunce, ha scelto di reagire introducendo un'interpretazione restrittiva: soltanto i gruppi chiusi, dotati di stringenti meccanismi di selezione degli ingressi, possono integrare gli estremi dell'associazione criminale. Ciò ha comportato un rovesciamento rispetto alla tendenza espansiva che aveva caratterizzato l'evoluzione della norma nel corso del Novecento, restituendo centralità alla tutela delle garanzie individuali rispetto alle istanze di difesa sociale.

Tale inversione di rotta appare significativa sotto due profili: da un lato, essa dimostra come il diritto non sia impermeabile al mutamento tecnologico e sociale, ma anzi sia costretto a ricalibrare le proprie categorie alla luce delle nuove forme di criminalità; dall'altro lato, segnala la consapevolezza della magistratura circa i rischi insiti in un'applicazione indiscriminata della fattispecie associativa, che nel contesto immateriale della rete potrebbe tradursi in un pericoloso strumento di criminalizzazione del dissenso politico o di altre forme di aggregazione sociale prive di reale pericolosità.

Parallelamente, la letteratura criminologica invita a considerare che le tradizionali categorie di gravità e organizzazione non siano più sufficienti per qualificare i crimini informatici.

Nel cyberspazio, infatti, singoli individui o reti informali possono produrre danni sistemici e minacce all'ordine sociale paragonabili a quelli derivanti dai gruppi criminali strutturati. Ciò impone di abbandonare l'"organizzazione" come indicatore proxy di pericolosità, privilegiando invece un'analisi incentrata sui danni effettivi, sui rischi e sulle conseguenze sociali delle condotte.

In questa prospettiva, lo sviluppo teorico futuro dovrà concentrarsi sulla costruzione di metriche capaci di misurare l'impatto delle condotte criminali digitali, anziché limitarsi a ricondurle forzosamente all'interno di categorie preesistenti.

Un altro nodo emerso con chiarezza riguarda la relazione circolare tra politiche di sicurezza, produzione normativa e costruzione sociale delle minacce. La cristallizzazione della narrativa sul cyber-OC, se non costantemente problematizzata, rischia di produrre un diritto penale d'emergenza fondato su presupposti più ideologici che empirici. Applicare questo modello al contesto cibernetico comporterebbe il pericolo di trasformare ogni reato informatico in una minaccia alla sicurezza nazionale, con conseguenze sproporzionate in termini di repressione e distribuzione delle risorse.

Tali considerazioni portano ad affermare la necessità di un approccio multilivello e multidisciplinare. Le scienze sociali, la criminologia e il diritto sono chiamati a dialogare costantemente, evitando il rischio di ridurre la complessità del fenomeno a un unico registro interpretativo. In particolare, la riflessione sociologica aiuta a comprendere la dimensione relazionale del cyberspazio, inteso non come "mondo virtuale" separato, bensì come arena di interazione sociale in cui emergono comunità, legami deboli e forti, e talvolta forme di appartenenza collettiva. La giurisprudenza, a sua volta, ha dimostrato

di interiorizzare progressivamente questa visione, riconoscendo che la dimensione digitale non rappresenta un ostacolo alla formazione di sodalizi criminali, bensì un contesto privilegiato che favorisce cooperazione e anonimato.

Alla luce di quanto emerso, è possibile formulare alcune considerazioni conclusive di carattere propositivo.

Sul piano teorico, è necessario ripensare le categorie criminologiche tradizionali, evitando sia la tentazione di una semplice trasposizione nel contesto digitale, sia il rischio di elaborare nuove definizioni prive di rigore concettuale. Occorre piuttosto costruire un quadro analitico capace di cogliere la specificità delle minacce online, distinguendo tra fenomeni organizzati e fenomeni destrutturati ma altamente dannosi.

Sul piano giuridico, la sfida principale è quella di mantenere un equilibrio tra esigenze di difesa sociale e tutela delle garanzie individuali. La restrizione interpretativa introdotta dalla magistratura in relazione al requisito organizzativo va letta come un tentativo di tracciare confini più netti, in un contesto in cui la fluidità delle relazioni digitali rischia di dilatare eccessivamente il campo di applicazione della fattispecie.

Tuttavia, tale soluzione non può essere considerata definitiva: occorre interrogarsi su eventuali riforme legislative che, senza snaturare la logica della norma, sappiano adattarla in modo più coerente alle peculiarità del cyberspazio.

Sul piano politico-criminale, infine, appare urgente una riflessione sulla costruzione narrativa del cyber-OC. La lotta alla criminalità organizzata cibernetica richiede strumenti efficaci, ma questi non possono fondarsi su presupposti vaghi o retorici. Una politica criminale sostenibile deve basarsi su evidenze empiriche solide, su un'attenta valutazione dei costi e dei benefici delle misure repressive e su una chiara distinzione tra minacce alla sicurezza nazionale e crimini informatici di minore entità.

In conclusione, la ricerca condotta mostra come il crimine organizzato cibernetico non possa essere compreso né efficacemente contrastato mediante la mera trasposizione di categorie pensate per il mondo fisico.

Il mutamento tecnologico e sociale ha generato un fenomeno ambivalente: da un lato, ha favorito l'emergere di nuove forme associative che rispecchiano in maniera quasi paradigmatica i requisiti della fattispecie astratta; dall'altro lato, ha imposto una riformulazione del concetto stesso di organizzazione criminale, in un'ottica più restrittiva e garantista. Le scienze giuridiche e sociali sono dunque chiamate a un compito comune:

interrogarsi criticamente sul valore euristico delle definizioni, evitare la cristallizzazione di narrazioni inflazionate e costruire strumenti concettuali e normativi in grado di leggere la criminalità organizzata nel cyberspazio senza sacrificare la complessità della realtà.

La sfida per il futuro sarà quella di sviluppare un modello interpretativo e operativo che, senza cedere a semplificazioni riduttive, sappia integrare la dimensione empirica, teorica e normativa del fenomeno. Solo così sarà possibile preservare l'equilibrio tra sicurezza collettiva e diritti individuali, evitando che il cyberspazio diventi terreno di sperimentazione di nuove forme di diritto penale simbolico o d'emergenza. È in questo senso che la riflessione sul cyber-OC non rappresenta soltanto un esercizio di aggiornamento terminologico, ma un banco di prova fondamentale per la capacità delle nostre società di coniugare innovazione tecnologica, giustizia e libertà.

BIBLIOGRAFIA

FONTI DOTTRINALI

AHMED W. ET AL., *Whatsapp network Forensics: discovering the IP addresses of suspects, in International Conference of new technologies*, 2021.

ALBANESE J., *Cybercrime as an Essential Element in Transnational Counterfeiting Schemes. Presentation at International Academic Conference: Linking Organized Crime and Cybercrime*, UNODC, 2018.

ALBRECHT C. ET AL., *The use of cryptocurrencies in the money laundering process*, in *Journal of Money Laundering Control*, 22, 2, 2019.

ALDRIDGE, J., DÈCARY-HÈTU, D.,*Cryptomarkets and the future of illicit drug markets. In the internet and drug markets* (pp. 23–30), EMCDDA, Publication Office of the European Union, 2016.

ALEXANDROU A., *Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security*, *Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices*, CRC Press, 2022.

ANSALONE G., *Cyberspazio e nuove sfide*, in *GNOSIS – Rivista italiana di intelligence*, 3, 2012.

ANTOLISEI F., *Manuale di diritto penale*, *Parte Speciale*, vol. II, XVI ed., 2016.

BARRATT M.J., *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*, UK Palgrave pivot, 2014.

BASSOLI E., *I crimini informatici, il dark web e le web room*, Pacini giuridica, 2021.

BENJAMIN V., ZHANG B., NUNAMAKER JR., CHEN H., *Examining Hacker ParticipationLength in Cybercriminal Internet-Relay-Chat Communities*, in *Journal of Management Information Systems*, 2016, vol. 33, Is.2 (DOI: 10.1080/07421222.2016.1205918).

BERTOLA F., *Drug Trafficking on Darkmarkets: How Cryptomarkets are changing drug global trade and the role of organized crime,* in *American Journal of Qualitative Research*, 4, 2, 2020.

BETTINELLI E., *Società digitale/società della conoscenza: per una ulteriore analisi, tra progresso e crisi*, in *Studi di Sociologia*, 3, 2022.

BIRK D., GAJEK S., GROBART F., SADEGHI A., *Phishing Phishers: observing and tracing Organized cybercrime*, in Second International Conference on Internet Monitoring and Protection, 2007.

BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. inf*., 1, 2017.

BRAGHÒ G., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in LUPARIA L., (a cura di) *Sistema penale e criminalità informatica*, Milano, 2009, 196.

BRENNER S. W., *Organized Cybercrime? How Cyberspace may affect the structure of criminal relationships,* in *North Carolina Journal of Law & Technology*, 4, 1, 2002.

BROADHURST R., GRABOSKY P., ALAZAB M., CHON S., *Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime*, in *International Journal of Cyber Criminology*, 2014, 8, 1, pp. 1-20; MARAS M., *Cybercriminology*, Oxford University Press, 2016.

BUSSOLATI N., *L'associazione per delinquere "informatica",* in AA. VV., Cybercrime, (a cura di) CADOPPI, CANESTRARI, MANNA, PAPA, 2019, UTET Giuridica.

CALAFOS M.W., DIMITOGLOU G., *Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency*, in *Principles and Practice of Blockchain*, a cura di Daimi K., Dionysiou I., El Madhoun N., 2022.

CALDWELL M., ANDREWS J. T. A., TANAY T., GRIFN L. D., *AI-enabled future crime*, in *Crime Science*, 2020.

CALEMME C., *Criptovalute e diritto penale: progresso tecnologico, limiti normativi, linee di riforma*, Insubria, 2024.

CAMPBELL-VERDUYN, *Bitcoin and beyond: cryptocurrencies, blockchains and global governance*, Routledge, 2018.

CAMPLANI F., *Locus commissi delicti, norme di collegamento e reati informatici a soggetto passivo indeterminato*, in *Archivio Penale*, 2. 2020.

CARBONE M., *Riflessioni sul contrasto al riciclaggio nel contest di un'economia che cambia*, in *Rivista della Guardia di Finanza*, 1, 2025.

CARBONE M., *Follow the money a trent'anni dall'uccisione di Giovanni Falcone. Le indagini finanziarie e patrimoniali 3.0*, in *Rivista della Guardia di Finanza*, supplemento al n. 1-2022.

CARNEVALE S., FORLATI S., GIOLO O., *The Notion of Organised Crime: Why Definitions Matter*, in *Redefining Organised Crime: A Challenge for the European Union?*, Oxford, Hart Publishing, 2017.

CASTELLS M., *The Internet galaxy: Reflections on the Internet, business and society*, Oxford University Press, Oxford, 2001.

CATINO M., *Mafia Organizations, The Visible Hand of Criminal Enterprise*, Cambridge University Press, 2019.

CAVALIERE A., *I reati associativi tra teoria, prassi e prospettive di riforma*, in FIANDACA G., VISCONTI C. (a cura di), *Scenari di mafia. Orizzonte criminologico e innovazioni normative*, Giappichelli, 2010.

CONFENTE L., *Intelligenza artificiale e investigazioni. La tecnologia come strumento nella lotta alla mafia*, Corso di Dottorato in Studi sulla criminalità organizzata, Unimi, 2024.

CONSULICH F., *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali, in Diritto penale e processo,* 2, 2022.

CHAWKI M., *The Dark Web and the future of illicit drug markets*, in *Journal of Transportation Security*, 2022.

CHILDS A., BERNOT A., *The platformisation of illicit drug markets: How datafication, technological affordances, and platform-mediated labour practices shape illicit drug markets*, in *Crime, Media, Culture, an International journal,* 21, 2, 2024.

CHOO K.R., SMITH R.G., *Criminal Exploitation of Online Systems by Organised Crime Groups,* in *Asian Criminology*, 3, 2008.

CHOO K. R., *Organised crime groups in cyberspace a typology,* in *Trends in Organised crime*, 2008.

CONSULICH F., *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali, in Diritto penale e processo,* 2, 2022.

CROCE M., *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy*, in *Sistema penale*, 4, 2021.

CROSS S., HIRRLE S., LIM M.A., *Cybercrime Strategy Guidebook,* Interpol, 2021.

CURTOTTI D., RIZZI V., NOCERINO W., RUSSITTO A., GILIBERTI G., SCARPA G., *Piattaforme criptate e prova penale*, in *Sistema penale*, 6, 2023.

DAMAP N.Y., MAZA K. D., *Jurisdictional Challenges in Cryptocurrency Disputes: Navigating the Legal Maze of a Borderless Technology*, in *African Journal of stability and development*, 17, 1, 2025.

DANIELE M., *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/ Encrochat in attesa delle Sezioni Unite*, in *Sistema Penale*, 2023.

DANIELE M., *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*, in *Sistema penale*, 2024.

DANIELE M., *La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge*, in *Processo penale e giustizia*, 5, 2018.

DELLA RAGIONE L., *D.Lgs. 203/2023: l'Italia si adegua alla normativa europea in tema di congelamento e confisca*, in *Il Quotidiano Giuridico*, *Rivista on line*, 2024.

DELL'OSSO A., *Riciclaggio di proventi illeciti e Sistema penale*, in *Itinerari di diritto penale*, collana diretta Dolcini E., Fiandaca G., Musco E., Padovani T., Palazzo F., Sgubbi F., Giappichelli Editore, Torino, 2017.

DE FRANCESCO G., *Associazione per delinquere e associazione di tipo mafioso*, in *Digesto penale*, I, Torino, 1987.

DE FRANCESCO G., *Dogmatica e Politica criminale nei rapporti tra concorso di persone ed interventi normativi contro il crimine organizzato*, in *RIDPP*, 1994.

DE FRANCESCO G., *Gli articoli 416, 416-bis, 416-ter, 417, 418 c.p.,* in *Mafia e criminalità organizzata*, I, Torino, 1995, p. 34.

DEMETIS D., *Organised crime The Cyber dimension*, in *A research agenda for organized crime* edito a cura di Barry Rider, 2023.

DI LERNIA A., *Crowdfounding @ ICOs: esigenze di prevenzione del rischio di commissione di reati nell'era della digital economy,* in *Diritto penale contemporaneo*, 2, 2019.

DI NICOLA A., *Towards digital organized crime and digital sociology of organized crime*, in *Trends in Organized Crime*, 2022.

DIOTALLEVI G., *Riciclaggio, autoriciclaggio (...ed altro ancora) nel tempo della moneta virtuale e della cybersicurezza)*, in *Questione Giustizia*, 2024.

DI PAOLO E., *Cyber crime. Il Phishing: prospettive di un delitto*, in Archivio penale, 2, 2017.

DITTRICH D., HIMMA K.E., *Hackers, Crackers, and Computer Criminals*, in *Handbook of Information Security, Information Warfare, Social, Legal, and and International Issues and Security Foundations*, edito da Bidgoli H., 2, 2006.

DI VIZIO F., *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, in *Diritto penale contemporaneo*, 10, 2018.

DOBRIINOIU M., *Proposals for a broader approach of misuse of devices and programs' provision in combating cyber-dependent and cyber-enabled crimes*, in *Lex et Scientia International Journal*, XXXI, 1, 2024.

DUMITRACHE A., MODIGA G., *New trends and perspectives in the money laundering process, in Challenges of the Knowledge Society*, 1, 2011.

DUNCAN P., LORD N., *Organized crime money laundering through online gambling businesses in Great Britain*, in The Private Sector and Organized Crime, Ed. ZABYELINA Y., THACHUK K, Routledge, London, New York.

ERTOLA F., *L'ordine europeo di indagine penale,* in *Trattato di Procedura penale*, XLIV.3, diretto da Ubertis G. e Voena G.P., Giuffrè, 2025.

FIANDACA G., *Il «bene giuridico» come problema teorico e come criterio di politica criminale, in Riv. it. dir. proc. e pen.*, 1, 1982.

FIANDACA G., *Criminalità organizzata e controllo penale*, in *Indice penale*, 1991.

FIANDACA G., MUSCO E., *Diritto penale, Parte Speciale*, vol. I, IV ed., Bologna, Zanichelli, 2012.

FILIPPI L., *Criptofonini SKY- ECC e messaggi criptati: la Corte di cassazione attua i principi di diritto enunciati dalle Sezioni Unite*, in *Penale Diritto e Procedura*, 11 aprile 2024.

FIORE C., voce *Ordine Pubblico (penale*), in Enc. Dir., Vol. XXX, 1980.

FLOR R., LUPARIA L., *Criminalità organizzata e criminalità informatica ("cyber-organized-crime")*, in *Diritto penale contemporaneo*, 2019.

FLOR R., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in *Diritto penale contemporaneo*, 2012.

FLOR R., *Frodi identitarie e diritto penale*, in *Penale.it*, 2008.

FURNELL S., EMM D., PAPADAKI M., *The challenge of measuring cyber- dependent crimes*, in *Computer fraud and Security*, 2015.

GABRIELLI I., *Come le mafie si muovono nel mondo della rete, in Scintille. Trimestrale della fondazione Scintille di futuro*, 1, 2023.

GAITO A., *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC),* in *Archivio Penale*, 1, 2024.

GHAPPOUR A., *Searching Places Unknown/ Law Enforcement Jurisdiction on the Dark Web*, Stanford Law review 69, 4, 2017.

GRABOSKY P., *The Internet, Technology and Organised crime*, in *Asian criminology*, 2, 2007.

GRANIERI G., *La società digitale*, Editori Laterza, 2006.

GRATTERI N., NICASO A., *Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*, Mondadori, 2023.

GUAGLIARDI G., *Utilizzo nel processo penale di messaggi criptati ottenuti tramite una operazione di hacking massiva all'estero e acquisiti in Italia tramite Ordine Europeo di Indagine. Il fine giustifica i mezzi?,* in *Giurisprudenza penale*, 2024, 6.

GUERINI T., INSOLERA G., *Diritto penale e criminalità organizzata*, Giappichelli, 2019.

HARINAM V., BARAK A., *Law Enforcement Strategies for Disrupting Cryptomarkets*, Springer, 2024.

HUDSON J., WITT P., *Internet Relay Chat (IRC),* in AA.VV., *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications,* 3, 2017, a cura di Bidgoli, John Wiley & Sons Ltd. (DOI: https://doi.org/10.1002/9781118256107.ch57).

HUTCHINGS A., *Crime from the keyboard: organized cybercrime, co-offending, initiation and knowledge transmission*, in *Crime, Law and Social Change*, 62, 1, 2014.

IACOVIELLO F.M., *Ordine pubblico e associazione per delinquere*, in *Giustizia Penale*, 1990.

IACOVIELLO F.M., *L'organizzazione criminogena prevista dall'art. 416 c.p.*, in *Cass. pen.*, 1994.

INGROIA A., *L'associazione di tipo mafioso*, Giuffrè, 1993.

IOVINO P., *Le criptovalute nella fase di layering del riciclaggio*, in *Giurisprudenza penale*, 3, 2022.

KABRA S., GORI S., *Drug trafficking on cryptomarkets and the role of organized crime groups,* in *Journal of economic criminology*, 2, 2023.

KALM K., *Illicit Network Structures in Cyberspace*, *5th International Conference on Cyber Conflict*, 2013.

KAREEM K.M., *Cybersecurity in Onion Routing Environments: Strategies to Thwart Cyber Threats,* in *Journal Of High-Frequency Communication Technologies*, 2024.

KAZAKOVA A., TELEANU S., KOVAC B., HAMZA F., *Comparative analysis: The Budapest Convention vs the UN Convention Against Cybercrime*, in *Digital Watch Observatory*, 2024.

KOOPS B., *The Internet and its Opportunities for Cybercrime,* in *Tilburg Law School Legal Studies Research Paper Series*, 9, 2011.

KRANENBARG M., *Cyber-Dependent Crime Versus Traditional Crime*, in *Kranenbarg, and Leukfeldt, Cybercrime in context: The human factor in victimization, offending, and policing, Crime and Justice in Digital Society*, 1, 2021, pp. 195-216.

KRISHNAN A., *Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organization*s, in *Journal of Strategic Security*, 13, 1, 2020.

KRUISBERGENA E.W., LEUKFELDT E.R., KLEEMANSC E.R, ROKSD R.A., *Money talks money laundering choices of organized crime offenders in a digital age*, in *Journal of Crime and Justice*, 42, 5, 2019.

KUEL T. D., *From Cyberspace to Cyberpower: Defining the Problem*, in *Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Cyberpower and National Security*, in *National Defence University Press*, 2009.

LAIBY T., SUBRAMANYA B., *A Comprehensive Overview of Telegram Services - A Case Study*, in *International Journal of Case Studies in Business, IT, and Education*, 6, 1, 2022.

LAVORGNA A., *Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics,* in *Trends in Organised Crime, 17, 4*, 2014.

LAVORGNA A., *Organised crime goes online: realities and challenges,* in *Journal of Money Laundering Control,* 18, 2, 2015.

LAVORGNA A., *Cyber-organised crime. A case of moral panic?,* in *Trends in Organized Crime*, 4, 2019.

LAVORGNA A., *Exploring the cyber-organised crime narrative: The hunt for a new bogeyman?, 2016,* in *Narratives on organised crime in Europe. Criminals, corrupters and policy*, a cura di Van Duyne P., Scheinost M., Antonopoulos G. A., Harvey J., Von Lampe K., The Hague, Wolf Legal Publisher, 2016.

LAVORGNA, A. *Unpacking the political-criminal nexus in state-cybercrimes: a macro-level typology.* in *Trends in Organised Crime,* 2023.

LAVORGNA A., SERGI A., *Types of organised crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies*, in *International Journal of law, crime and Justice*, 2014, 42.

LAVORGNA A., SERGI A., *Intergenerational and technological changes in mafia- type groups/ a transcultural research agenda to study the 'ndrangheta and its mobility*, in *SN Soc Sci*, 4, 2024.

LAVORGNA A., SERGI A., *Serious, therefore organised? A critique of the emerging "Cyber-organised crime" rhetoric in the United Kingdom*, in *International Journal of Cyber criminology*, 10, 2, 2016.

LESLIE A., *Legal Principles for Combatting Cyberlaundering, Law, Governance and Technology Series*, 2014.

LEUKFELDT, E. R., KLEEMANS E.R., STOL W.P., *Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks*, in *British Journal of Criminology*, 57, 3, 2017.

LEUKFELDT, E. R., LAVORGNA A., KLEEMANS E. R., *Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, in *European Journal on Criminal Policy and Research*, 23, 3, 2017.

LEVI M., *Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation*, in *Trends in Organized crime*, 24, 2021.

LEVI M., *Money Laundering Risks And E-Gaming: A European Overview And Assessment*, in *Era Forum*, in *Journal of the Academy of European law*, 10, 2010.

LEVI M., ET AL.., *The Implications of Economic Cybercrime for Policing*, Cardiff University, 2015, http://orca.cf.ac.uk/88156/1/Economic-Cybercrime-FullReport.pdf.

LIBICKI M. C., *Cyberdeterrence and Cyberwarfare*, Santa Monica, 2009.

LIGUORI F., *Il principio di mutuo riconoscimento nell'ambito della cooperazione giudiziaria in materia penale: le condizioni di ammissibilità dell'Ordine europeo di indagine penale*, in *Quaderni AISDUE - Rivista quadrimestrale*, 1, 2024.

LIVI A., *I diversi settori del FinTech - Problemi e prospettive*, (a cura di) CORAPI E., LENER R., Wolters Kluwer, Cedam, Università degli studi di Roma "Tor Vergata", Collana pubblicazioni Facoltà di Giurisprudenza - Dipartimenti di Diritto Privato e di Diritto Pubblico, Terza serie, 2019.

LORENZETTO E., *Il caso Encrochat e l'ordine europeo di indagine penale nella staffetta fra Corte di Giustizia e diritto dello stato di emissione*, in *Cass. pen.*, 9, 2024.

Lupària L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (l. 18 Marzo 2008, n. 48). I profili processuali*, in *Dir. pen. proc.*, 6, 2008.

LUPARIA L., *Computer crimes e procedimento penale,* in *Trattato di Procedura penale*, *Modelli differenziati di accertamento*, a cura di Garuti G., VII, I, Torino, 2011.

LUPTON D., *Digital sociology*, Routledge, London, 2014.

LUSTHAUS J., *How organised is organised cybercrime?*, in *Global Crime Journal*, 14, 1, 2013.

MAIELLO V., I*l concorso esterno tra indeterminatezza legislativa e tipizzazione giurisprudenziale. Raccolta di scritti,* Torino, 2014.

MAIMON D., LOUDERBCK E.R., *Cyber-Dependent Crimes: An Interdisciplinary Review*, in *Annual Review of Criminology*, 2019.

MANZINI V., *Trattato di diritto penale italiano,* V ed., vol. VI, 1987.

MARAS M., *Cybercriminology*, Oxford University Press, 2016.

MARTIN J., *Lost on the Silk Road: Online drug distribution and the 'cryptomarket'*, in *Criminology and Criminal Justice*, 14, 2013.

MARTINU, O., MCEWEN, G., *Crime in the age of technology*, in E*uropean law enforcement research Bulletin*, (4 sce), Cepol, 2018.

MC GOVERN V., FORTIN F., *The Anonymous Collective: Operations and Gender Differences*, in *Women and Criminal Justice*, 30, 2, 2019.

MC GUIRE M., *Organised crime in the digital age*, London, John Grieve Center for policy and security and Bae, 2012.

MCGUIRE M., DOWLING S., *Cybercrime: A Review of the Evidence: Summary of Kedy Findings and Implications*, Home Office, London, UK, 2013.

MICHELINI G., *La Convenzione Di Palermo/2. Il ruolo dell'italia nella redazione del testo finale*, in *Cross*, 5, 2, 2019.

MINNAAR A., *Organised Crime And The 'New More Sophisticated' Criminals Within The Cybercrime Environment: How 'Organised' Are They In The Traditional Sense?,* in *Acta Criminologica: Southern African Journal of Criminology,* 29, 2, 2016.

MIRANDA M. L., *L'utilizzabilità delle chat criptate acquisite mediante ordine europeo di indagine*, in *Quotidiano Legale*, 4, 2024.

MIRTI M., *Struttura e caratteri del Cyberspace*, in *Opinio Iuris Law and Politics review*, 2020.

MONTALDO S., *I limiti della cooperazione in materia penale nell'Unione europea*, Editoriale scientifica Napoli, 2015.

MORELATO, M., BROSÉUS, J., DE GRAZIA, A., TAHTOUH, M., ESSEIVA, P., ROUX, C., 2018. *Forensic drug intelligence and the rise of cryptomarkets. Part II: Combination of data from the physical and virtual markets,* in *Forensic Sci. Int*., 288, pp. 201-210, https://doi.org/10. 1016/j.forsciint.2018.05.002.

MORSELLI, C., TURCOTTE, M., TENTI, V, *The mobility of criminal groups*, in *Global Crime*, 12, 2011.

MURRO O, NOCERINO W., *Più ombre che luci nelle sentenze delle Sezioni Unite in tema di criptofonini*, in *Penale Diritto e Procedura*, 2024.

MUSIANI F., *La crittografia nei sistemi di messaggistica sicura: le libertà digitali tra sviluppo tecnologico e regolazione*, in *Rivista di Digital Politics*, 3, 2022.

NADDEO M., *Criptovalute: Profili Di Rilevanza Penale*, in *Penale Diritto e Procedura*, 2022.

NAKAMOTO S., *Bitcoin: A peer-to-peer electronic cash system*, 2008.

NICOLICCHIA F., *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla querelle giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero*, in *Sistema Penale*, 2, 2024.

NIMMA S., *Money Laundering In The Cyberworld: Emerging Trends*, in *Indian Journal of Integrated Research in Law*, 2, 2, 2022.

NURSE J., BADA M., *The Group element of cybercrime: types, dynamics and criminal operations*, in *The Oxford handbook of cyberpsychology*, DOI: 10.1093/oxfordhb/9780198812746.013.36, 2018.

OERLEMANS J.J., VAN TOOR D., *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in E*uropean journal of crime, criminal law and criminal justice*, 30, 2022.

OERLEMANS J., ROYER S., *The future of data-driven investigations in light of the Sky ECC operation*, in *New Journal pf European Criminal law*, 14, 4, 2023.

OLSON P., *We Are Anonymous: Inside the Hacker World of LulzSec*, in *Anonymous, and the Global Cyber Insurgency*, London: Little, Brown, 2012.

PASSERELLI N., *Bitcoin e antiriciclaggio*, in *Gnosis, Rivista italiana di intelligence*, 2016.

PATALANO V., *L'associazione per delinquere*, Jovene, Napoli, 1971.

PATALANO R., *Riciclaggio e flussi finanziari illeciti nel capitalismo contemporaneo*, in *Riv. Online della politica economica*, 2022.

PAYNE R., *Defining cybercrime*, in *The Palgrave handbook of international cybercrime and cyberdeviance*, (a cura di) T. Holt – A. Bossler, Palgrave Macmillan, Cham, 2020.

PICARELLA L., *Criminalità in rete. Dalle piattaforme illegali alle cybermafie*, Roma, Donzelli Editore, 2025.

PICARELLA L., *La criminalità organizzata cibernetica. Il reato associativo tra mutamento sociale e giurisprudenziale*, in *Meridiana*, 106, 2023.

PICKLES R., *'Money Mules': Exploited Victims or Collaborators in Organised Crime?*, in *Irish Probation Journal*, 18, 2021.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale,* in *Dir. pen. proc.*, 6, 2008.

PICOTTI L., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo,* in *Diritto dell'Internet,* 2008.

PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Diritto dell'Internet*, 2, 2005.

PICOTTI L., *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. Trim. Dir. pen. dell'economia*, 3-4, 2018.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in Id., (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Cedam, Padova 2004.

PILLER G., ZACCARIOTTO E., *Cyber-Laundering: The Union Between New Electronic Payment Systems and Criminal Organizations*, in *Transition Study Review*, 2009.

PIOLETTI U., voce *Associazione per delinquere*, in *Enc. forense*, vol. I, 1958.

POMES F., *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, in *Diritto penale contemporaneo*, 2, 2019.

PRETATTO R. *Digitalizzazione e giusto processo: la digital evidence nella giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *DPCE online*, 1, 2024.

PRUZELIUS G., GYLLNER T., *Phishing in the workplace: organizational practices, culture and phishing vulnerability*, in *Diva Portal*, 2025.

PUJIA P., *L'acquisizione della messaggistica criptata conservata su server straniero tra classificazioni concettuali e divergenze giurisprudenziali*, in *Archivio Penale*, 2024, 2.

RAGAZZI S., SPIEZIA F., *Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano*, in *Sistema penale*, 2, 2024.

RAMPIONI M., *I limiti di utilizzabilità della messaggistica criptata SkyEcc acquisita tramite ordine europeo di indagine tra obblighi europei e principi costituzionali*, in *Giurisprudenza penale*, 10, 2023.

RAUCCI P., *L'ordine europeo di indagine e prove digitali: tra presunzione di legittimità degli atti compiuti all'estero e diritti fondamentali*, in *Penale diritto e procedura*, 2025.

ROMAGNA M., RUTGER LEUKFELDTB E., *Hacktivism: From Loners to Formal Organizations? Assessing the Social Organization of Hacktivist Networks,* in *Deviant Behavior*, 2024.

ROMAGNA M., VAN DEN HOUT N.J., *Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats*, Virus Bullettin Conference October, Madrid, 2017.

ROSLER P. ET AL., *More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema*, in *EuroS&P*, 2018.

RUGGIERO V., *Economie sporche. L'impresa criminale in Europa*, Bollati Boringhieri, Torino, 1996.

SABELLA P.M., *Il fenomeno del cybercrime nello spazio giuridico contemporaneo. Prevenzione e repressione degli illeciti penali connessi all'utilizzo di Internet per fini di terrorismo, tra esigenze di sicurezza e rispetto dei diritti fondamentali*, in *Informatica e diritto*, XXVI, 1-2, 2017.

SANDOIU A., *Combating organised crime: The analysis, effects, and control of crimes committed by means of the emerging Dark Net*, Ambassadeurs de la Jeunesse, 2019.

SANTONS M. ET AL., *Affordance is power: contradictions between communicational and technical dimensions of Whatsapp's end-to-end encryption*, in *Social media and Society*, 2018.

SAVASTANO L., *La regola "follow the money" nello spazio virtuale della blockchain: l'individuazione ed il sequestro di asset digitali*, in *Il mercato dei non fungible tokens tra arte, moda e gamification*, a cura di CANEPA A., Milano University Press, 2024.

SCIARRONE R., *Le mafie dalla società locale all'economia globale*, in *Meridiana*, 43, 2002.

SEELAM N., PALISETTI V., *Comparative research of WhatsApp and Telegram by using heuristic principles*, Faculty of Computing, Sweden, 2022.

SERGI A., *Divergent mind-sets, convergent policies. Policing models against organised crime in Italy and in England within international frameworks*, in *European Journal of Criminology*, 12, 6, 2015.

SHEKHAWAT KS., *Legal Challenges in Regulating the Dark Web: Balancing Privacy, Security, and Jurisdiction*, disponibile in Academia EDU.

SICIGNANO G.J., *Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain?,* in *Diritto Penale Contemporaneo*, 4, 2020.

SICURELLA S., *Le mafie italiane nel cyberspazio/ nuova frontiera o terreno di sperimentazione?*, in *Rivista di Criminologia, Vittimologia e Sicurezza*, XVI, 2022.

SIMIOL E. ET AL., *A security analysis comparison between Signal, WhatsApp and Telegram,* in *Cryptology ePrint Archive*, 2023.

SINGH J., AHLUWALIA J.K., *Dark Web And Cybercrime: Challenges In Legal Enforcement*, in *Tijer international research journal*, 12, 4, 2025.

STILE A., *Riciclaggio e reimpiego di proventi illeciti*, 2009.

STOYKOVA, R., *Encrochat: The hacker with a warrant and fair trials?*, in *Forensic Science International: Digital Investigation*, 46, 2023.

STRATTON G, POWELL A, CAMERON R., *Crime and justice in digital society: Towards a 'digital criminology'*, in *International Journal for Crime Justice Social Democracy*, 6, 2, 2017.

TROPINA, T., "*This is not a human rights convention!": The perils of overlooking human rights in the UN cybercrime treaty*, in *Journal of Cyber Policy*, 9, 2, 2024.

TROPINA T., *The Evolving Structure of Online Criminality*, in *eucrim*, 4, 2012.

VACIAGO G., *Remote forensics and cloudcomputing: an italian and european legal overview*, in *Digital evidence and electronic signature law review*, 8, 2011.

VALIANTE M., *Natura plurisoggettiva della partecipazione all'associazione criminale*, in *Riv. it. dir. e proc. pen*., 1, 1987.

VALIANTE M., *Il reato associativo*, Giuffrè, 1990.

VAN DER HULST R.C., NEVE R.J.M., *High-tech crime*, *Soorten Criminaliteit En hun daders*, *Een literatuurinventarisatie*, The Hague: WODC, 2008.

VOLK K., *Criminalità organizzata e criminalità economica*, in S. Moccia (*a cura di*), *Criminalità organizzata e risposte ordinamentali. Tra efficienza e garanzia*, Edizioni Scientifiche Italiane, Napoli, 1999.

VON LAMPE K., *A Systematic Overview of Definitions of Organized Crime*, in *Organized Crime: Analyzing illegal activities, criminal structures, and extra-legal governance*, Sage Publications, 2016.

WALL, D. S., *Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'*, in Jewkes, Y. and Yar, M. (Ed.s) *Handbook of Internet Crime*, 2010.

WALL D., *Cybercrime. The Transformation of Crime in the Information Age,* Cambridge Polity press, 2007.

WALL D.S*., Digital realism and the governance of spam as cybercrime*, in *European Journal on Criminal Policy and Research*, 10, 4, 2005.

WALL D.S., *Internet mafias? The dis-organisation of crime on the internet*, in S. Canappele – F. Calderoni (a cura di), *Organized crime, Corruption and crime prevention*, Springer, Cham, 2014.

WALL, D.S., *Towards a conceptualisation of cloud (Cyber) crime*, in *Tryfonas, T, (ed.) Lecture Notes in Computer Science. International Conference on Human Aspects of Information Security, Privacy, and Trust,* 2017.

WALL D.S., *The Internet as a Conduit for Criminals*, in Pattavina A. (ed*) Information technology and the criminal justice system*. Sage, Thousand Oaks, 2015.

WALL D., *Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, in *The European Review of Organized Crime*, 2, 2, 2015.

WANG P., SU M., WANG J., *Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer- to-peer lending market in China,* in *Brit. Journal Criminology*, 61, 2021.

WRONKA C., *"Cyber laundering": the change of money laundering in the digital age*, in *Journal of Money Laundering Control*, 25, 2, 2021.

YAR M., *Cybercrime and society*, London, Sage, 2006.

FONTI INTERNAZIONALI

Ad Hoc Committee, Unione Europea, *Contribution from the European Union and its member states, Preparation for the first session of the United Nations Ad Hoc Committee to elaborate a Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, disponibile in https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/EU_Position_for_AHC_first_session.pdf

Ad Hoc Committee, Cina, *China's Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes*, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

BAE Systems Detica and London Metropolitan University, *Organised Crime in the Digital Age*, *Norton Cybercrime Report 2011,* 2012.

Commissione parlamentare antimafia, *Relazione sulle infiltrazioni mafiose e criminali nel gioco*, 6 luglio 2016.

Consiglio d'Europa, *Convenzione sulla criminalità informatica*, STE n.185, 2001, in *www.coe.int*

Consiglio d'Europa, *Explanatory Report to the Convention on Cybercrime*, ets n. 185.

Crown Prosecution Service, *Cybercrime - prosecution guidance*, in *Legal Guidance Cyber*, online crime, 15 luglio 2024.

EMCDDA, *EU drug markets report: a strategic analysis*, European Monitoring Center for Drugs and Drug Addiction, Publications office of the European Union, Luxembourg, 2013.

European Commission, Europol, *Drugs and the darknet: Perspectives for enforcement, research and policy*, Publications Office of the European Union, 2017.

European Commission, *Policing the Dark Web: Ethical and Legal Issues,* Horizon 2020 Framework Programme of the European Union, Ref. Ares, 2019, 1666154 - 13/03/2019.

Europol, *How Illegal Drugs Sustain Organised Crime in the EU*, 2017.

Europol, *Internet Organised crime threat assessment*, IOCTA, 2021.

Europol, *Cyber-Attacks: The Apex Of Crime-As-A-Service*, IOCTA 2023.

Europol, *Internet Organised Crime Threat Assessment*, IOCTA, 2024, Publications Office of the European Union, Luxembourg.

Europol, *Serious and Organised crime threat assessment, A Corrupting Influence: The Infiltration And Undermining Of Europe's Economy And Society By Organised Crime*, 2021, in *https://www.europol.europa.eu/publications-events/main-reports/socta-report*, pp. 22 ss.

Europol/Eurojust press release, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, 2 luglio 2020.

Europol, *Global Coalition Takes Down New Criminal Communication Platform*, 18 settembre 2024.

Europol's European Cybercrime Centre, Trend Micro Research, Unicri, *Malicious Uses and Abuses of Artificial Intelligence*, 2020, in *https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence#downloads*

FAFT Report, *Vulnerabilities of Casinos and Gaming Sector*, 2009, http://www fatf-

gafi.org/dataoecd/47/49/42458373.pdf.

Interpol, *Cybercrime Strategy Guidebook,* a cura di S. CROSS S., HIRRLE S., LIM M.A., 2021,

National Crime Agency, *High end money laundering strategy and action plan. National Crime Agency*, London, 2014.

National Crime Agency*, NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation*, 2020, https://www.nationalcrimeagency.gov.uk/news/operation-venetic.

OCSE Report "*Ending the Shell Game- Cracking down on the Professionals who enable Tax and White Collar Crimes*", 25 febbraio 2021.

Parlamento europeo, *Understanding cybercrime*, in *European Parliament Research Service*, 2024.

Trend Micro Research, Unicri, Europol's European Cybercrime Centre, *Malicious Uses and Abuses of Artificial Intelligence*, 2020, in *https://www.europol.europa.eu/publications-events/publications/malicious-uses-and-abuses-of-artificial-intelligence#downloads*.

United Nation Office on Drug and Crime, *Comprehensive Study on cybercrime*, Draft, 2013.

United Nations Office on Drugs and Crime, European Monitoring Centre for drugs and drug addiction, *Organized Crime Markets. Drug Trafficking*, in Organized Crime, Module 3 E4J, 2018.

United Nations Office on Drugs and Crime, *Conceptualizing organized crime and defining the actors involved*, in E4J mod. 13 "*Cyber organized crime*", 2019.

United Nation Office on Drug and Crime, *Digest of cyber organized crime*, II ed., 2022.

United Nations Office on Drugs and Crime, *Use Of The Dark Web And Social Media For Drug Supply*, in World Drug report, 2023, pp. 223-234.

United Nations Office on Drugs and Crime, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

United Nations Office on Drugs and Crime, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*, 2024, p. 4.

United Nations, *UN Toolkit on synthetic drugs*, https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/onlinetrafficking/onlinesalesplatforms.html.

FONTI GIURISPRUDENZIALI

Giurisprudenza di merito

Ordinanza di applicazione cautelare personale n. 39 + 45/2022 nei confronti, tra gli altri, di Rocco Morabito, del Gip del Tribunale di Reggio Calabria, 7 marzo 2023, p.p. n. 4837/2022 r.g.n.r. d.d.a.

Ordinanza di applicazione di misure cautelari custodiali in carcere nei confronti, tra gli altri, sempre di Rocco Morabito, del GIP del Tribunale di Genova, 27 aprile 2023, p.p. 6267/2021 r.g.n.r.

Ordinanza di custodia cautelare n. 362/22, nei confronti, tra gli altri, di Raffaele Imperiale, del Gip del Tribunale di Napoli, p.p. n. 32678/16 r.g.n.r

Tribunale di Reggio Calabria, p.p. n. 3886/2022 r.g.n.r., DDA p.p. n. 2520/2022 Reg. G. L P. DDA/2022 R. O. C. C. 44/2022 R. O. C. C. 4/202S R. O. C. C., p. 2139.

Ordinanza di applicazione di misure cautelari personali nei confronti di Annunziata Katia + 72, 6 novembre 2018, GIP del Tribunale di Reggio Calabria, p. 223.

Procura della Repubblica presso il Tribunale di Catanzaro, richiesta di applicazione di misure cautelari personali nei confronti di A.N. + 122, 22 luglio 2022, pp. 3268-69.

Ordinanze del Trib. Reggio Calabria, del 5 novembre 2022, n. 801 e del 19 novembre 2022, n. 868.

G.I.P., Tribunale di Milano, sentenza 10 dicembre 2007, n. 888.

Giurisprudenza di legittimità

Cass. pen., sez. I, 13 marzo 1968, n. 434.

Cass.pen., 13 febbraio 1970, n. 345.
Cass. pen., sez. I, 21 aprile 1982, n. 1674
Cass. pen., sez. V, 8 febbraio 1983, n. 1768.
Cass. pen., sez. I, 22 aprile 1985, n. 7462
Cass. pen., sez. I, n. 1440 del 1986.
Cass. pen., sez. VI, 12 aprile 1986, n. 2894.
Cass. pen., sez. VI, 10 aprile 1987, n. 7789.
Cass. pen., sez. VI, 21 novembre 1989, n. 16164.
Cass. pen., sez. I, 1 febbraio 1991, n. 1332.
Cass. pen., sez. I, 24 marzo 1992, n. 3402.
Cass. pen., sez. III, 7 luglio 1992, n. 8539.
Cass. pen., sez. I, 9 dicembre 1993, n. 11307.
Cass. pen., sez. VI, 10 maggio 1994, n. 11446.
Cass. pen., sez. VI, 17 novembre 1994, n. 11446.
Cass. pen., sez VI, 14 giugno 1995, n. 11413.
Cass. pen., sez. I, 13 dicembre 1995, n. 6553.
Cass. pen., sez. VI, 21 maggio 1998, n. 3089.
Cass. pen., sez. I, 14 luglio 1998, n. 10107.
Cass. pen., sez. VI, 2 novembre 1998, n. 1472.
Cass. pen., sez. V, 28 giugno 2000, n. 12525.
Cass. pen., sez. V, 1 dicembre 2000, n. 12525.
Cass. pen., 10 aprile 2003, n. 17027.
Cass. pen., sez. I, 5 agosto 2003, n. 33033.
Cass. pen, sez. IV, 27 novembre 2003, n. 7187.
Cass. pen., sez. III, 2 dicembre 2004, n. 8296.
Cass. pen., sez. II, 26 gennaio 2005, n. 2350.
Cass. pen., Sez. VI, 12 luglio 2005, n. 33748.
Cass. pen., sez. I, 28 settembre 2005, n. 39757.
Cass. pen., sez. V., 11 giugno 2008, n. 31389.
Cass. pen., sez. V, 5 maggio 2009, n. 31149.
Cass. pen., sez. II, 22 gennaio 2010, n. 5424.
Cass. pen., sez. II, 11 febbraio 2010, n. 5424.

Cass. pen., sez. I, 18 marzo 2011, n. 31845.

Cass. pen., sez. II, 24 marzo 2011, n. 16606.

Cass. pen., sez. VI, 15 giugno 2011, n. 25698.

Cass. pen., sez. VI, 7 novembre 2011, n. 3886.

Cass. pen., sez. VI, 16 dicembre 2011, n. 9117.

Cass. pen., sez. III, 25 gennaio 2012, n. 8024.

Cass. pen., sez. III, 28 giugno 2012, n. 33563.

Cass. pen., sez. VI, 24 settembre 2012, n. 9061.

Cass. pen., sez. II, 15 gennaio 2013, n. 19917.

Cass. pen., sez. II, 17 gennaio 2013, n. 16339.

Cass. pen., sez. VI, 30 gennaio 2013, n. 34489.

Cass pen., sez. III, 14 marzo 2013, n. 20921.

Cass. pen., sez. II, 3 aprile 2013, n. 20451.

Cass. pen., sez. fer., 29 agosto 2013, n. 46156.

Cass. pen.. sez. fer., 12 settembre 2013, n. 50620.

Cass.pen., sez. II, 8 novembre 2013, n. 46989.

Cass. pen.,, sez. IV, 28 gennaio 2014, n. 8092.

Cass. pen., sez. I, 26 febbraio 2014, n. 39222.

Cass. pen., sez. VI, 13 maggio 2014, n. 36131.

Cass. pen., sez. V, 8 ottobre 2014, n. 18756.

Cass. Pen., sez. III, 4 marzo 2015, n. 26724.

Cass. pen, sez. III, 6 novembre 2015, n. 9459.

Cass. pen., sez. I, 18 dicembre 2015, n. 1911.

Cass. pen, sez. I, 8 gennaio 2016, n. 15955.

Cass. pen., sez. II, 27 settembre 2016, n. 52316.

Cass. pen., sez. II, 4 ottobre 2016, n. 53000.

Cass. pen., sez. VI, 14 ottobre 2016, n. 52590.

Cass. pen., sez. II, 24 novembre 2016, n. 52005.

Cass. pen., sez. VI, 28 febbraio 2017, n. 15573.

Cass. pen., sez. VI, 11 luglio 2018, n. 38524.

Cass. pen., sez. V, 24 ottobre 2018, n.15041.

Cass., sez.VI, 27 aprile 2020, n. 12975.

Cass. pen., sez. VI, 30 settembre 2020, n. 28821.
Cass. pen., sez. II, 12 febbraio 2021, n.7839.
Cass. pen., sez. II, 12 febbraio 2021, n.7837.
Cass. pen., sez. III, 11 giugno 2021, n. 47291.
Cass. pen., sez. V, 15 luglio 2021, n. 32767
Cass. pen., sez. II, 26 ottobre 2021, n.1688
Cass. pen. sez.I, 1 luglio 2022, n. 34059.
Cass. pen. sez. I, 13 ottobre 2022, n. 6363 e 6364
Cass., sez.I, 15 febbraio 2023, n. 6364.
Cass. pen. sez. IV, 4 aprile 2023, n. 18514.
Cass. pen. sez. IV, 5 aprile 2023, n. 16347.
Cass., sez. IV, 12 aprile 2023, n. 18523.
Cass., sez. IV, 18 aprile 2023, n. 16347.
Cass. pen., sez. II, 28 aprile 2023, n. 17945.
Cass. pen., sez. IV, 26 ottobre 2023, n. 44155.
Cass.pen., sez.VI, 2 novembre 2023, n. 44154.
Cass., S.U. penali, 14 giugno 2024, n. 23755 e n. 23756.
Cass. pen., sez. III, 25 giugno 2024, n. 39478.
Cass. pen., 20 novembre 2024, n. 1760.

Giurisprudenza internazionale

Corte di giustizia dell'Unione europea, sentenza 2 marzo 2021, H.K. c. Prokuratuur, C-746/18.

Corte giust., 30 aprile 2024, *M.N.*, C-670/22

Dreamboard v. *United States of America v. John Doe #1, Edward Odewaldt, et al*., Case n.. 10-CR-00319, (W.D. Louisiana, 16 March 2011).

United States District Court, *United States of America v. Gal Vallerius* (2018), United States District Court Southern District Of Florida Case n. 17-Cr-20648-Scola/Torres

United States Of America, Plaintiff, V. Gal Vallerius, Defendant *Report And Recommendation On Defendant's Motion To Suppress*

United States Court Of Appeals For The Second Circuit August Term, 2016 (Argued: October 6, 2016 Decided: May 31, 2017) No. 15-1815 United States Of America, Appellee, — V. — Ross William Ulbricht, A/K/A Dread Pirate Roberts, A/K/A Silk Road, A/K/A Sealed Defendant 1, A/K/A Dpr, Defendant-Appellant.