doi: 10.14664/rcvs/241

Le mafie italiane nel cyberspazio: nuova frontiera o terreno di sperimentazione?

Les mafias italiennes dans le cyberespace : nouvelle frontière ou champ d'expérimentation ?

Italian mafias in cyberspace: new frontier or experimental ground?

*Sandra Sicurella**

Riassunto
Lo studio e l'interesse per il fenomeno mafioso sono all'origine di questo contributo, che nasce dalla curiosità di approfondire la diffusione a livello mediatico e istituzionale di informazioni non sempre corroborate da prove incontrovertibili sulla presenza online delle mafie italiane. L'interesse è pertanto motivato dalla volontà di comprendere se la capacità di adattamento al mutamento sociale delle mafie endogene si riverberi e con quali effetti nel cyberspazio. Questa breve riflessione sul tema, che si avvale del contributo della letteratura e dell'apporto di alcune recenti indagini, non vuole né può certamente essere esaustiva anche per la natura stessa dei fenomeni presi in esame, ma intende rappresentare un'istantanea in vista di ulteriori approfondimenti.

Résumé
L'étude et l'intérêt pour le phénomène mafieux sont à l'origine de cette contribution, qui naît de la curiosité d'approfondir la diffusion au niveau médiatique et institutionnel d'informations qui ne sont pas toujours corroborées par des preuves incontestables de la présence en ligne des mafias italiennes. L'intérêt est donc motivé par la volonté de comprendre si la capacité d'adaptation au changement social des mafias endogènes se reflète dans le cyberespace et, si cela est le cas, avec quels effets. En raison de la nature même des phénomènes examinés, cette contribution ne veut ni ne peut être exhaustive, mais elle vise plutôt à proposer des pistes de réflexion pour des travaux futurs à partir de l'analyse de la littérature et des études les plus récentes en la matière.

Abstract
The study and interest in the mafia phenomenon are at the origin of this contribution, which stems from the curiosity to investigate the media and institutional dissemination of information, that are not always corroborated by incontrovertible evidence, about the online presence of Italian mafias.
The interest is therefore motivated by the desire to understand whether the capacity of endogenous mafias to adapt to social change reverberates in cyberspace and, if so, with what effects.
Drawing from the most recent literature and researches, this brief reflection on the topic is certainly not intended or cannot be exhaustive, also due to the very nature of the phenomena examined, but rather aims to suggest some directions for further investigation.

Key words: mafie, cyberspazio, mutamento sociale

* Professoressa associata in Sociologia giuridica, della devianza e del mutamento sociale. Dipartimento di Sociologia e Diritto dell'Economia – Università di Bologna.

1. Introduzione

È sulle opportunità offerte dalla rete che dobbiamo interrogarci per comprendere quale possa essere il ruolo della criminalità organizzata di stampo mafioso, da tempo ormai presenza consolidata nello spazio offline del nostro paese.

Il capitale sociale da cui trae linfa vitale la criminalità organizzata sembra tuttavia alimentarsi maggiormente nella dimensione offline, ma le nuove sfide e le nuove opportunità offerte dalla tecnologia hanno inciso anche sulle modalità di cooperazione (Leukfeld *et al.*, 2019).

Come ricordano Leukfeld e colleghi (2019), esistono due tipi di crimini informatici che riguardano nuovi illeciti commessi attraverso l'uso di tecnologie dell'informazione e reati tradizionali per i quali il mezzo tecnologico innova le tecniche e facilita l'azione.

Ciononostante, secondo alcune ricerche (Leukfeld *et al.* 2016; Leukfeld *et al.* 2019), nelle reti criminali informatiche un ruolo di primo piano è svolto dai legami sociali del mondo fisico, offline.

Broadhurst *et al.* (2014) sottolineano come il dibattito sulla criminalità informatica e su quella organizzata risenta di alcuni stereotipi. Da una parte, infatti, si trova la figura dell'hacker solitario che sembra smentire la dimensione collettiva del crimine e, dall'altra, le definizioni di criminalità organizzata sembrano, per certi versi, obsolete se considerate alla luce dell'evoluzione del fenomeno. Secondo tale studio, la maggior parte del crimine informatico organizzato si fonda sul lavoro di tecnici qualificati, che mettono le loro conoscenze a servizio dell'attività criminale, ma ci sono altresì gruppi criminali tradizionali, che approfittano della tecnologia digitale per finalità criminali. Presumibilmente, sostengono gli autori, questa distinzione si assottiglierà di fronte ad un mezzo, quello tecnologico, che diventa sempre più pervasivo (Broadhurst *et al.* 2014).

La Convenzione di Budapest sulla criminalità informatica del 2001, unico strumento internazionale vincolante in questo ambito, ratificata in Italia con la Legge 48/2008, con il termine cybercriminalità si riferisce a una molteplicità di reati[1] «tuttavia, se da un lato è vero che questo termine comprende una pluralità di condotte criminali il cui unico comune denominatore è il fatto di essere realizzate "nel" o "attraverso" il cyberspazio, dall'altro si rileva come esista un sottile filo rosso che unisce queste diverse realtà illecite, accomunate dalla possibilità di inserirsi in un nuovo spazio, quello digitale, del quale sfruttare tutte le potenzialità e caratterizzate da problematiche simili per quanto concerne la loro regolazione e il loro contrasto» (Macilotti, 2018, pp. 23-24).

La diffusione di internet e delle tecnologie dell'informazione ha determinato nuove opportunità per tutti, i cittadini possono usufruire della rete e sfruttarne i vantaggi per esigenze diverse. Gli scopi per i quali si accede alla rete, infatti, non sono sempre determinati dalle stesse motivazioni o necessità, pertanto, le potenzialità del digitale vengono utilizzate anche per fini illeciti.

Il cyberspazio e le tecnologie digitali possono dunque determinare nuove forme di criminalità (*Internet integrity crime*) oppure contribuire all'evoluzione di forme tradizionali di illeciti (*Internet related crime*) (Macilotti, 2018).

[1] Tra gli obiettivi, ricordiamo «Criminalizzare le infrazioni contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici, le infrazioni associate all'informatica, le infrazioni associate ai contenuti (ovvero pedopornografia, razzismo e xenofobia) e le infrazioni legate alla violazione del copyright e dei diritti correlati» in https://www.coe.int/it

Una materia controversa quella del crimine informatico che, in letteratura, comprende una serie di crimini che variano in termini di *mediation by technologies* (Wall, 2015, p. 4). È pertanto possibile distinguere i *cyber-assisted crimes*, che si verificherebbero comunque in assenza del mezzo tecnologico, dai *cyberdependent crimes* che, invece, diversamente non esisterebbero. Oltre al livello di mediazione, secondo Wall (2015), è necessario considerare anche il *modus operandi*, differenziando *crimes against the machine (haking)*, *crimes using the machine* (frodi), *crimes in the machine* (incitamento all'odio), nonché volgere uno sguardo sulle implicazioni di natura vittimologica (Wall, 2015).

2. Le mafie italiane[2]

Una prima riflessione, pensando alle peculiarità volte a definire il fenomeno mafioso, potrebbe essere inerente allo stretto rapporto che, fin dalle loro origini, le mafie intrattengono con il proprio contesto territoriale. Il controllo del territorio, lo stretto vincolo che lega le consorterie mafiose all'ambiente sociale è un dato incontrovertibile e costituisce parte della linfa vitale, che alimenta costantemente il potere delle mafie. Come opportunamente concettualizzato da Sciarrone (2009), è possibile comprendere meglio la natura delle organizzazioni criminali di stampo mafioso, intendendo queste ultime come società segrete, che agiscono al fine di ottenere profitti economici, sicurezza e reputazione. Un fenomeno di "società locale", di cui l'estorsione è l'elemento più manifesto, che si origina, nelle sue diverse declinazioni geografiche del mezzogiorno di Italia, in un preciso contesto territoriale, di cui condiziona le dimensioni sociali, politiche ed economiche, e a partire dal quale si riproduce e si diffonde, grazie anche a un consistente capitale sociale, dato dalla creazione di reti relazionali con attori diversi, e dunque alla capacità di *networking*, vale a dire capacità di «allacciare relazioni, instaurare scambi, creare vincoli di fiducia, incentivare obblighi e favori reciproci» (Sciarrone, 2009, p. 51). Un peculiare tipo di criminalità organizzata, quella mafiosa appunto, all'interno del quale si fondono due dimensioni rilevanti: «quella di organizzazione di controllo del territorio, da cui deriva il suo potere e agire politico, e quella di organizzazione dei traffici illeciti, che la caratterizza come impresa che opera a cavallo dei mercati illegali e di quelli legali» (Sciarrone, 2009, pp. 22-23).

Il legame con il territorio di origine, tratto distintivo della criminalità mafiosa, non si indebolisce in seguito alla scelta strategica di espandersi in territori non tradizionali, sia nel resto di Italia sia all'estero. L'elemento della territorialità si accompagna a una straordinaria capacità di adattamento, notoriamente riconosciuta dagli organi investigativi. A tal proposito, nelle ultime relazioni semestrali della Direzione investigativa antimafia[3], si evidenzia come dalle più recenti attività info-investigative emerga un «incessante processo di adattamento alla mutevolezza dei contesti» (DIA, I semestre 2021, p. 406) di tutte le organizzazioni mafiose, che comunque non rinunciano « (…) all'indispensabile radicamento sul territorio e a quella pressione intimidatoria che garantisce la riconoscibilità in termini di "potere" criminale» (DIA, II semestre 2020, p. 402).

È proprio quindi a questa capacità di adattamento, alla dinamicità e alla flessibilità dei sodalizi mafiosi

[2] Il riferimento, in questo articolo, è esclusivamente da intendersi alle mafie endogene tradizionali, in particolare: mafia siciliana, 'ndrangheta e camorra.

[3] In particolare, il riferimento è alle relazioni semestrali del 2020 e alla relazione del 2021 (I semestre) - https://direzioneinvestigativaantimafia.interno.gov.it/relazioni-semestrali/

che bisogna guardare per comprendere se, pur nell'irrinunciabile vincolo che li tiene saldi al contesto sociale, si possano intravedere, in quella dimensione organizzativa inerente ai traffici illeciti, scelte strategiche di ampliamento dei mercati nel cyberspazio.

A tal proposito, la DIA, nella prima relazione semestrale del 2020, evidenzia l'interesse delle mafie verso il mondo del *cybercrime* nonché rispetto alle opportunità offerte dal *darkweb* (DIA, 2020).

Ulteriori evidenze investigative confermano l'attenzione verso alcune possibilità facilitate dalla tecnologia in relazione a settori specifici e ben delimitati quali, per esempio, il gioco d'azzardo e le scommesse *online*, che consentono guadagni ingenti, operazioni di riciclaggio del denaro e rischi contenuti.

Un altro aspetto da non sottovalutare è relativo al pagamento in criptovalute, con particolare riferimento bitcoin e monero, che eludono il monitoraggio bancario. (DIA, II semestre 2020). L'utilizzo illecito delle criptovalute sembra interessare in particolar modo la 'ndrangheta, organizzazione criminale pioniera in tale settore, che avrebbe sviluppato competenze elevate riuscendo a coniugare l'ambito finanziario e quello tecnologico nelle operazioni transnazionali. (Balia, 2020).

Inoltre, l'adattamento al contesto socioeconomico, secondo la DIA, è stato dimostrato anche durante le limitazioni ai movimenti imposte dal governo per il contenimento del covid19, quando i sodalizi criminali hanno adeguato modalità di trasporto e distribuzione degli stupefacenti, utilizzando la pratica del *darknet market*, che prevede la spedizione per posta della sostanza acquistata *online* su mercati stranieri (DIA, II semestre 2020).

Da queste risultanze investigative si potrebbe dunque affermare che le mafie italiane, allargando i loro orizzonti, abbiano conquistato anche il cyberspazio incrementando i loro profitti e specializzandosi anche in mercati virtuali rispetto ai tradizionali più noti, tuttavia il dibattito accademico in relazione a questa presenza ingombrante, anche nella dimensione *online*, porta ad un atteggiamento più cauto e a una riflessione maggiormente complessa.

I gruppi mafiosi sembrano effettivamente aver sviluppato un interesse più settoriale, mostrando, secondo Lavorgna (2015), una certa riluttanza al trasferimento *online* e utilizzando la tecnologia principalmente come strumento di comunicazione, atto ad eludere le intercettazioni telefoniche, non cogliendo pertanto a pieno le opportunità criminali che il mezzo tecnologico potrebbe offrire. Dalle ricerche svolte, in riferimento soprattutto ai gruppi mafiosi in aree tradizionali, emerge che la prevalente ritrosia delle organizzazioni mafiose sia da imputare al fatto che queste, nelle loro configurazioni tradizionali, siano già molto efficienti, inoltre agli apici delle gerarchie è ancora presto per trovare nativi digitali tanto che, presumibilmente, questo ultimo dato tra qualche anno potrà subire dei cambiamenti. Nelle aree non tradizionali, al nord Italia come all'estero, il *modus operandi* adottato dalle organizzazioni mafiose muta ma, in ogni caso, le relazioni nello spazio fisico restano di primaria importanza e servono ad alimentare rapporti di fiducia (Lavorgna, 2015).

Il gioco d'azzardo su internet invece merita una riflessione a parte in quanto, così come riportato anche dalle ultime evidenze investigate della direzione investigativa antimafia, non solo rappresenta un settore molto remunerativo per le mafie che ne utilizzano i canali per il riciclaggio dei proventi illeciti, ma rappresenta altresì l'attività criminale nella quale Internet ha maggiore rilevanza.

È, infatti, un'attività che consente di aumentare i profitti con un rischio relativamente basso senza inficiare la rete di relazioni sociali, perno centrale delle organizzazioni mafiose (Lavorgna, 2015).

I maggiori contributi in materia sottolineano l'importanza di una distinzione, sottovalutata a volte, ritenuta scontata altre, ma fondamentale rispetto alla definizione di criminalità organizzata, che comprende al suo interno realtà eterogenee, tra le quali una tra le più note in Italia è appunto quella di natura mafiosa. Non bisogna però commettere l'errore di assimilare ed equiparare o, più semplicemente, ricondurre, per comodità, la seconda alla prima. La criminalità organizzata di stampo mafioso non può essere ritenuta alla stessa stregua della criminalità organizzata da intendersi in senso lato, comprendente quindi una serie di attività criminali di natura ed entità diversa.

Come suggerisce Lavorgna (2020), il crimine organizzato ha una presenza nel cyberspazio, ma non è opportuno accomunare le reti criminali *online*, responsabili di gravi crimini informatici, e la criminalità organizzata, che necessita di elementi più precisi per essere definita tale.

Non esistono consistenti risultanze empiriche in grado di attestare il trasferimento di attività *online* da parte dei gruppi criminali tradizionali, di spiegare come i gruppi criminali svolgano le loro attività nel cyberspazio oppure se siano emerse *online* attività illecite inedite da parte di nuovi gruppi pertanto la connessione tra criminalità informatica e criminalità organizzata necessita di uno sguardo critico proprio in virtù del fatto che le prove empiriche sono ancora limitate (Lavorgna, 2020).

Come facilmente intuibile, non esiste una definizione condivisa di criminalità organizzata a livello globale, von Lampe, per esempio, ne ha raccolte più di 200 (von Lampe, 2022).

La nozione di criminalità organizzata è fortemente connotata da elementi storici e culturali, che implicano sfumature diverse del fenomeno in relazione al contesto geografico di riferimento, e include al suo interno tipi diversi di criminalità accomunati semmai dall'idea di una più seria minaccia dettata proprio dall'elemento organizzativo delle attività rispetto, per esempio, a una criminalità che possiamo definire non organizzata. Se analizziamo il ruolo della criminalità organizzata nei crimini informatici è necessario distinguere i criminali informatici organizzati, autori di crimini informatici, dai gruppi di criminalità organizzata tradizionali, che si servono della rete perché in grado di facilitare determinati reati (Lavorgna, 2020).

Perché un'organizzazione criminale possa essere definita mafiosa, invece, seguendo un approccio multidisciplinare, non ci si può limitare esclusivamente al dettato normativo, previsto all'articolo 416bis del Codice penale, ma è necessario un approfondimento di natura socio-criminologica. Il dettato normativo certamente chiarisce e definisce i contorni all'interno dei quali è possibile distinguere un'associazione di tipo mafioso. Com'è ormai noto, l'articolo 416bis, introdotto nel nostro Codice penale nel 1982 dalla Legge n° 646, Rognoni-La Torre, per la configurazione del reato prevede alcuni elementi imprescindibili, che classificano un certo tipo di condotta. Gli associati si avvalgono della forza intimidatrice del vincolo associativo nonché della condizione di assoggettamento e di omertà derivanti per commettere delitti, ma anche, per esempio, per acquisire la gestione o il controllo di attività economiche o appalti oppure realizzare profitti o vantaggi ingiusti, senza tralasciare, tra le possibilità, un'illecita ingerenza, volta ad ostacolare il libero

esercizio del voto, o un'interferenza nelle consultazioni elettorali[4].

Per avere un'idea più chiara del panorama criminale italiano, può essere utile riprendere la distinzione, operata da Lavorgna e Sergi (2014) sui tipi criminologici di criminalità organizzata, che contribuisce a comprendere meglio una peculiarità criminale, connotata dall'elemento organizzativo, che non include al suo interno esclusivamente la criminalità di tipo mafioso, sebbene l'Italia continui a mantenere un triste primato rispetto alla pervasività di un fenomeno sistemico e longevo qual è appunto quello mafioso.

Le autrici (Lavorgna, Sergi, 2014) descrivono i contributi degli strumenti giuridici alla definizione del problema partendo da una dimensione internazionale con la Convenzione delle nazioni Unite contro la criminalità organizzata transnazionale[5], sottoscritta a Palermo nel 2000, citando poi la decisione quadro 2008/841/GAI[6] del Consiglio dell'Unione Europea, relativa alla lotta contro la criminalità organizzata, per giungere ad un'analisi dettagliata del quadro giuridico italiano, con particolare riferimento a una disamina relativa agli articoli 416[7], associazione per delinquere, e 416bis[8], associazioni di tipo mafioso anche straniere, del Codice penale. I reati appena menzionati però potrebbero non essere sufficienti a inquadrare specifiche condotte delinquenziali di gruppi, determinando di fatto un vuoto normativo del quale i criminali potrebbero approfittare (Lavorgna, Sergi, 2014). Tenendo ferme tali riflessioni, le Autrici delineano pertanto quattro diversi tipi di gruppi criminali due dei quali, organizzazione criminale "semplice" e criminalità organizzata mafiosa, sono direttamente riconducibili al dettato normativo previsto dai due articoli precedentemente citati (416 e 416bis c.p.). Le restanti due configurazioni riguardano, nel primo caso, reti criminali miste, che possono coinvolgere tanto autoctoni quanto stranieri o entrambi e riguardare connessioni criminali e pericolosità di diversa entità e, nel secondo caso, gruppi con connotazioni mafiose migrati in altri territori cosiddetti non tradizionali. Questa distinzione risulta interessante anche per le implicazioni argomentative di natura socio-criminologica che

[4] Articolo 416bis Codice penale.

[5] Convenzione delle NU contro la criminalità organizzata transnazionale, art. 2: (a) "Gruppo criminale organizzato" indica un gruppo strutturato, esistente per un periodo di tempo, composto da tre o più persone che agiscono di concerto al fine di commettere uno o più reati gravi o reati stabiliti dalla presente Convenzione, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale; (b) "Reato grave" indica la condotta che costituisce un reato sanzionabile con una pena privativa della libertà personale di almeno quattro anni nel massimo o con una pena più elevata;

[6] Decisione quadro 2008/841/GAI relativa alla lotta contro la criminalità organizzata del 24 ottobre 2008. Articolo 1 – definizioni: Ai fini della presente decisione quadro: 1. per «organizzazione criminale» si intende un'associazione strutturata di più di due persone, stabilita da tempo, che agisce in modo concertato allo scopo di commettere reati punibili con una pena privativa della libertà o con una misura di sicurezza privativa della libertà non inferiore a quattro anni o con una pena più grave per ricavarne, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale; 2. per «associazione strutturata» si intende un'associazione che non si è costituita fortuitamente per la commissione estemporanea di un reato e che non deve necessariamente prevedere ruoli formalmente definiti per i suoi membri, continuità nella composizione o una struttura articolata.

[7] Articolo 416 c.p.: Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazion e sono puniti, per ciò solo, con la reclusione da tre a sette anni. Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni. (…)

[8] Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da dieci a quindici anni. Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da dodici a diciotto anni. L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgano della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri, ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali. (…)

determina, in quanto, così come sottolineato dalle Autrici, ciascun gruppo presenta connotazioni differenti, obiettivi eterogenei, un diverso grado di sofisticazione nonché, elemento fondamentale, un rapporto dissimile con la società nella quale il gruppo si trova ad operare e a interagire con gli attori presenti. Le differenti opportunità sociali e le diverse capacità di adattamento dei gruppi criminali implicano reazioni eterogenee di fronte alle innovazioni tecnologiche e ai cambiamenti sociali. Le Autrici ritengono, infatti, che i gruppi identificati come misti possano trarre vantaggi da internet, che non si limita in questo caso a rappresentare un mero strumento di comunicazione, ma può influenzare significativamente determinati mercati criminali, implicando comunque un livello basso di rischio. Esiste però la possibilità che reti di questo tipo, dotate di una maggiore sofisticazione e di un interesse verso attività cosiddette tradizionali, quali per esempio il traffico di sostanze stupefacenti, possano avvalersi di internet per comunicazioni più sicure e possano, diversamente dalle prime, gestire i loro traffici soprattutto nel *deep web*. Un utilizzo analogo potrebbe essere riconducibile anche ai gruppi mafiosi operanti in zone non tradizionali, favorevoli ad intrattenere rapporti con soggetti esterni al sodalizio mafioso, che potrebbero avere competenze tecnologiche specifiche. Sostanzialmente però le opportunità offerte dal *web* non possono sostituire completamente la necessità di stabilire legami fiduciari, basati su interazioni faccia a faccia. A maggior ragione, le organizzazioni mafiose, che nelle zone di origine hanno stabilito forti e irrinunciabili legami con il territorio, non possono certo astenersi da una presenza fisica e, per certi versi, ben visibile che si traduce in un controllo capillare del territorio; pertanto, queste sembrano più riluttanti ad un trasferimento nel cyberspazio. Anche in quest'ultimo caso, a conferma di quanto già precedentemente sostenuto, Lavorgna e Sergi, oltre all'utilizzo di internet come mezzo di comunicazione, menzionano alcuni specifici ambiti di interesse quali, per esempio, il gioco d'azzardo online, ma anche offline purché pubblicizzato su internet e il ricorso ai *social network* per carpire informazioni utili sulle abitudini delle vittime. In questi casi la rete sociale di contatti, risorsa imprescindibile per l'organizzazione, non viene infatti intaccata (Lavorgna, Sergi, 2014).

Un'altra classica distinzione, nota in letteratura, è quella di McGuire (2012) il quale, sulla base delle conoscenze acquisite, ha realizzato una tipologia relativa ai gruppi di criminalità informatica che tiene conto di tre tipi principali, ciascuno con due sottogruppi: il primo gruppo opera esclusivamente *online* (sciami e hub); il secondo è ibrido (raggruppati e estesi) e integra reati *online* o *offline*; il terzo opera prevalentemente *offline* (gerarchie e aggregati), ma utilizza la tecnologia per facilitare le attività criminali. A quest'ultimo gruppo sono riconducibili i gruppi mafiosi, che esportano alcune delle loro attività *online*. L'ambiente sociale digitale di internet e i progressi tecnologici hanno inevitabilmente condizionato la criminalità organizzata, anche di stampo mafioso, che sembra, come già affermato, attiva soprattutto in determinate attività legate, per esempio, al riciclaggio di proventi illeciti o al gioco d'azzardo.

3. Dalle comunicazioni criptate all'esposizione social

Secondo alcuni studiosi (Bijlenga, Kleemans, 2018) i gruppi mafiosi ricorrono al mezzo tecnologico e in particolare a internet semplicemente come strumento comunicativo volto ad eludere le intercettazioni.

A tal proposito si ha un effettivo riscontro anche in recenti operazioni[9], che confermano l'uso di codici crittografati, in questo caso numerici, che rendono più complessa l'attività investigativa. Il mercato dei criptofonini[10] interessa sicuramente le organizzazioni criminali così come confermato da Europol relativamente all'operazione, che ha consentito di smantellare EncroChat, una rete telefonica crittografata. Reti criminali che utilizzano tecnologie avanzate per comunicazioni inerenti alle loro attività criminali quali il traffico internazionale di droga per esempio. Dal comunicato stampa di Europol[11] si apprende che l'azione investigativa ha coinvolto Francia, Paesi Bassi, ma anche Regno Unito, Svezia e Norvegia, nessun riferimento alle mafie italiane, che tuttavia giunge esplicitamente dall'audizione del Prefetto, Vittorio Rizzi, direttore della direzione centrale della Polizia criminale. Nel novembre del 2020, infatti, il Prefetto Rizzi, intervenuto presso la Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere, facendo riferimento all'indagine, coordinata da Europol, della polizia francese e della polizia olandese, con le quali l'Italia sta entrando in partnership, conferma il coinvolgimento della criminalità organizzata italiana, anche di stampo mafioso, nell'uso della piattaforma Encrochat per l'organizzazione di traffici illeciti, soprattutto relativamente al traffico di droga[12] e sottolinea la necessità di prestare maggiore attenzione alle dinamiche del *deep web* e del *dark web*, che costituiscono una reale minaccia transnazionale e una modalità di gestione del narcotraffico e dei pagamenti, che raggiunge elevati livelli di sofisticazione. Nella stessa direzione si muovono le rilevazioni del rapporto CLUSIT[13] di ottobre 2021 nel quale si legge che «Il momento attuale è (…) segnato dalla definitiva presa di coscienza circa l'ingresso delle grandi organizzazioni criminali transnazionali, come pure le principali mafie nazionali, nel crimine informatico, in considerazione delle enormi potenzialità che la rete esprime in ogni senso, anche in termini di realizzazione e moltiplicazione di profitti illeciti» (Clusit, 2021, p. 57).

Le mafie italiane, dunque, restano al passo con l'evoluzione tecnologica utilizzando i medesimi strumenti, come affermato anche dal procuratore nazionale antimafia e antiterrorismo, Federico Cafiero de Raho, che ha definito l'utilizzo di telefoni con protocollo Encrochat e gli apparati con sistema criptato SKY Ecc come una via ordinaria di comunicazione[14].

Le comunicazioni criptate, del resto, ben si attagliano ad organizzazioni mafiose che fondano la loro origine sul vincolo della segretezza che «(…) non solo svolge una funzione di protezione nei confronti dell'esterno, ma serve anche a dare un'immagine di potenza sia agli appartenenti sia a non appartenenti» (Sciarrone, 2009, p. 39) mentre decisamente più bizzarra appare la scelta di

[9] Guardia di finanza Catanzaro, DDA Reggio Calabria – operazione Crypto, settembre 2021; GdF Catanzaro – operazione Molo 13, aprile 2021.

[10] Telefono cellulare tecnologicamente avanzato, dotato di un sistema di cifratura del segnale e di protezione dall'accesso (Treccani.it)

[11] Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

[12] Audizione l'audizione del prefetto Vittorio Rizzi, vicecapo della Polizia di Stato – direttore della Direzione centrale della Polizia criminale, presso la Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere. 4 novembre 2020, disponibile al seguente link: https://www.interno.gov.it/it/notizie/antimafia-audizione-prefetto-vittorio-rizzi-video

[13] Associazione Italiana per la Sicurezza Informatica - Rapporto 2021 sulla Sicurezza ICT in Italia - aggiornamento ottobre 2021 disponibile al seguente link: https://clusit.it/wp-content/uploads/download/Rapporto-Clusit-ottobre-2021_web.pdf

[14] Conferenza stampa Operazione Platinum Dia – 5 maggio 2021

ostentazione *social*, che alcuni affiliati palesano sulle piattaforme *online*.

Nella letteratura internazionale, alcuni studi (Patton *et al.*, 2013; Dmello&Bichler, 2020) hanno indagato l'uso dei social media da parte delle bande di strada, focalizzando l'analisi sul fenomeno culturale dell'*internet banging* o *cyberbanging*, termine usato per descrivere una tendenza riscontrata nel comportamento *online* di soggetti appartenenti a bande statunitensi, che si servono di social media come *Twitter*, *Facebook* e *YouTube* per veicolare determinati messaggi quali minacce, insulti e lanciare sfide sul *web* e che, secondo la stampa locale, presentano alcuni elementi chiave come promuovere l'affiliazione al gruppo o comunicare l'interesse per le attività dello stesso, acquisire notorietà, nonché condividere informazioni sui gruppi rivali o entrare in contatto con altri membri della banda (Patton *et al.*, 2013). Gli autori ritengono che l'evoluzione di tale fenomeno culturale sia dovuta a un maggiore accesso e a una più ampia partecipazione ai social media ed esaminano criticamente il ruolo dell'hip-hop come canale attraverso il quale si verifica il *cyberbanging*.

Nello studio più recente di Dmello e Bichler (2020), l'uso dello spazio digitale da parte delle bande di strada per attività devianti (*cyberbanging*) viene interpretato quale naturale cambiamento nei processi di socializzazione, successivo alla rivoluzione digitale, una migrazione del comportamento dallo spazio fisico a quello *online*. Dalla letteratura analizzata in tale studio, infatti, si può evincere come l'utilizzo dei social media ad opera delle bande di strada sia finalizzato alla promozione del gruppo, alla reputazione, alla condivisione di un certo stile di vita, veicolando determinati messaggi. Profitti illeciti, armi, scelte musicali, mascolinità sono alcuni degli elementi che emergono nella dimensione social e che non escludono, da una parte, campagne di reclutamento, e dall'altra, provocazione e dileggio dei gruppi rivali.

L'obiettivo della ricerca di Dmello e Bichler (2020) è quello di valutare l'impatto delle ingiunzioni restrittive[15] sull'uso dei media *online* con particolare riferimento a *YouTube*, piattaforma tra le più utilizzate dalle *street gangs* negli Stati Uniti e che consente loro di analizzare 128 video prodotti da membri appartenenti a tali bande. Gli autori rilevano che le interazioni nello spazio fisico si riverberano in quello digitale e che i membri della banda sono abili ad eludere i controlli scegliendo la visualizzazione dei contenuti solo per un tempo limitato. Le restrizioni cui sono sottoposte le bande sostanzialmente comportano un trasferimento sullo spazio *online* volto anche a preservare la loro reputazione, ma implicano, da una parte, una maggiore cautela in termini di proiezioni dello stile di vita (ricchezza e reputazione) e, dall'altra, un aumento del loro indice di *branding* (simbolismo, dominio, marcatura del territorio). Pertanto, le limitazioni imposte, sebbene possano avere qualche effetto sulla riduzione della violenza nello spazio fisico, non azzerano l'attività delle bande, ma ne determinano una trasformazione digitale, incidendo sulla rappresentazione e sull'immagine che viene trasmessa (Dmello e Bichler, 2020).

Questi studi presentano delle analogie con la ricerca di M. Ravveduto (2018, 2019) sulla *Google generation* criminale, che analizza l'uso di *Facebook* da parte dei ragazzi affiliati ai clan di camorra. I mafiosi, così come gli altri utenti, sperimentano tre fasi di apprendimento: una prima fase, dal 2007 al 2012, durante la quale si registra un utilizzo ludico del *web*

[15] Gli autori parlano di Civil gang injunctions, CGI. «Civil gang injunctions (CGIs) impose significant behavioral restrictions on individuals, that is, setting curfews, prohibiting free movement, and restricting social activity» (Bichler *et al.*, 2019, p. 876).

non privo di conseguenze indesiderabili dovute alla scarsa dimestichezza con la geolocalizzazione, ma nella quale comincia anche a diffondersi un primo immaginario derivante dalla creazione di gruppi, pagine e profili che celebrano le imprese dei vecchi boss e la potenza delle organizzazioni criminali; nella seconda fase, dal 2012 al 2016, definita di consolidamento, invece è quella in cui «(…) si radica una specifica retorica mafiosa» (Ravveduto, 2019, p. 100) e i giovani camorristi si avvalgono del *socialcasting* per diffondere specifici contenuti; la terza fase, attuale, è quella in cui prevale la cosiddetta *Google generation* criminale, in grado di cogliere al meglio le potenzialità del mezzo tecnologico. Ravveduto si riferisce ad «un processo di acculturazione criminale fondato sullo *sharing online* di modi di dire e di vestire, di posture del corpo da tenere, di armi da usare, di oggetti cult da possedere, di frasi da ricordare, di foto da condividere, di dialoghi da tramandare, di clip da visualizzare» (Ravveduto, 2019, p. 101). Giovani immersi in una dimensione "interreale" dove mondo digitale e reale si influenzano reciprocamente. Questa generazione criminale dei clan di camorra ama l'ostentazione, esibisce un determinato stile di vita, veicola specifici messaggi e richiama la violenza di strada, tipica dei giovani americani, ponendo l'accento sui traffici illeciti (spaccio), sul controllo del territorio, sulla fierezza data dall'appartenenza al gruppo e arriva a riecheggiarne i gusti musicali riconducili all'hip-hop, quest'ultimo elemento confermato dal fatto che, nei loro profili, diminuisce la condivisione di brani neomelodici per lasciare posto alla musica rap e alla trap (Ravveduto, 2019). Le ricerche dell'Autore pertanto confermano non solo l'utilizzo dei social media, che può sembrare scontato dato l'elevato numero di utenti italiani[16] attivi *online*, ma anche una corrispondenza tra l'identità reale e quelle digitale, «l'attivismo social della Google generation criminale esibisce con naturalezza l'orgoglio della propria identità deviante, come un aspetto del tutto normale, all'interno di un ambiente virtuale che ha come scopo la replicazione della vita reale» (Ravveduto, 2017[17]).

4. Conclusioni

Secondo Europol (SOCTA 2021), che distingue diverse reti criminali, la trasformazione digitale continua a progredire rapidamente riverberando i suoi effetti anche sulla criminalità organizzata. Tutte le attività criminali presentano componenti *online*. I mercati criminali, in grado di offrire merci e servizi, si muovono con dimestichezza tra il *surface* e il *dark web* e consentono l'acquisto in criptovalute, che sembra un importante mezzo di pagamento oltre che un mezzo per nuove tecniche di riciclaggio. Inoltre, i social media fungono da canali di *marketing* o di comunicazione per i criminali, che sfruttano la crittografia per scambiare messaggi, contenuti e informazioni sui traffici illeciti (SOCTA, 2021).

Da quanto emerso dall'analisi della letteratura e dalle evidenze investigative, è accertato l'interesse, anche delle mafie italiane, del mezzo tecnologico e del mondo virtuale per facilitare, da una parte, specifiche attività e, dall'altra, per preservare informazioni relative per esempio ai traffici illeciti.

[16] Secondo il Rapporto Digital 2022 (febbraio) in Italia sono più di 43 milioni (71.6%) le persone attive sulle piattaforme social e Facebook, per quanto riguarda gli utenti tra i 16 e i 64 anni, è la seconda piattaforma più utilizzata, dopo WhatsApp. https://wearesocial.com/it/blog/2022/02/digital-2022-i-dati-italiani/

[17] Ravveduto M., "La paranza dei bambini". La Google Generation di Gomorra, in Questione Giustizia, 14 gennaio 2017 https://www.questionegiustizia.it/articolo/la-paranza-dei-bambini-la-google-generation-di-gomorra_14-01-2017.php

Secondo Lavorgna, è necessario distinguere i criminali informatici organizzati che commettono nuovi reati contro le reti di *computer* (*malware*, *hacking*) oppure attraverso un sistema informatico (dal furto di identità alla pedopornografia) dai gruppi di criminalità organizzata tradizionale, che usano internet come facilitatore del crimine. I primi spesso non soddisfano né le definizioni accademiche né quelle legali di criminalità organizzata, enucleate, per esempio, nella Convenzione di Palermo, pertanto, definire le reti criminali nel cyberspazio può implicare ambiguità analitiche (Lavorgna, 2020).

Per quanto concerne la presenza nel cyberspazio di organizzazioni mafiose, date le note capacità di adattamento al mutamento sociale, si può affermare che queste abbiano valutato anche le diverse opportunità offerte da internet. In particolare, però le organizzazioni mafiose, come più volte sottolineato, hanno mostrato interesse in settori specifici quali il gioco d'azzardo *online* che può essere utile per operazioni di riciclaggio, attività di *trafficking online* tuttavia «Overall, the existing empirical evidence suggests that for most mafia-type groups, cyberspace has not significantly changed the social opportunity structure on which they rely» (Lavorgna, 2020, p. 126).

In letteratura il dibattito vede la compresenza di studi che, da una parte, associano i crimini informatici alla criminalità organizzata e, dall'altra, esprimono una posizione più critica rispetto a una specifica corrispondenza tra le due componenti. Tali posizioni, non meramente speculative, possono implicare una diversa allocazione delle risorse e conseguenze differenti in termini di contrasto, di intervento nonché di impatto sull'opinione pubblica e sui media (Lavorgna, 2018).

McGuire (2012), per esempio, come abbiamo visto, realizza una tipologia per descrivere le diverse forme di gruppi che agiscono nel cyberspazio mentre Wall (2015), riprendendo Brenner (2002), condivide l'idea secondo la quale il crimine informatico si manifesterebbe in forme più transitorie e fluide e in termini di reti, differenziandosi in tal modo da modelli strutturati e gerarchici, quali quelli mafiosi, che si evolvono in relazione ad opportunità e vincoli del mondo fisico (Wall, 2015). Le organizzazioni criminali *online* pertanto, secondo Wall, differiscono notevolmente dal modello tradizionale mafioso, ancorato geograficamente e socialmente (Wall, 2015).

La criminalità organizzata di stampo mafioso nel corso del tempo non ha mutato i settori tradizionali di interesse né abbandonato quella peculiare caratteristica che le consente di adattarsi ai mutamenti sociali cogliendo nuove opportunità anche in situazioni di crisi ed emergenza, come recentemente appurato da più fonti a proposito della contingenza pandemica (Santino, 2020; Libera, 2020).

L'avvento della tecnologia e le sue continue trasformazioni, che permeano molti aspetti della vita sociale, non lasciano indifferenti le mafie che tuttavia, come si riscontra in letteratura, hanno finora manifestato un interesse piuttosto settoriale, limitato a determinati ambiti. Le evidenze empiriche non sono abbastanza consistenti per dimostrare un trasferimento *online* di gruppi *offline* preesistenti allo sviluppo tecnologico (Lavorgna, 2020). Pur avvalendosi di internet, i gruppi mafiosi non stanno sfruttando a tutto tondo il cyberspazio per i loro scopi illeciti anche perché, soprattutto nelle zone di origine del fenomeno criminale sistemico, il controllo del territorio, il presidio assiduo, la presenza fisica e visibile diventano elementi imprescindibili per garantire potere e longevità all'organizzazione.

Non si può dunque pensare a organizzazioni mafiose «liquide e immateriali» come afferma Cornelli (2013), il quale rimarca anche che la mafia «(…) mira a governare i processi economici locali, è radicata in un territorio definito che protegge e controlla, ha un rapporto continuativo con il sistema politico (…). Il loro vero punto di forza è costituito proprio dal "potere territoriale" (…)» (Ceretti, Cornelli, 2013, pp. 142-143).

Questo panorama, così delineato, non rispecchia però una realtà immutabile ma, anzi, proprio in virtù della natura transitoria e mutevole, perché in continua trasformazione, delle tecnologie dell'informazione e data la straordinaria capacità di adattamento delle mafie italiane saranno necessari ulteriori approfondimenti e studi, corroborati dalla ricerca empirica, per comprendere in quale direzione orientare risorse e interventi.

Bibliografia

1. Bichler G., Norris A., Dmello J., Randle J., «The Impact of Civil Gang Injunctions on Networked Violence Between the Bloods and the Crips», *Crime and Delinquency* 65.7, 2019, pp. 875-915.
2. Bijlenga N., Kleemans E.R. «Criminals Seeking ICT-expertise: An Exploratory Study of Dutch Cases», *European Journal on Criminal Policy and Research* 24, 2018, pp. 253-268.
3. Broadhurst R., Grabosky P., Alazab M., Chon S. «Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime», *International Journal of Cyber Criminology* 8.1, 2014, pp. 1-20.
4. Ceretti A., Cornelli R., *Oltre la paura*, Feltrinelli, Milano, 2013.
5. Dmello J.R., Bichler G. «Assessing the Impact of Civil Gang Injunctions on the Use of Online Media by Criminal Street Gangs». *International Journal of Cyber Criminology* 14.1, 2020, pp. 44-62.
6. 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», *International Journal of Law, Crime and Justice* 42.1, 2014, pp. 16-32.
7. Lavorgna A. «Organised Crime Goes Online: Realities and Challenges», *Journal of Money Laundering Control* 18.2, 2015, pp. 153-168.
8. Lavorgna A., Sergi A. «Serious, Therefore Organised? A Critique of the Emerging Cyber-Organised Crime" Rhetoric in the United Kingdom» *International Journal of Cyber Criminology* 10.2, 2016, pp. 170-187.
9. Lavorgna A., «Cyber-organised Crime. A Case of Moral Panic? », *Trends in Organized Crime* 22.4, 2018, pp. 357-74.
10. Lavorgna A., «Organized Crime and Cybercrime», in Holt T.J, Bossler A.M., *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, London, 2020, pp. 117-34.
11. 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», *European Journal on Criminal Policy and Research* 23.3, 2016, pp. 287-300.
12. Macilotti G., *Pedopornografia e tecnologie dell'informazione devianza e controllo sociale nella realtà italiana e francese*. Franco Angeli, Milano, 2018.
13. McGuire M., *Organized Crime in the Digital Age*. John Grieve Centre for Policing and Security & Detica, London, 2012.
14. Musotto R., Wall D.S., «More Amazon than Mafia: Analysing a DDoS Stresser Service as Organised Cybercrime», *Trends in Organized Crime* 25.2, 2020, pp. 173-91.
15. Patton D.U., Eschmann R.D., Butler D.A. «Internet Banging: New Trends in Social Media, Gang Violence, Masculinity and Hip Hop», *Computers in Human Behavior* 29.5, 2013, pp. A54-59.
16. Ravveduto M., «La Google generation criminale: i giovani della camorra su Facebook», V. 4 N. 4 (2018) *Rivista di Studi*

e Ricerche Sulla Criminalità Organizzata, pp. 57-78
17. Ravveduto M., *Lo spettacolo della Mafia. Storia di un immaginario tra realtà e finzione*, Edizioni Gruppo Abele, Torino, 2019.
18. Santino S., «Appunti sulla questione criminale, la pandemia e lo stato d'eccezione», in Ciattini A., Pirrone M.A., *Pandemia nel capitalismo del XXI secolo*, PM edizioni, Verazze (Savona), 2020, pp. 139-162.
19. Sciarrone R., *Mafie vecchie, mafie nuove. Radicamento ed espansione*. Donzelli, Roma, 2009.
20. Wall D., «Dis-organised crime: towards a distributed model of the organisation of cybercrime». *The European Review of Organised Crime* 2(2), 2015, pp. 71-90.

Sitografia

1. Balia E., «L'uso delle criptovalute nelle attività internazionali della 'ndrangheta», Centro studi internazionali disponibile al seguente link: https://www.cesi-italia.org/it/articoli/luso-delle-criptovalute-nelle-attivita-internazionali-della-ndrangheta
2. Europol, European Union serious and organised crime threat assessment (SOCTA) 2021: a corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, 2021, https://data.europa.eu/doi/10.2813/346806
3. Libera Associazioni, nomi e numeri contro le mafie e Lavialibera (a cura di), La tempesta perfetta. Le mani della criminalità organizzata sulla pandemia, 2020, https://www.libera.it/documenti/schede/la_tempesta_perfetta_web_chiuso3_12.pdf
4. Rapporto Clusit 2021 (ottobre) sulla sicurezza ICT in Italia, disponibile al seguente link: https://clusit.it/wp-content/uploads/download/Rapporto-Clusit-ottobre-2021_web.pdf
5. Ravveduto M., «"La paranza dei bambini". La Google Generation di Gomorra», *Questione Giustizia*, 14 gennaio 2017 https://www.questionegiustizia.it/articolo/la-paranza-dei-bambini-la-google-generation-di-gomorra_14-01-2017.php
6. Relazione del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia (II semestre 2020; I semestre 2021), disponibili al seguente link: https://direzioneinvestigativaantimafia.interno.gov.it/relazioni-semestrali/
7. Von Lampe K., Definitions of Organized Crime, in www.organized-crime.de/organizedcrimedefinitions.htm