Rivista di Criminologia, Vittimologia e Sicurezza

Organo ufficiale della

Società Italiana di Vittimologia (S.I.V.)

World Society of Victimology (WSV)

Affiliated Journal

Anno XVI Gennaio-Dicembre 2022

Numero Unico

Numero curato da Giorgia Macilotti e Sandra Sicurella

Rivista di Criminologia, Vittimologia e Sicurezza

Rivista quadrimestrale fondata a Bologna nel 2007
ISSN: 1971-033X
Registrazione n. 7728 del 14/2/2007 presso il Tribunale di Bologna

Redazione e amministrazione: Società Italiana di Vittimologia (S.I.V.) - Via Sant'Isaia 8 - 40123 Bologna – Italia; Tel. e Fax. +39-051-585709; e-mail: augustoballoni@virgilio.it

Rivista peer reviewed (procedura double-bind) e indicizzata su:
Catalogo italiano dei periodici/**ACNP**, Progetto **CNR SOLAR** (Scientific Open-access Literature Archive and Repository), directory internazionale delle riviste open access **DOAJ** (Directory of Open Access Journals), **CrossRef, ScienceOpen, Google Scholar, EBSCO Discovery Service, Academic Journal Database, InfoBase Index**

Rivista di Criminologia, Vittimologia e Sicurezza

ISSN 1971-033X
Anno XVI, Numero Unico
Gennaio-Dicembre 2022

INDICE

Editoriale

Il sapere criminologico tra rischi e opportunità

Le savoir criminologique entre risques et opportunités

Criminological knowledge between risks and opportunities

*Augusto Balloni**

Nell'ambito di questo numero della Rivista sono affrontati argomenti riguardanti soprattutto particolari aspetti dei delitti non convenzionali.

Questi ultimi richiedono una particolare attenzione poiché si manifestano con una frequenza tale da creare una sempre maggiore consapevolezza dei danni che provocano. Infatti, i crimini cibernetici investono, oltre alla pubblica amministrazione, anche il settore delle piccole e medie industrie, danneggiando servizi pubblici, in particolare l'approvvigionamento energetico, il settore sanitario e quello scolastico, le comunicazioni, i tarsporti e la finanza sistemica.

Nel settore privato i danni causati dal cybercrime investono soprattutto il settore bancario e quello degli intermediari finanziari.

Le frodi online e i cosiddetti *financial cybercrime* attraggono la criminalità organizzata che può realizzare profitti illeciti riuscendo ad accedere, per esempio, anche a forme di riciclaggio cibernetico su scala internazionale.

La rete è poi diventata il terreno virtuale attraverso cui il terrorismo e la violenza politica possono diffondere ideologie, reclutare e radicalizzare i propri adepti, promuovendo azioni dimostrative e criminose.

Attraverso le nuove tecnologie, con la realizzazione di crimini particolarmente odiosi, si può giungere a ledere la sfera giuridica personale aggredendo la reputazione e la riservatezza degli individui e recando grave

*Presidente Società Italiana di Vittimologia, neuropsichiatra, medico legale, psicologo, già professore ordinario di criminologia all'Università di Bologna.

nocumento alla qualità della vita e all'incolumità dei cittadini.

In tal senso, basti pensare ai numerosi episodi che vedono coinvolti giovani sempre più attratti e soggiogati dall'idea di vivere uno stato di eccitazione perpetua, febbrile, intossicandosi di stimoli senza preoccuparsi di dar loro un senso.

In tale prospettiva si collocano i contributi contenuti in questo numero della Rivista, sollecitati e curati con encomiabile attenzione e impegno dalle professoresse Giorgia Macilotti e Sandra Sicurella. Le curatrici, sulla scorta delle loro esperienze didattiche e di ricerca, hanno proposto indagini e riflessioni riguardanti possibili approcci per l'interpretazione di varie forme di criminalità e per la prevenzione della vittimizzazione nelle sue più variegate manifestazioni. Uno degli aspetti che caratterizza i contributi contenuti in questo numero è certamente l'attenzione che gli Autori hanno, secondo modalità diverse, rivolto ad una serie di fattori, legati sia alle caratteristiche di personalità che agli aspetti relazionali e sociali, utili per prevenire i rischi di vittimizzazione.

In tal senso, sono sicuramente da considerare le esperienze infantili e i vissuti ad esse collegati, le pratiche educative, la tolleranza alle frustrazioni, le capacità di *coping* e di *problem solving*.

In ambito giovanile e non solo, Internet e i nuovi media sono piazze virtuali di incontro: non si tratta solo di mezzi di comunicazione che si aggiungono ai vecchi, ma la novità di questi circuiti e la loro pervasività ha ristrutturato la costruzione della conoscenza, la percezione di sé, i rapporti interpersonali. Tutto l'insieme di queste tecnologie rappresenta un contesto privilegiato dei giovani d'oggi rispetto alle generazioni del passato, un luogo di incontro e di comunicazione che si sottrae al controllo degli adulti, come è successo per ogni generazione di giovani, alla ricerca di uno spazio proprio in cui parlare indisturbati. È evidente la necessità di trovare un equilibrio tra l'esigenza di un accesso sempre più ampio e la sicurezza; tra le dinamiche di espressione di sé e la tutela della privacy, tra i rischi e le opportunità.

Il ruolo del criminologo sarà allora quello di essere latore e interprete di un sapere il cui contributo al perseguimento di politiche migliori consisterà nell'indirizzare tali conoscenze verso tematiche di pubblico interesse. Ciò significa che il bene comune che la criminologia dovrebbe promuovere, dall'innalzamento del livello di sicurezza alla riduzione del crimine, alla protezione delle libertà individuali può realizzarsi soltanto a partire dalla consapevolezza che esistono tre differenti modi di produzione della conoscenza criminologica: quello della scoperta, legato principalmente alla conoscenza circa le dinamiche criminose e le loro motivazioni, quello connesso alla dimensione critica-istituzionale che implica il coinvolgimento del criminologo, quale specialista che persegue e sostiene una politica atta a migliorare la prevenzione del crimine ed infine quello legato alla dimensione normativa che esige una riflessione sul significato di giustizia e sul ruolo della legge.

doi: 10.14664/rcvs/240

Criminalità e cyberspazio, alcune riflessioni in materia di cybercriminalità

Criminalité et cyberespace : quelques réflexions sur la cybercriminalité

Criminality and cyberspace: some reflections on cybercrime

*Maurizio Tonellotto**

Riassunto
Lo sviluppo tecnologico avvenuto negli ultimi anni ha trasformato la società in uno "spazio iperconnesso" determinando terreno fertile per la proliferazione di nuove forme di criminalità. In questo articolo si vogliono delineare gli aspetti salienti della criminalità nel cyberspazio attraverso un approccio socio-criminologico con un'analisi del quadro teorico di riferimento ed uno sguardo alla normativa nazionale ed europea. Saranno poi presentate alcune riflessioni in merito agli attori coinvolti in questi nuovi scenari, evidenziando la necessità di dover elevare gli standard di sicurezza e di scambio informativo ma anche di consapevolezza e conoscenza degli strumenti e delle tecnologie da parte di chi quotidianamente ne fa largo utilizzo.

Résumé
L'évolution technologique de ces dernières années a transformé la société en un "espace hyper-connecté", tout en créant un terrain fertile pour l'émergence de nouvelles formes de criminalité. À partir d'une perspective socio-criminologique, cet article vise dans un premier temps à décrire les principaux aspects de la criminalité dans le cyberespace en proposant une analyse des approches théoriques en la matière et quelques réflexions sur législation nationale et européenne. Ensuite, l'attention sera focalisée sur les acteurs impliqués dans ces nouveaux scénarios, en soulignant notamment la nécessité de renforcer les standards de sécurité, l'échange d'informations mais aussi la sensibilisation et la connaissance des technologies par ceux qui en font un usage quotidien.

Abstract
The development of information technologies in recent years has transformed our society into a "hyper-connected space" in which the pitfalls, the risks as well as the damages to the victims have grown exponentially, developing new forms of crime. This article aims to outline the aspects of crime in cyberspace through a socio-criminological approach with an analysis of the theoretical framework and a look at national and European legislation. Some reflections on security will then be presented on the actors involved in new scenarios, highlighting the need to raise the security standards and data and information exchange but also of awareness and knowledge of tools and technologies by those who daily use them extensively.

Key words: criminalità informatica, cyber-criminologia, sicurezza informatica, NIS, hacking

* Dottore di Ricerca in Sociologia, professore a contratto presso l'Università di Bologna.

1. Introduzione

Lo sviluppo tecnologico avvenuto negli ultimi anni ha trasformato la nostra società in uno spazio iperconnesso dove progressivamente buona parte delle attività si sono spostate verso scenari virtuali. In questo senso parafrasando Hobsbawm[1], gli ultimi trent'anni potrebbero essere definiti come "il secolo brevissimo": sistemi di comunicazione mobili, dispositivi *smart* sempre connessi, gps, sistemi domotici, IoT e assistenti vocali, hanno radicalmente cambiato il nostro quotidiano, riducendo le distanze, velocizzando le interazioni, sviluppando nuove opportunità di *business* e definendo altrettante nuove dinamiche sociali[2]. Il cyberspazio, lo *spazio-non-spazio*, astrattamente può essere immaginato come sviluppato su tre livelli distinti. Alla base, lo strato tecnologico che ne garantisce i confini ed il funzionamento: è in costante divenire e risponde alle necessità del mercato, dei governi, delle multinazionali e degli attori che fruiscono dei servizi proposti. Al vertice vi è lo strato di *governance*, un livello strategico dove attori istituzionali e privati ne definiscono le regole ed i limiti, sviluppando nuovi mercati, programmi economici o politici. È il livello di appannaggio dei governi e delle società *high tech*. In questo livello coesistono ed interagiscono soggetti pubblici e privati, attori che cooperano e competono sul mercato, definendo l'offerta ma anche attivando meccanismi di desiderio sul consumatore finale, sviluppando modalità di risposta innovative per generare nuove domande e, in taluni casi, anche limitandone l'accesso attraverso politiche censorie che incidono sulla fruibilità dei servizi e sulle libertà individuali. Lo strato intermedio, quello sociale, è lo spazio non fisico dei fruitori (consumatori?) dei servizi offerti: vengono svolte le molteplici attività, siano esse produttive, di comunicazione, condivisione e scambio informativo ma anche ludiche; a questo livello avvengono tutte quelle continue interazioni necessarie ed ormai indispensabili per il quotidiano (Tonellotto, 2020).

Tre strati paralleli in continua interazione tra loro. Qualsiasi modifica all'interno di un determinato livello ingenera un *feedback* immediato ed un adattamento ancora più rapido nei restanti. Il crimine, in questo dominio, può essere considerato un elemento di rottura, un *breakdown*; un collasso delle interazioni, che si riflette su ogni singolo strato. La mancanza di una delimitazione spaziale e la speditezza delle interazioni produce, in tal senso, minacce globali e troppo spesso indifferenti dai confini nazionali. Il crimine informatico può determinare processi di vittimizzazione con effetti a lungo termine, può essere diretto indifferentemente verso persone, infrastrutture, istituzioni, imprese o governi, provocando effetti devastanti anche sulle economie nazionali. L'interconnessione dei sistemi di informazione e comunicazione e la natura globale ed a-territoriale del cyberspazio richiedono un costante impegno ed una continua ed incessante cooperazione internazionale per affrontare in maniera concertata le sfide, calmierare i rischi e contrastare gli effetti della criminalità.

Il cyberspazio presenta elementi innovativi e unici che producono terreno fertile allo sviluppo di nuove forme di criminalità. Innanzitutto le reti

[1] Lo storico britannico Eric Hobsbawm nel suo *Il secolo breve. 1914-1991: l'era dei grandi cataclismi*, ed Ita. Rizzoli 2014, espone la tesi che il periodo compreso fra la prima guerra mondiale ed il crollo dell'Unione Sovietica presenti un carattere coerente che, pur non coincidendo con il ventesimo secolo, ne rappresenti la parte fondamentale.

[2] Sono passati poco più di 30 anni dal primo collegamento italiano a quella che verrà chiamata rete Internet. Il 30 Aprile del 1986 dai laboratori di Pisa del CNUCE-CNR (Centro universitario per il calcolo elettronico), viene inviato il primo pacchetto ICMP (Ping) dall'Italia con destinazione Roaring Creek, in Pennsylvania (USA), pochi instanti dopo dagli Stati Uniti arrivò la risposta "Ok", dando così formalmente vita al primo nodo della rete Internet in Italia.

informatiche, Internet tra tutte, riducono anche se in maniera virtuale, le distanze tra una enorme molteplicità di utenti con estrema rapidità d'azione, semplicità ed economicità. Si stima che ad oggi siano circa 5,2 miliardi gli utenti connessi alla rete Internet, ciò significa che il 65,6% della popolazione mondiale è *online* e, con un tasso di crescita annuo pari a 1,35%, oltre 1 milione di nuovi utenti si uniscono alla rete ogni singolo giorno (Internet WorldStats, 2021). Sono invece oltre 10 miliardi i dispositivi mobili collegati alla rete in tutto il mondo, numero che supera abbondantemente l'attuale popolazione mondiale stimata in 7,9 miliardi (GSMA Intelligence, 2021). Lo studio di Datareportal (2019) ha evidenziato come tre quarti degli utenti di Internet effettuano almeno un acquisto *online* ogni mese e il numero di utenti che acquista esclusivamente attraverso dispositivi mobili è in rapidissimo aumento. Solo nel 2018, oltre 2,8 miliardi di persone hanno acquistato beni di consumo, generi alimentari o elettrodomestici *online*, con un incremento di crescita del 3% rispetto all'anno precedente. Si stima poi che la quantità di denaro destinata al mercato dei beni di consumo online superi 1,75 trilioni di dollari all'anno (Datareportal, 2019).

È ormai assodato come solo pochissime aziende attualmente non facciano uso di tecnologie cablate per la produzione di beni o servizi e sicuramente nessun ente governativo al mondo è isolato dalla rete o è avulso dai servizi IT. Le nuove tecnologie sono diventate accessibili a tutti, anche a persone che non hanno particolari competenze tecniche.

2. Criminologia e cybercriminologia: un approccio teorico allo studio della criminalità nel cyberspazio

Prima di analizzare gli aspetti fenomenologici del *cybercrime*, appare necessario definire a livello teorico la criminogenesi del comportamento deviante all'interno della società dell'informazione. É stato evidenziato come il modello proposto da Cohen e Felson (1979) nella teoria delle attività abituali possa essere applicabile, con i necessari adattamenti, anche al contesto adimensionale del cyber spazio (Eck, Clark, 2003; Junger *et al.*, 2017). Il modello nella sua elaborazione originaria prende spunto dagli approcci culturali proposti nella tradizione della Scuola di Chicago, che postulano una convergenza tra crimine, momento dell'azione e spazio. Individuando dunque un elemento di contatto o un legame diretto tra aggressore, vittima e azione deviante (Shaw, McKay 1942; Eck, Weisburd, 1995). Alcuni autori forniscono una critica all'applicazione del modello proposto da Cohen e Felson nell'ambito del crimine informatico, rilevando come il momento dell'azione sia caratterizzato dall'assenza di contatto diretto tra criminale e vittima e secondariamente, evidenziando una asincronia temporale tra azione deviante e le sue conseguenze (vittimizzazione) (Reyns, *et al.* 2011).

Eck e Clarke (2003) sono stati tra i primi a rilevare tale eccezione nell'applicazione del modello di Cohen e Felson in uno spazio fluido quale può essere definita la rete internet: luogo dove il tempo e lo spazio sono relativi. La lacuna, sostenevano, si evidenzia a meno di definire le reti come spazi integrati e dunque concepiti come luoghi compositi: uno spazio, almeno in senso simbolico, in cui il trasgressore e la vittima si incontrano per procura, in maniera mediata dalla tecnologia, ma con sufficiente profondità di contatto, per applicare correttamente il modello delle attività di routine (Arntfield, 2015, p. 375). È bene ricordare come il modello proposto da Cohen e Felson presuppone che per la realizzazione di un'azione deviante sia

necessario che sussistano contemporaneamente tre condizioni minime, in assenza delle quali il crimine non si può consumare. Tali condizioni contemplano la presenza di una persona disposta a compiere l'azione, il criminale, l'attore deviante; un bersaglio appetibile, sia esso un bene da danneggiare, sottrarre ovvero un individuo da aggredire e, in ultimo ma fondamentale, l'assenza di un guardiano in grado di impedire tale condotta (Cohen, Felson, 1979). Il concetto di guardiano non deve essere ricondotto esclusivamente a quello di agenzia di controllo formale poiché questa funzione può essere esercitata sia da un soggetto che applica un controllo sociale informale sia, in maniera più generale, da un vincolo fisico o da una barriera efficace che si interpone a protezione del bene oggetto di interesse per il criminale. L'assenza di uno solo di questi elementi comporterà l'attuazione della condotta criminale. In base a tale approccio teorico un gruppo sociale o una singola persona, risulta a rischio di vittimizzazione quando si situa nelle vicinanze di un criminale potenziale, criterio di prossimità, costituisce un bersaglio interessante dal punto di vista economico o simbolico, criterio di remunerativà, e non è sufficientemente protetto, criterio di accessibilità (Scarscelli, Vidoni Guidoni, 2008). Nell'ambito dei crimini informatici queste tre condizioni si verificano con estrema frequenza. Si può infatti affermare come il bene appetibile, oggetto di attenzione da parte di attori devianti, sia costituito dal "dato", inteso nella sua accezione più ampia, quale singolo elemento computazionale che incorpora in sé il valore stesso dell'informazione: dato personale, finanziario, sanitario, segreto industriale o scientifico; ma anche come porzione di codice sorgente, software, che consente la gestione di dispositivi connessi alla rete, permettendo o impedendo determinate operazioni. È dunque il "dato" che, nella società dell'informazione, assume un valore incommensurabile ed una appetibilità tale da creare la necessità di domanda negli ambienti criminali. La frequente assenza di adeguati guardiani (*gatekeepers*) intesi come tecnologie e/o persone tecnologicamente preparate e l'enorme disponibilità di vittime "poco" consapevoli genera le necessarie condizioni per la realizzazione dell'azione criminale stessa.

L'analisi eziologica della criminalità informatica si può altresì inquadrare all'interno delle teorie della scelta razionale, nel più ampio paradigma criminologico della Scuola Classica, con particolare riferimento alla teoria economica sulla criminalità di Becker (1968). I teorici della scelta razionale individuano come un'azione venga considerata razionale quando l'attore sociale, di fronte a diversi corsi d'azione, intraprende quella che a suo giudizio fornirà il risultato migliore. In tal senso l'atto deviante diviene quel comportamento razionale che appare all'attore la scelta più adeguata a raggiungere i propri fini (Elster, 1993). La teoria economica del comportamento criminale considera quindi il deviante al pari di un consumatore all'interno del libero mercato (Becker, 1968). Il criminale in tal senso viene definito come quell'attore razionale mosso dal desiderio di massimizzare il proprio benessere.

Becker sintetizza la teoria economica del comportamento criminale attraverso l'ormai nota formulazione $Oj = Oj(pj, fj, uj)$, dove il numero dei reati commessi (O) da una persona in un particolare momento (j) è funzione della probabilità (p) di essere individuato, arrestato e condannato per il suo comportamento, della sanzione (f) prevista per quella tipologia di reato e da altra variabile cumulativa (u). Quest'ultima individua ad esempio l'utilità derivante dallo svolgimento di attività legali

o di attività non conformi, ma anche la volontà stessa di commettere quello specifico atto illegale (Becker, 1968). In base a quanto postulato da Becker, un aumento della probabilità (p) di essere individuato, ma anche un incremento dell'entità della sanzione (f) a seguito di condanna, produce la riduzione dell'utilità attesa nel compiere l'azione criminale.

Si deve considerare come il crimine informatico sia ontologicamente caratterizzato da una elevata rapidità nell'azione e da una forte componente di anonimato, oltre che da confini labili e frastagliati che limitano la possibilità di una rapida identificazione del criminale ed una adeguata e pronta azione di contrasto. La quasi totale assenza di una armonizzazione delle norme di diritto sostanziale a livello internazionale e le difficoltà operative di collaborazione tra forze di polizia di differenti paesi incide oltremodo sulla buona riuscita delle attività investigative, con una conseguente ricaduta a livello giudiziario.

Recenti studi sui fattori causali della criminalità nel cyberspazio hanno poi evidenziato che l'analisi della fenomenologia dei reati informatici necessita di una nuova e più ampia lettura in termini teorici. Jaishankar (2008) considera la criminalità informatica come una nuova forma di criminalità che si sviluppa in uno *spazio-non-spazio*, il cyberspazio appunto, che presenta caratteristiche e peculiarità differenti da quello che viene considerato lo spazio fisico (Jaishankar, 2007a, 2008). Il criminologo indiano proponendo la "*Space Transition Theory of Cyber Crime*" evidenzia come l'analisi di questa nuova tipologia di criminalità non può prescindere da sette postulati fondamentali, colonne portanti di quella che Egli definisce la "*Cybercriminology*": una nuova sub-disciplina inserita all'interno della più ampia cornice teorica della Criminologia[3]. La *Cybercriminology* o cybercriminologia viene intesa dallo studioso come "lo studio causale del crimine che si sviluppa nel cyberspazio ma che ha ricadute nello spazio fisico" (Jaishankar, 2007a, p. 1).

Jaishankar osserva come il comportamento delle persone possa subire variazioni nel passaggio tra lo spazio fisico e quello virtuale. La *Space Transition Theory* è concepita quindi come la teoria che vuole evidenziare il mutare del comportamento del singolo soggetto nel passaggio tra lo spazio fisico e lo spazio cibernetico. Lo studioso rileva infatti che le persone che presentano un comportamento criminale represso all'interno dello spazio fisico abbiano la propensione a commettere azioni criminali nel cyberspazio, azioni che non avrebbero commesso nel mondo reale a causa del loro *status* o della loro posizione sociale. Jaishankar introduce poi il concetto di «*Identity Flexibility*», identità flessibile, inteso come un anonimato dissociativo tipico del cyberspazio, che comporta una mancanza di deterrenza nel passaggio tra lo spazio fisico e lo spazio virtuale, con conseguente propensione alla commissione di azioni devianti (Jaishankar, 2008). Il cyberspazio è quindi da considerarsi un nuovo *locus commissi delicti* all'interno del quale l'anonimato

[3] I sette postulati fondamentali proposti da Jainshnkar sono: "1.Persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position; 2.Identity Flexibility, Dissociative Anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cyber crime; 3.Criminal behavior of offenders in cyberspace is likely to be imported to physical space which, in physical space may be exported to cyberspace as well; 4.Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape; 5.Strangers are likely to unite together in cyberspace to commit crime in the physical space; (5b) Associates of physical space are likely to unite to commit crime in cyberspace; 6.Persons from closed society are more likely to commit crimes in cyberspace than persons from open society; 7.The conflict of Norms and Values of Physical Space with the Norms and Values of cyberspace may lead to cybercrimes" (Jaishankar, 2007b, p.7).

produce un effetto inibitorio favorendo l'azione criminale[4].

3. Cosa si intende per cybercriminalità?

La multidisciplinarità che caratterizza lo studio dei fenomeni riguardanti la criminalità informatica, l'assenza di contatto tra criminale e vittima, l'evidente asincronia causa-effetto che impone una rimodulazione del concetto di spazio e di tempo comporta, dal punto di vista teorico, alcune disambiguità definitorie il cui risultato, talvolta, può limitare il campo d'analisi. La rapida evoluzione tecnologica e la sempre più stretta convergenza tra dispositivi elettronici e le reti di comunicazione hanno modificato nel tempo il concetto di criminalità, al punto tale che difficilmente una qualsiasi indagine criminale possa risultare scevra dalle evidenze digitali. Termini quali *computer crime*, *computer related crime*, *hight tech crime* o *net crime* vengono spesso utilizzati in letteratura per descrivere la medesima fenomenologia che vede coinvolti a vario titolo dispositivi e competenze ad alto impatto tecnologico. Numerosi autori, Clough (2010) tra tanti, ritengono che il termine più appropriato da utilizzare per definire tale fenomenologia criminale sia quello di *cybercrime*, richiamando per altro la nota classificazione a tre livelli fornita dal *US Departement of Justice* (US DOJ, 1997), che individua il *cybercrime* come quell'insieme di azioni criminali dove il computer o le reti di comunicazione possono essere l'obbiettivo dell'azione, lo strumento per poter attuare tale attività, ma anche tutte quelle situazioni nelle quali i dispositivi o le reti possono intervenire incidentalmente nell'attuazione o definizione dell'attività criminale. Ad oggi infatti, l'analisi delle tracce digitali permette di acquisire elementi di prova talvolta fondamentali per sviluppare nuovi approcci investigativi o proporre ipotesi accusatorie, anche in circostanze dove le tecnologie intervengono in maniera meramente marginale rispetto al fatto reato per cui si procede. Ne è un esempio l'analisi dei dati presenti nei tabulati telefonici, dei dispositivi gps, dei varchi autostradali, delle telecamere di sicurezza o delle connessioni alla rete, funzionali all'individuazione di un soggetto autore di un crimine comune (Tonellotto, 2015). La classificazione tripartita del Dipartimento di Giustizia americano si può riassumere perciò come *computer crimes*, *computer-facilitates crimes* e *computer-supported crimes* (Clough, 2010, p.10).

Il Consiglio d'Europa all'interno della Convenzione sul *Cybercrime* fatta a Budapest nel 2001, pur non fornendone una definizione puntuale, individua con il termine *cybercrime* tutte quelle attività criminali che possono incidere sulla sicurezza dei dati o sulle reti, ma anche quelle azioni che ledono il *copyright*, che favoriscono frodi tramite dispositivi elettronici ed in fine che abbiano come finalità lo sfruttamento sessuale di minori attraverso la rete.

Nella sintesi iniziale della norma viene evidenziato come "La Convenzione è il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche, e tratta in particolare le violazioni dei diritti d'autore, la frode informatica, la pornografia infantile e le violazioni della sicurezza della rete. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Il suo obiettivo principale,

[4] Anche se per l'economia di questo articolo ci si riferisce esclusivamente all'approccio teorico di Jaishankar sulla cybercriminologia, è bene rilevare come l'influenza dell'anonimato sulla propensione al delinquere nel cyberspazio non sia un concetto nuovo, già altri autori in precedenza hanno rilevato come tale fattore riduca uteriormente il legame empatico autore-vittima favorendo quindi azioni devianti, *ex multis* Suler (2004), Saponaro e Prosperi (2007).

enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cyber criminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale."[5] (CoE, 2011).

Lo scopo della Convenzione è quello di fornire un'armonizzazione delle norme di diritto sostanziale e di diritto processuale, al fine di garantire una cooperazione internazionale per contrastare il cybercrime. La norma, in apertura, presenta definizioni che riassumono il complesso delle attività criminali che rientrano nel novero dei reati informatici. In particolare si evidenziano: a) i reati contro la riservatezza, l'integrità e la disponibilità dei dati, che contemplano l'accesso abusivo a sistema informatico, le intercettazioni non autorizzate, l'interferenza illecita su dati, programmi o sistemi informatici; b) i "*computer related crime*", che definiscono i concetti di falsificazioni informatiche e le frodi; c) i reati cd. di "contenuto", associati alla produzione, diffusione e detenzione di materiale pedopornografico; d) i reati connessi alla violazione del diritto d'autore.

Gordon e Ford (2006) in maniera più ampia definiscono invece *cybercrime* "qualsiasi reato che è stato agevolato o commesso utilizzando un computer, una rete o un dispositivo hardware"[6] (Gordon & Ford, 2006 p. 2) in quanto, secondo il modello proposto, l'offesa può essere posta in essere sia su un computer, *computer alone,* sia nei confronti di qualsiasi altro luogo "non virtuale", *non-virtual location*. In tal senso il dispositivo hardware può essere considerato l'attore del crimine, *agent of crime*, lo strumento che agevola il crimine, *facilitator of the crime* ovvero, l'obbiettivo stesso della condotta criminale, *objective of the criminal conduct*. Gli studiosi poi individuano due tipologie di *cybercrime* che definiscono come Tipo I e Tipo II. La criminalità informatica di Tipo I dal punto di vista vittimologico è generalmente un evento singolare, spesso posto in essere utilizzando programmi malevoli (virus, malware, rootkit, ecc.) che sfruttano le vulnerabilità del sistema attaccato. Il Tipo II invece include attività plurioffensive come il *cyberstalking*, le molestie, lo sfruttamento sessuale di minori, l'estorsione, lo spionaggio industriale, la pianificazione o lo svolgimento di attività terroristiche online, ecc. (Gordon, Ford, 2006 p. 3). Appare evidente come risulti estremamente difficile fornire un'unica definizione di criminalità informatica ed in particolare definire una linea di demarcazione tra lo spazio fisico e lo spazio virtuale, anche in un'ottica di azioni di contrasto o di prevenzione.

Analizzando gli effetti della condotta illecita si può asserire come tutte quelle azioni dirette a colpire la confidenzialità delle comunicazioni, l'integrità e la disponibilità dei dati abbiano una diretta ricaduta sul mondo reale, in particolare sull'aspetto economico. Un accesso abusivo o ad un danneggiamento ad un sistema informatico deputato al controllo dell'erogazione di corrente elettrica, oppure ai server di gestione del sistema sanitario nazionale, produrrà effetti nefasti sia sui sistemi elettronici, ingenerando la non disponibilità di servizi computazionali, sia sulle persone, inibendo il normale accesso e fruizione dei servizi stessi. Analogamente un furto identità o un utilizzo fraudolento di codici di carta di credito colpirà le persone, titolari di questi sistemi di pagamento, ma anche il sistema bancario stesso,

[5] Recentemente, il 12 maggio 2022, in occasione della conferenza internazionale organizzata sotto la Presidenza italiana del Comitato dei Ministri del Consiglio d'Europa, è stato aperto alla firma il secondo protocollo addizionale alla Convenzione sulla criminalità informatica, con l'intento di rafforzare la cooperazione e la trasmissione delle prove elettroniche nel campo della lotta alla criminalità informatica.

[6] Per completezza si riporta il testo originale degli autori: "any crime that is facilitated or commited using a computer, network, or hardaware device".

comportando il blocco dei pagamenti, la sostituzione della carta di credito e influenzando in ultimo, anche il sistema assicurativo.

Sintetizzando al massimo si potrebbe comunque affermare come il *cybercrime* possa essere considerato una particolare espressione del crimine tradizionale ma orientato tecnologicamente: sono mutati gli strumenti ma le finalità sono analoghe, ovvero porre in essere comportamenti antisociali plurioffensivi il cui contrasto richiede una forte specializzazione da parte delle forze di polizia, una armonizzazione delle norme ed una elevata cooperazione internazionale (Brenner, 2004).

4. Fenomenologia, tipizzazione dei crimini informatici e attori

Bunch, Clay-Warner e Lei, in *Demographic characteristics and victimization risk: Testing the mediating effects of routine activities*, hanno dimostrato come le vittime della criminalità tradizionale siano spesso giovani, maschi, con un basso livello di istruzione e di reddito e con tendenze a trascorrere più tempo all'aperto (Bunch *et al.* 2012). Al contrario, Junger e Montoya (2017) hanno evidenziato come le vittime di *cybercrime* siano più simili al cittadino medio[7] rispetto alle vittime della criminalità tradizionale. In *Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe* (Junger *et al.* 2017) gli studiosi, rilevano come la condizione di vittimia in questo contesto sia trasversale al genere ed all'età, anche se, per le frodi *online* vi è un maggiore scostamento verso le donne di età più avanzata, rispetto alle vittime delle frodi tradizionali. Nello studio gli Autori introducono la nozione di "normalizzazione" delle vittime di cybercrime, concetto legato al fatto che i computer sono presenti ovunque e le persone trascorrono *online* una notevole quantità di tempo: persone di diverso status socioeconomico hanno le stesse possibilità di essere vittimizzate. La ricerca evidenzia poi come alcuni comportamenti possano aumentare il rischio di vittimizzazione, tra questi i principali sono il tempo trascorso *online*, la tendenza a fare "click" facilmente su collegamenti senza verificarne il contenuto o la spasmodica ricerca del "prezzo migliore" a discapito del rischio di incappare in truffe talvolta banali (Junger *et al.* 2017). Dunque la consapevolezza e la conoscenza degli strumenti, oltre al tempo di utilizzo, rappresentano enormi fattori di rischio di vittimizzazione (Pratt *et al.* 2010).

Ad esclusione dei fenomeni criminali che vedono la tecnologia in termini meramente strumentali alla commissione dell'illecito[8], la criminalità informatica *stricto sensu* può essere generalmente associata ad azioni devianti mosse principalmente da motivazioni economiche o ideologiche, intese nella loro accezione più ampia, ed hanno come fine ultimo l'arricchimento, l'acquisizione illecita di informazioni sensibili o strategicamente appetibili ovvero il danneggiamento dei sistemi (Friedman, Bouchard, 2015). A tal proposito, per una analisi fenomenologica di questa tipologia di criminalità nel cyberspazio appare necessario fornire una tipizzazione degli attori coinvolti. Analizzando motivazione, obbiettivi e *modus operandi*, alcuni ricercatori hanno sviluppato una classificazione dei criminali informatici basata su tre livelli: i cybercriminali, i *competitor* o agenti di cyber spionaggio e gli hacktivisti (Friedman, Bouchard,

[7] Seppur in termini astrattamente teorici la locuzione "cittadino medio" potrebbe dar adito ad ambigue interpretazioni, nell'articolo proposto da Junger e Montoya la si deve intrepretare come quel cittadino le cui condizioni socioeconomiche e culturali lo collocano nella media nazionale.

[8] In tal senso, in questa sede, ci si riferisce ad esempio alla pedopornografia, al (cyber)stalking, al (cyber)bullismo o comunque a tutte quelle fattispecie che si perfezionano attraverso la rete ma le cui condotte potrebbero essere poste in essere anche al di fuori dei confini virtuali.

2015). A prescindere dalla tipologia dei soggetti coinvolti il fattore motivazionale risulta sempre riconducibile o comunque strettamente correlato a finalità di carattere economico finanziario oppure a motivazioni di tipo ideologico-politico. In linea di principio l'universo criminale nel cyberspazio può dunque essere ripartito tra tre tipologie di attori principali, le cosiddette *cyber gang*, i *competitor* o *state-sponsored* e gli hactivisti.

I primi sono riconducibili a gruppi criminali che perseguono illecitamente un arricchimento finanziario: utilizzano tecniche di *hacking* con il fine di acquisire ed esfiltrare informazioni a fini estorsivi, oppure per carpire e gestire in maniera fraudolenta i sistemi di pagamento delle singole vittime. Molto spesso sfruttano il fattore umano con tecniche di *social engineering*[9], come il *phishing*[10] distribuito (*spear phishing*), per poi inoculare software malevoli che vengono utilizzati per danneggiare o rendere inservibili i sistemi colpiti, chiedendo successivamente un riscatto per permetterne il ripristino. Gli attacchi di tipo *ransomware* o *cryptolocker*[11] hanno visto negli ultimi periodi un'impennata enorme: a livello globale nel 2021 sono stati registrati oltre 623 milioni di attacchi *ransomware*, con un incremento del 105% rispetto al 2020 e del 232% rispetto al 2019 (Crowdstrike, 2022).

I *competitor* o *state-sponsored* mirano invece ad ottenere un vantaggio competitivo sul piano economico, industriale, commerciale, politico o militare (Friedman, Bouchard, 2015 p. 14). Sono orientati ad acquisire informazioni strategiche, proprietà intellettuali, dati o informazioni, carpendo illecitamente credenziali di accesso dei sistemi informatici concorrenti o installando software malevoli che ne permetto il controllo da remoto, l'intercettazione delle comunicazioni ed il danneggiamento irreversibile dei dati. Il *modus operandi* e gli strumenti utilizzati sono molto simili a quelli in uso ai cybercriminali (*cyber gang*) ma hanno motivazioni differenti, maggiori risorse ed *expertise* tecniche. Utilizzano metodologie e approcci di tipo APT, *Advanced Persistent Threat,* stabiliscono una presenza illecita e duratura, una persistenza, all'interno del sistema avversario, con l'obiettivo di acquisire informazioni riservate, esfiltrare dati o prendere il controllo dell'infrastruttura attaccata. Con l'acronimo APT si identificano anche gli stessi gruppi criminali *state-sponsored* che sfruttano tali metodologie di attacco[12]. Questi gruppi fanno ampio uso di tecniche di *social engineering*, poiché il fattore umano è sicuramente l'anello più debole

[9] In linea generale per *social engineering* si devono intendere tutte quelle tecniche che sfruttano il fattore umano per acquisire informazioni o dati sensili dalla vittima, approfittando delle debolezze delle persone attraverso manipolazioni emotive. La casistica più classica è rappresentata dall'impersonificare uno specifico ruolo o una qualifica particolare presentandosi alla vittima come la persona che ha detiene prerogative per richiedere determinate informazioni altrimenti riservate.

[10] Il *phishing* si annovera nelle tecniche di social engineering, nella maggioranza dei casi viene attuato attraverso invio di messaggi di posta elettronica, sms, etc. artefatti in modo tale che la vittima, nel credere di ricevere comunicazioni ufficiali da parte di soggetti quali istituti di credito, corrieri, enti governativi etc. aderisce all'invio di informazioni, fornendo all'aggressore dati personali come codici di carte di pagamento, password di accesso al servizio di home banking, ecc. ovvero eseguendo procedure tali che consentono l'attivazione di software malevoli, solitamente offuscati all'interno dei messaggi stessi.

[11] Con il termine *ransomware* si fa riferimento ad una tipologia di *malware* (software dannoso) che ha lo scopo di bloccare o inibire l'accesso al sistema colpito. Per poter ripristinare le funzionalità i cybercriminali richiedono alle vittime il pagamento di un riscatto in denaro (tipicamente in cryprovaluta). Il *cryptolocker* o *crypto-ransomware* invece, una volta attivato sul sistema vittima, inizia a cifrare con chiave asimmetrica tutti i dati presenti: documenti, file di backup, progetti, etc, rendendoli completamente inutilizzabili senza però interferire con le funzioni di base del computer. Anche in questo caso vi è la richiesta di un riscatto che, se perfezionato, attiverà l'invio alla vittima della chiave di decodifica dei file per poterli utilizzare nuovamente.

[12]Gli attacchi di tipo APT vengono supportati e ricevono indicazioni sugli obbiettivi da attaccare da Governi o Stati Nazionali. Il loro principale scopo è quello di carpire dati sensibili e/o danneggiare o distruggere infrastrutture di rilevanza strategica utilizzando differenti tecniche e strumenti di attacco, a riguardo si rimanda a FireEye (2016) p. 3.

nella cosiddetta catena della sicurezza: sistemi, procedure e persone. Utilizzano poi le vulnerabilità dei sistemi non correttamente aggiornati ovvero le vulnerabilità ancora non del tutto conosciute, *exploit zero days*, per garantirsi la persistenza all'interno dell'infrastruttura attaccata. Nel 2021 i tentativi di *exploit* per la vulnerabilità denominata "Log4j" sono stati oltre 142 milioni in sei settimane. Il numero di varianti malware inedite sviluppate su tale vulnerabilità ha segnato un +65% (Crowdstrike, 2022). I gruppi *state-sponsored* sviluppano in maniera metodica un elevato numero di agenti software malevoli, sfruttano tecniche di dns *hijacking*[13] per intercettare e dirottare le comunicazioni della vittima, oltre che *tool* di tipo RAT (*remote access trojan*) per garantire, una volta installato sul sistema attaccato, la persistenza, il controllo e l'esfiltrazione di dati e delle informazioni sensibili. Il *Threat Analysis Group* (TAG) di Google ha pubblicato un report relativo ai tentativi di *hacking* commissionati da governi non occidentali nel terzo quadrimestre del 2019, dallo studio emerge che si sono identificati oltre 270 gruppi con legami con i governi di più di 50 paesi. Gruppi specializzati nella raccolta di informazioni, nel furto di proprietà intellettuali ovvero in attacchi informatici ai danni di dissidenti politici, giornalisti e attivisti scomodi. Gli stessi gruppi agiscono anche attraverso coordinate attività di disinformazione, disseminando in rete di notizie non veritiere, del tutto false o forvianti nei confronti di avversari politici (TAG, 2019).

Gli obiettivi tipici di questi attacchi sono rappresentati da istituzioni straniere, enti governativi e grandi gruppi industriali, mentre le finalità sono legate all'acquisizione di informazioni strategiche ed alla compromissione e sabotaggio di intere infrastrutture critiche o di siti produttivi. Gli APT si differenziano dagli attacchi informatici tradizionali per il grado di sofisticazione, decisamente più elevato, ma anche per la loro durata, ovvero la permanenza all'interno del sistema attaccato. In un recente studio presentato da Mediant, società di *threats intelligence*[14], si evidenzia come il cosiddetto *dwell time* o tempo di permanenza media di un attaccante all'interno di un sistema informatico, prima che venga riconosciuta e rimossa la minaccia, varia tra i 30 ed i 140 giorni (Mediant, 2021).

Gli hacktivisti sono invece spinti da motivazioni ideologiche con lo scopo di screditare o danneggiare una istituzione, un governo, un gruppo industriale, un'azienda (Friedman, Bouchard, 2015). Agiscono per ragioni etiche o politiche. Tipicamente le azioni dei cyber-attivisti sono orientate a screditare la vittima con attività di divulgazione sulla rete di informazioni o dati sensibili illecitamente esfiltrati, ovvero contrastare l'operatività del sistema attaccato attraverso azioni di tipo *denial of service* (DOS). Il *denial of service*, letteralmente negazione del servizio, viene generalmente effettuato attraverso l'invio massiccio di pacchetti di dati artefatti verso la rete o il sistema informatico attaccato, allo scopo di sovraccaricare i sistemi colpiti e di impedirne, anche solo temporaneamente, il regolare funzionamento. Le finalità sono di tipo quasi esclusivamente dimostrativo, spesso causano danni temporanei o

[13] Il *DNS Hijacking* o anche *DNS cache poisoning* è una tipologia di attacco informatico che ha lo scopo di modificare la *cache* dei *name server* in modo da alterare l'associazione indirizzo IP / nome di dominio; in questa maniera è possibile per l'attaccante dirottare il traffico della vittima verso falsi server DNS e dunque verso indirizzi IP / siti web malevoli. Con questa tipologia di attacco si possono carpire informazioni sensibili o indurre una potenziale vittima ad accedere a servizi malevoli o che presentano dati o informazioni artefatte.

[14] Per (cyber) *Threat Intelligence* si deve intendere la capacità di raccogliere, elaborare ed analizzare informazioni, notizie ma anche tecniche, tattiche e proceure (tactics, techniques, and procedures, TTPs) utilizzate dai cybercriminali per poter improntare un sistema di difesa adeguato e gestire in maniera efficacie le minacce in ambito cyber.

rallentamenti ai singoli sistemi attaccati. L'hacktivista, da iscrivere all'interno di movimenti di matrice ideologico-culturale, può operare in maniera isolata o collaborare con gruppi più o meno organizzati e strutturati di individui che condividono intenti, ideologie, credenze ed obiettivi. Organizzazioni come Anonymous, ad esempio, sono diventate famose già dal 2008 con l'Operazione Chanology: un attacco contro la chiesa di Scientology. Da allora sono molti gli attacchi che sono stati attribuiti a questo gruppo e che hanno visto colpire diversi obiettivi con differenti finalità politico-ideologiche (Tonellotto, 2020). È importante notare come, anche se alcuni autori includono l'hacktivismo all'interno del *cybercrime*, altri sostengono che questo approccio sia discutibile: a seconda della situazione o delle finalità, i gruppi di cyber hacktivisti, come il citato Anonymous, possono essere alternativamente visti come criminali o protettori dei diritti civili (George & Leidner, 2019). Quello che è certo è che le azioni dei cyber hacktivisti producono un impatto importante su differenti soggetti: individui, governi o istituzioni, con devastanti conseguenze economiche, politiche e sociali. Esiste dunque un forte legame tra *cybercrime* e *hacktivismo,* inteso come condotta multi-offensiva con risvolti *high tech*.

5. Quali attività di contrasto? Cooperazione internazionale, armonizzazione normativa, partnership pubblico-privato

Si è detto come il *cybercrime* si distingua rispetto alla criminalità reale poiché non prevede un contatto diretto tra autore e vittima (Brenner, 2004), in quanto risulta sempre necessaria la mediazione del mezzo tecnologico per l'attuazione della condotta deviante. È noto poi come in linea generale un elemento che facilita la commissione di un crimine risulti essere l'anonimato. Si consideri però che dal punto di vista meramente tecnico una qualsiasi attività svolta attraverso sistemi informatici lascia sempre elementi che possono essere ricostruiti, analizzati e tracciati, permettendo dunque di individuare origine e destinatario di una comunicazione[15]. Esiste però un anonimato *de facto* dettato, in particolare, dalle difficoltà di una pronta cooperazione giudiziaria internazionale da parte delle forze di polizia. Tentativi di armonizzazione delle normative a livello internazionale, come la già citata *Convenzione sul Cybercrime* del Consiglio d'Europa, hanno lo scopo di colmare tali limiti, ma si scontrano comunque con l'estrema velocità dell'azione criminale oltre che con la fragilità e la rapidità di dispersione delle evidenze digitali. Brenner (2004) evidenzia infatti come a livello locale le strategie di contrasto al *cybercrime* sono sviluppate per combattere crimini all'interno del territorio e della giurisdizione nazionale anche se, molto frequentemente, le azioni criminali sono originate o hanno ricadute al di fuori dei confini dei singoli Stati. Sempre di più dunque vi è la necessità di politiche di contrasto comuni che esulino dal concetto di giurisdizione nazionale. Politiche orientate a favorire una puntuale attività preventiva, mettendo a fattore comune competenze, attività info-investigative o di intelligence, che prevedano condivisione e scambio informativo costante, promuovendo una fattiva cooperazione internazionale e facilititando accordi di partenariato pubblico-privato. La definizione di politiche comuni ed il partenariato pubblico-privato diviene fondamentale nella gestione della tutela delle infrastrutture critiche o delle attività sensibili. Si

[15] In tal senso ci si riferisce alle metodiche di *incident response* e *digital forensics*, *ex multis*: Johansen Gerard, *Digital forensics and incident response: incident response techniques and procedures to respond to modern cyber threats*, Packt Publishing Ltd., Birmingham, 2020.

pensi al settore energetico, a quello dei trasporti o delle telecomunicazioni ed alle inevitabili ricadute sul sistema paese e sull'economia nazionale nel caso di attacchi informatici mirati a tali strutture. La storia recente ha evidenziato come le minacce alle infrastrutture sensibili o critiche siano concrete e di estrema attualità e come, in assenza di una stretta collaborazione pubblico-privato, le aziende possono ben poco nei confronti di situazioni emergenziali, che hanno riflessi anche sulla sfera geopolitica internazionale (Tonellotto, 2017).

Negli ultimi anni l'Unione Europea e gli Stati Uniti hanno compreso la necessità della cooperazione internazionale e dell'armonizzazione normativa a favore della gestione della protezione della sicurezza delle informazioni. Gli Stati Uniti e l'UE cooperano in numerose contesti e assemblee in materia di sicurezza informatica. Gli Stati Uniti hanno per altro siglato la Convenzione del Consiglio d'Europa sulla criminalità informatica e collaborano nel settore della sicurezza informatica in organizzazioni multilaterali. L'Unione Europea nel 2016 ha emanato la direttiva sulla sicurezza delle reti di informazione (direttiva NIS, *Network and Information Security*) ed il regolamento generale sulla protezione dei dati personali (GDPR). La Direttiva UE NIS[16], ha come scopo principale quello di aumentare e migliorare, per ogni singolo Stato membro dell'Unione, la propria capacità di gestire la sicurezza delle reti. Gli Stati europei in maniera concertata devono elevare gli standard di sicurezza e di scambio informativo in relazione ai cosiddetti "incidenti informatici". La direttiva prevede che ogni Stato membro sia obbligato ad adottare una strategia a livello nazionale in materia di cyber sicurezza, avendo il compito di nominare autorità competenti, nonché entità investite dalla responsabilità di monitorare gli incidenti informatici. I tal senso sono stati istituiti i CSIRT nazionali: *Computer Security Incident Response Team*. I CSIRT hanno il compito di monitorare gli incidenti informatici a livello nazionale, diramare preallarmi e allerte, inviare comunicazioni sul territorio, favorire lo scambio informativo tra le parti interessate in merito a rischi e alle minacce, intervenire in caso di incidente, analizzandone la dinamica e gestire i rapporti tra gli altri Stati membri dell'UE eventualmente coinvolti. Ai sensi della direttiva NIS gli Stati membri devono adottare una strategia nazionale di *cybersecurity* che garantisca elevati livelli di sicurezza per i sistemi e le reti informatiche, con particolare riguardo a quelli ritenuti essenziali, designando autorità competenti per monitorare a livello nazionale l'applicazione della direttiva ed individuando un unico punto di contatto per la cooperazione tra i singoli Stati. La norma ha poi definito il ruolo degli operatori di servizi essenziali (OSE), ovvero soggetti pubblici o privati che forniscono servizi direttamente dipendenti dalle reti di comunicazioni o da sistemi informatici e che sono essenziali per il mantenimento di attività sociali o economiche e per i quali un eventuale incidente informatico potrebbe avere ripercussioni rilevanti sulla fornitura dei servizi stessi e sulla collettività. Rientrano in questa classificazione le realtà pubbliche o private che operano in vari settori, in particolare quello dei trasporti, delle infrastrutture deputate alla produzione, erogazione e fornitura di energia elettrica, gas ed idrocarburi, gli enti creditizi, il settore sanitario, etc[17].

[16] Direttiva 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016, Recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[17] L'allegato II del d.lgs. n. 65 del 2018, norma che recepisce la Direttiva NIS in Italia, prevede l'elenco dei soggetti classificati come operatori di servizi essenziali (OSE). Con la medesima norma, all'art. 4, è stato istituito presso il Ministero dello sviluppo economico un elenco nazionale

L'Italia ha dato attuazione alla direttiva NIS recependola con il decreto legislativo 18 maggio 2018, n. 65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018. Con l'art.12, rubricato "obblighi in materia di sicurezza e notifica degli incidenti", viene previsto come gli OSE siano tenuti ad adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi alla sicurezza delle reti e dei sistemi informativi. Tali misure devono essere adeguate a prevenire e minimizzare l'impatto di incidenti a carico dei sistemi informativi e applicate al fine di assicurarne la continuità operativa. Vi è poi l'obbligo da parte degli Operatori di Servizi Esenziali di notifica al CSIRT italiano e all'Autorità NIS di tutti gli incidenti con impatto rilevante. La rilevanza dell'impatto di un incidente viene definita a livello normativo sulla base di specifici parametri quali, il numero degli utenti coinvolti dal malfunzionamento dei sistemi, la durata dell'incidente, la diffusione geografica, etc. A seguito della ricezione della notifica di incidente, il CSIRT può informare i singoli Stati membri interessati nel caso in cui l'evento abbia causato un impatto rilevante sulla continuità dei servizi essenziali in quella specifica area geografica.

L'art. 8 d.lgs. n. 65/2018 istituisce il CSIRT Nazionale o *Gruppo di Intervento per la Sicurezza Informatica*, che ha compiti di definire le procedure per la prevenzione e la gestione degli incidenti informatici, ricevere e gestire le notifiche di incidenti inviate dai fornitori dei servizi essenziali e garantire la "collaborazione effettiva, efficiente e sicura" nella rete di CSIRT europea.

A seguito dell'approvazione della Direttiva NIS nel 2016 sono state adottate, a livello comunitario, ulteriori misure con lo scopo di rafforzare la sicurezza cibernetica nell'Unione. Il Cybersecurity Act del 2019[18] si prefigge lo scopo di definire un quadro comune europeo per la certificazione della sicurezza informatica dei prodotti ICT e dei servizi digitali, oltre che quello di rafforzare il ruolo dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA). Il Cybersecurity Act costituisce un tassello fondamentale della nuova strategia dell'UE per la sicurezza cibernetica che ha l'obbiettivo di rafforzare la resilienza degli Stati membri agli attacchi informatici oltre che a sviluppare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi. Recentemente il Consiglio e il Parlamento Europeo hanno poi concordato un pacchetto di misure con lo scopo di migliorare ulteriormente le capacità di risposta agli incidenti del settore pubblico e privato, tale protocollo aggiornerà l'attuale direttiva NIS al fine di predisporre la nuova direttiva, NIS2, che avrà l'obiettivo di definire ulteriormente le misure di gestione del rischio di cybersecurity e gli obblighi di segnalazione in tutti i settori coperti dalla nuova direttiva, come l'energia, i trasporti, la salute e le infrastrutture digitali (EC, 2022).

In Italia, con il D.L. 14 giugno 2021, n. 82, è stata altresì istituita l'Agenzia Nazionale per la Cybersicurezza (ACN), che ha il compito di garantire l'implementazione della strategia nazionale di cybersicurezza adottata dal Presidente del Consiglio, promuovere un quadro normativo coerente nel settore delle nuove tecnologie, oltre che esercitare funzioni ispettive e sanzionatorie nel caso di soggetti inottemperanti alle linee di indirizzo del Governo in materia di cybersicurezza. L'Agenzia

degli operatori di servizi essenziali. Tale elenco deve essere riesaminato almeno a cadenza biennale a cura delle autorità competenti NIS e comunicato al MISE.

[18] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

deve poi sviluppare collaborazioni a livello internazionale con agenzie omologhe ed assicurare il coordinamento tra soggetti pubblici per la realizzazione di azioni pubblico-private, volte a garantire la sicurezza e la resilienza cibernetica. In ultimo, il recentissimo decreto del Presidente della Repubblica n. 231 del 19 novembre 2021, entrato in vigore il 14 gennaio 2022, concernente "L'organizzazione degli uffici centrali di livello dirigenziale del Ministero dell'Interno" ha istituito, nell'ambito del Dipartimento di Pubblica Sicurezza, la nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, nella quale sono confluite le attribuzioni sinora svolte dal Servizio Polizia Scientifica e dal Servizio Polizia Postale e delle Comunicazioni. La Direzione Centrale assumerà la gestione del *Computer Emergency Response Team* (CERT) del Viminale. La nuova organizzazione del Dipartimento di P.S. prevede poi l'istituzione dei Centri Operativi per la Sicurezza Cibernetica, C.O.S.C., in sostituzione dei Compartimenti Polizia Postale e delle Comunicazioni. Questi Centri, alle dirette dipendenze della Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, avranno competenza regionale. Lo stesso Decreto ha poi previsto la trasformazione anche delle Sezioni Polizia Postale che, con competenza provinciale, assumeranno la nuova denominazione di Sezioni Operative per la Sicurezza Cibernetica (S.O.S.C.).

La nuova riorganizzazione ha lo scopo di potenziare le capacità di intervento in caso di eventi di sicurezza informatica complessa e prevede l'istituzione, all'interno dei Centri C.O.S.C., di Nuclei Operativi per la Sicurezza Cibernetica (N.O.S.C.) che svolgeranno anche le funzioni di Organo periferico del Ministero dell'Interno per la regolarità dei servizi di telecomunicazione. Ai N.O.S.C. sono state attribuite specifiche competenze operative e di intervento rapido in caso di eventi informatici avversi e con criticità variabile, compiti info-investigativi e di *threat intelligence* funzionali al contrasto di reati informatici che coinvolgono infrastrutture critiche e sensibili del territorio.

6. Conclusioni

Si è visto come la criminalità informatica stia diventando una delle principali sfide alla sicurezza globale. Per contrastare e contenere la rapida evoluzione delle tecniche adottate dai cyber-criminali sono necessarie politiche internazionali integrate e comuni ma anche adeguata consapevolezza da parte di chi, quotidianamente, fa uso delle nuove tecnologie. Tale sfida richiede una collaborazione senza precedenti tra le parti interessate: governi, aziende, stakeholders, istituti di ricerca e mondo accademico. La necessità di una maggiore e più stretta collaborazione tra pubblico e privato appare attualmente la soluzione più auspicabile: azioni congiunte tra realtà differenti ma con medesimi scopi, come già pronunciato nel 2006 dall'Assemblea Generale delle Nazioni Unite con la risoluzione A/RES/60/288 del 20 settembre 2006 in tema di lotta al terrorismo internazionale. A livello europeo la strategia comune è quella della condivisione di intenti e responsabiltà sia tra i singoli Stati membri, sia coinvolgendo le realtà pubbliche e private che operano nei settori di intaresse strategico e che forniscono servizi esenziali, al fine di elevare i livelli di sicurezza per i sistemi e le reti informatiche.

Vi è infine da sottolineare come numerosi attacchi informatici si basino in primo luogo sulla cosiddetta ingegneria sociale: una metodologia di raccolta delle informazioni che sfrutta quello che viene definito

l'anello più debole della sicurezza, il fattore umano. Le tecnologie possono aiutare a definire e sviluppare un ambiente sicuro, le *policy* di sicurezza possono mitigare azioni malevoli ma senza la consapevolezza del rischio associato all'uso non corretto di tali tecnologie, le minacce saranno sempre estremamente attuali e produrranno enormi danni. Il fattore umano è la componente fondamentale ed è dunque importante promuovere a tutti livelli il concetto di *attenzione consapevole* (Balloni, 1998) come risorsa necessaria per limitare i rischi di vittimizzazione anche nel dominio delle nuove tecnologie. Consapevolezza, cultura della *cybersecurity*, tecnologie affidabili, procedure comuni, competenze, armonizzazione del diritto e cooperazione internazionale sono dunque le parole chiave per vincere questa sfida globale nel cyberspazio.

Bibliografia

1. Balloni A., «Il criminologo dell'organizzazione della sicurezza: problemi di formazione ed esigenze di professionalità», Balloni A. (dir.), *Criminologia e sicurezza*, Franco Angeli, Milano, 1998, pp. 13-21.
2. Becker G., «Crime and Punishment: An Economic Approach», *Journal of Political Economy*, vol. 76, n. 2, 1968, pp. 169-217.
3. Brenner S. W., «Cybercrime metrics: Old wine, new bottles?», *Virginia Journal of Law and Technology,* vol. 9, n. 13, 2004.
4. Bunch J., Clay-Warner J., Lei M.-K., «Demographic characteristics and victimization risk: Testing the mediating effects of routine activities», *Crime and Delinquency*, 6, 2012, pp. 1181-1205.
5. Clough J., *Principles of Cybercrime*, University Press, Cambridge, UK, 2010.
6. Friedman J., Bouchard M., *Definitive Guide to Cyber Threat Intelligence*, MD: CyberEdge Group, LLC, Annapolis, 2015.
7. George J. Leidner D., «From Clicktivism to Hacktivism: Understanding Digital Activism», *Information and Organization*, vol. 29, n. 3, 2009.
8. Gordon S., Ford R., «On the Definition and Classification of Cybercrime», *Journal in Computer Virology*, vol. 2, n. 1, 2006, pp. 13-20.
9. Jaishankar K., «Cyber criminology: Evolving a novel discipline with a new journal», *International Journal of Cyber Criminology*, vol. 1, n.1, 2007a, pp. 1-6.
10. Jaishankar K., «Establishing a theory of cyber crimes», *International Journal of Cyber Criminology*, vol. 1, n. 2, 2007b, pp. 7-9
11. Jaishankar K., «Space Transition Theory of Cyber Crimes» in Schmallager F., Pittaro M. (ed.), *Crimes of the Internet*, Upper Saddle River, NJ: Prentice Hall, 2008, pp. 283-301.
12. Jaishankar K., *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, CRC, Bca Raton, 2011.
13. Junger M, Montoya L., Hartel P, Heydari M., «Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe», *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA).*10.1109/CyberSA.2017.8073391, 2017.
14. Johansen G., *Digital forensics and incident response: incident response techniques and procedures to respond to modern cyber threats*, Packt Publishing Ltd., Birmingham, 2020.
15. Pratt T. C., Holtfreter K., Reisig M. D., «Routine online activity and internet fraud targeting: Extending the generality of routine activity theory», *Journal of Research in Crime and Delinquency*, vol. 47, n. 3, 2010, pp. 267-296.
16. Scarscelli D., Vidoni Guidoni O., *La devianza. Teorie e politiche di controllo*, Milano, Carrocci, 2008.
17. Suler J., «The online disinhibition effect», *CyberPsychology & Behavior*, vol. 7, n. 3, 2004, pp. 321-326.
18. Saponaro A., Prosperi G. (2007), «Computer crime, virtualità e cybervittimologia», in Pitasi A. (a cura di), *Webcrimes. Normalità, devianze e reati nel*

cyberspace, Angelo Guerrini e Associati, Milano, 2007.
19. Tonellotto M., *Computer forensics: l'acquisizione della prova informatica*, MD: EAI, Chisinau, 2015.
20. Tonellotto M., *La sicurezza nelle organizzazioni. Un approccio socio-criminologico alla security aziendale*, FrancoAngeli, Milano, 2017.
21. Tonellotto M., «Crime and Victimization in Cyberspace», in Balloni A., Sette R. (ed.), *Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim Support,* IGI GLOBAL, Hershey, pp. 248-264, 2020.
22. U.S. DOJ., *Computer Crime & Intellectual Prop. Section*, U.S. Dep't of Justice Criminal Div., Legislative Analysis of the 1996 National Information Infrastructure Protection Act, 2 Electronic Info.Pol'y & L. Rep., 240, 240, 1997.
23. Wall D. S., *Cybercrime: The transformation of crime in the information age*, Polity Press, Malden, MA, 2007.

Sitografia

1. Crowdstrike, *2022 Global Threat Report,* disponibile all'indirizzo: https://go.crowdstrike.com/global-threat-report-2022.html
2. Datareportal, *Digital around the world*, 2019, disponibile all'indirizzo: https://datareportal.com/global-digital-overview
3. E.C., «Commission welcomes political agreement on new rules on cybersecurity of network and information systems», *Eropean Commission Press Corner*, 2022, disponibile all'indirizzo: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985
4. FireEye, *Advanced persistent threat (APT) groups. A field guide to state sponsored cyber attackers, 2016,* disponibile all'indirizzo: www.fireeye.com/offers/apt-handbook.html
5. Mediant, *M-trends 2021 Insights into Today's Top Cyber Trends and Attacks*, 2021 disponibile all'indirizzo: www.mandiant.com/resources/m-trends-2021
6. Intelligence, G. S. M. A., *Definitive data and analysis for the mobile industry,* 2021, disponibile all'indirizzo: www.gsmaintelligence.com
7. Internet World Stats, *World Internet Users and 2021 Population Stats,* 2021 disponibile all'indirizzo: www.internetworldstats.com/stats.htm

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

doi: 10.14664/rcvs/242

Gli hacktivisti dall'interno: identità collettiva, selezione degli obiettivi e uso tattico dei media durante le proteste della Primavera dell'Acero in Québec

Les hacktivistes de l'intérieur : identité collective, sélection des cibles et utilisation tactique des médias pendant les manifestations du Printemps Érable au Québec

Hacktivists from the Inside: Collective Identity, Target Selection and Tactical Use of Media during the Quebec Maple Spring Protests

Francis Fortin[*]*, Francesco C. Campisi*[**]*, and Marie-Ève Néron*[***]

Riassunto
La maggior parte delle ricerche su Anonymous ha studiato il gruppo da un punto di vista etnografico o si è concentrata sull'analisi dei messaggi diffusi sui social media per comprendere gli interessi del movimento. Ci sono stati pochi tentativi di analizzare il modo in cui gli hacktivisti scelgono gli obiettivi appropriati per gli attacchi informatici a fini di protesta. Il presente studio cerca di fornire una panoramica dei valori condivisi da Anonymous esaminando le interazioni tra i membri del gruppo nelle chat room pubbliche durante i quattro mesi delle manifestazioni studentesche in Québec conosciute come *Primavera dell'Acero 2012*. In tal senso, è stata effettuata un'analisi tematica al fine di identificare i temi importanti. I risultati mostrano che i valori fondamentali di Anonymous sono coerenti con quelli diffusi attraverso gli account social media del gruppo, focalizzandosi in particolare sulla libertà di espressione spesso legata alla libertà di parola e di informazione come parte integrante del processo di selezione degli obiettivi. L'analisi mostra inoltre come i partecipanti alle chat abbiano proposto dei bersagli tipici dell'attivismo politico (ad esempio, il governo, la polizia, i partiti politici) e siano concordi sugli obiettivi da rifiutare, come i mezzi d'informazione tradizionali, in quanto considerati importanti per la diffusione dei messaggi del gruppo e delle informazioni relative alle operazioni svolte.

Résumé
Une grande partie de la recherche sur Anonymous a étudié le groupe d'un point de vue ethnographique ou s'est concentrée sur les messages des médias sociaux pour apprendre ce qui est le plus important pour le mouvement. Il n'y a eu que peu de tentatives d'analyse de la manière dont les hacktivistes choisissent les cibles appropriées pour les cyberattaques ayant des objectifs de protestation. La présente étude tente de donner un aperçu des valeurs partagées en examinant les interactions entre les membres d'Anonymous sur les salons de discussion publics pendant les quatre mois des manifestations étudiantes québécoises connues sous le nom de Printemps Érable 2012. Une analyse thématique a été réalisée pour catégoriser les thèmes importants. Les résultats montrent que les valeurs fondamentales du groupe Anonymous sont congruentes à celles des comptes de médias sociaux d'Anonymous, mettant l'accent sur la liberté d'expression, souvent liée à la liberté de parole et à la liberté d'information comme partie intégrante du processus de sélection des cibles. En outre, les participants au salon de discussion ont proposé des cibles traditionnellement appropriées (c'est-à-dire le gouvernement, la police, les partis politiques) et semblent s'accorder sur les cibles à rejeter, comme les médias d'information traditionnels, jugés importants pour diffuser son message et fournir des informations sur ses opérations.

Abstract
Much of the research on Anonymous has studied the group from an ethnographic perspective or focused on social media posts to learn what is most important for the movement. There have been only few attempts to analyze how hacktivists are choosing suitable targets for cyberattacks with protest objectives. The present study attempts to provide insight into their shared values by looking at interactions among Anonymous members on public chatrooms during the four months of the

[*] Ph.D., School of criminology, University of Montreal.
[**] M.A., Ph.D. candidate, School of criminology, University of Montreal.
[***] M.Sc., School of criminology, University of Montreal.

Quebec student demonstrations known as the 2012 *Printemps Érable* protests. A thematic analysis was performed to categorize the important themes. The results show that the core values of Anonymous's group is congruent to that of Anonymous's social media accounts, emphasizing freedom of expression, often linked to freedom of speech and freedom of information as integral to the target selection process. Also, participants in the chatroom proposed traditionally suitable targets (i.e., the government, the police, political parties) and seems to agree upon which targets should be rejected such as traditional news media, deemed important to diffuse its message and provide information about its operations.

Key words: hacktivism, Anonymous, online disobedience, values, cybercrime

1. Introduction[1]

In April 2012, an ominous video was published on YouTube. The video, projecting a man in a suit donning a Guy Fawkes mask spoke to the camera and stated the government of Québec's emergency law will "assassinate the right to protest" (Levesque, 2012, p. 1). The law in question, Bill-78, was, at that time, being discussed on the floor of the Quebec National Assembly as a response to the ongoing student protests. A month prior, the Liberal Party of Quebec announced a 75% tuition increase for CEGEP (Quebec publicly funded colleges) and university students across the province (Raynauld *et al.*, 2016). This caused students to protest on the streets, blocking entrances to university buildings, and clash with police over the course of several months. These protests, known as the Maple Spring or *le Printemps Érable* (in French), received national attention, attracting several thousand students to take part in voicing their concerns and outright opposition towards the tuition increase (Raynauld *et al.*, 2016). In response, Bill-78 proposed limitations on student protests by outlawing all rallies containing 50 people or more, unless the rallies were approved by police, as well as granting greater discretionary powers to police officers to control the crowds (Bégin-Caouette, Jones, 2014).

The Anonymous collective has been a trailblazer in the hacktivist movement, since its first involvement with social and political causes in 2008. For the purposes of this study, the term hacktivism is defined as the hybridization of computer technology and social activism (Gunkel, 2005). Hacktivists like Anonymous use a wide variety of hacker-typed techniques (website disfiguration, distributed denial of service attacks, virtual sit-ins and leaking classified documents, to name a few) for the purposes of disrupting, creating harm, bringing attention to a social movement or cause, and putting pressures on traditional institutions of power (Caldwell, 2015; Gunkel, 2005; Kelly, 2012; Renzi, 2015). Over the years, Anonymous has utilised these techniques (most notably DDoS attacks and website disfiguration) against institutions they deemed to have infringed on both individual and collective freedoms (Bardeau, Danet, 2011; Beyer, 2014; Coleman, 2014). Bill-78 and the Québec government were no exception. While the Anonymous cell in the province of Québec initially refrained from their involvement, it was the introduction of Bill-78 that sparked #OperationQuébec, where Anonymous members hacked several government and police websites between the months of April and May 2012.

The cyberattacks on the Québec government are representative of similar Anonymous campaigns spanning over a decade. Anonymous has pursued governments, religious institutions, and other targets who they deem to infringe on freedoms such as the freedom of expression, freedom of information, and individuals' ability to protest (Jones *et al.*, 2020; Pendergrass, 2013). For example,

[1] This study was funded through a Social Sciences and Humanities Research Council of Canada (SSHRC) grant (SSHRC/CRSH #430-2016-01048).

Operation Paris was an Anonymous campaign against ISIS, after a series of Islamist terrorist attacks that took place in a suburb of Paris and at soccer stadium in St-Denis on November 13, 2015 (de la Hamaide, 2015). This trend has remained stable over time, as Anonymous has more recently targeted American police forces and the Russian government, who, according to Anonymous social media accounts, demonstrated abuses in powers (Franceschi-Bicchierai, 2020; Purtill, 2022). And thusly, the consistency of targets chosen for cyber attacks is reflected in a consistency of values and collective identity advocated on social media.

Yet little is known about the values of those Anonymous members engaging in both the target selection process and the hacking operations themselves. This is due to both the secretive nature of the target selection process and the plethora of information Anonymous divulges on social media. Research has primarily analysed Anonymous' social media accounts as they provide information on different campaigns, successful hacking operations and social causes (Bergeron *et al.*, 2019; McGovern, Fortin, 2019). As such, values attributed to Anonymous stem from an interpretation of these sources, suggesting a cohesion of collective identity and values among the two strata of members: the hackers and the social media users. However, due to Anonymous' nebulous and informal structure, there is little evidence to suggest that the members hacking government websites and those operating social media are one and the same. For example, Anonymous's 'accept-all' strategy for membership allows for individuals with different goals and technical skills to participate (Kelly, 2012). Based on these characteristics, members can participate uniquely through social media if they so choose, raising questions as to the possible disconnect in values between hackers and other members.

The present study analyses the activities of Anonymous' Québec cell participants on two public chatrooms during the Maple Spring to determine which values were most important to Anonymous' hackers during their target selection process. This objective is significant due to Anonymous's loosely defined structure and addresses questions regarding their ability to organise post 2011. At the end of 2011, one of Anonymous's leader, known online as Sabu, was arrested, which consequently resulted in the dissolution of the more militant arms of Anonymous: LulzSec and AntiSec (Anderson, 2012). This has had an undesirable effect, causing Anonymous to cluster, more so than they already loosely connected, informal structure for which they are known for. Anonymous post-Sabu has been characterised as much more ineffective at organising, with less clear motivations, often ending in dissent and confusion over messages, operations, and target selection (Kelly, 2012). It is therefore imperative to analyze Anonymous's communications during operations to ascertain Anonymous' values during the target selection process rather than through social media posts.

2. Literature Review

The first use of the term *hacktivism* originates in the late 1990s, by an American hacker under the pseudonym Omega; a member of the activist group called the Cult of the Dead Cow (CDC) (Guiton, 2013). The term itself is an amalgamation of the terms "hacking" and "activism", which refers to the use of computer technology as the predominant physical tool for advancing the political causes of a given movement (Conway, 2003; Denning, 2001; Gunkel, 2005; Ludlow, 2010; Manion, Goodrum,

2000). Contrary to traditional protest movements, hacktivism generally occurs when triggered by a social event/policy or when a social protest shows signs of repression from traditional institutions of power (George, Leidner, 2019; Kahn, Kellner, 2004). This denotes a symbiotic interplay between social movements and hacktivism; as hacktivism frequently work together with more traditional social movements, differing mainly on the techniques utilised.

With the aid of computer technologies, traditional social movements employ tactics defined as electronic civil disobedience, which are *generally* legal means of online protest and expressions [emphasis added] (Karatzogianni, 2013). According to George and Leidner (2019), electronic civil disobedience is considered part of digital transitional activities, in which offline forms of protests have transitioned into digital equivalencies (like virtual sit-ins, online petitions, etc.). Comparatively, hacktivism is categorized as digital gladiatorial activity, in which hacktivists perform more direct actions which may have more potential impacts on society, government and organisations (George, Leidner, 2019). A clearer taxonomy of hacktivism is presented by Samuel Houghton (see Romagna, 2020), who argues electronic civil disobedience is one small aspect of hacktivism, subcategorising hacktivism into three: political cracking, performative hacktivism and political coding. The first is the most aggressive form of hacktivism, such as website defacements, cyber trespassing, and DDoS attacks. The second, performative hacktivism, entails civil disobedience actions that are undertaken but not necessarily illegal, such as virtual sit-ins. The third, political coding is the development of software for political use, like the creation and modification of VPN and IRC forums. What englobes these categorisations is the view of hacktivism as actionable, one where the type of actions requires computational technologies, and whose motivations stem from political or social tensions and events.

In general, due to the flexible definition of hacktivism, research has compiled hacktivist activities to include virtual sit-ins, website disfiguration, email bombing, site parodies, distributed denial of service attacks (DDoS attacks), disclosure of hacked confidential information, site parodies and assertions on social media (Auty, 2004; Caldwell, 2015; George, Leidner, 2019; Hampson, 2012; Karatzogianni, 2013; Li, 2013; West, 2017). Despite the multitude of techniques presented, an important technique in hacktivists' repertoire is that of assertion. Assertion is frequently used as a tool for dissemination of information, which range from posting content regarding certain hacktivist operations taking place on other platforms, interacting with citizens, other activists, and commentating on government activities (George, Leidner, 2019). This tactical form of media usage allows for hacktivists to critique powerful regimes by exposing temporary fissures of power and disrupt the incumbent power through online exposure (McKelvey, 2010).

The ability to demystify Anonymous' values is a direct result of assertion, as Anonymous is highly active on social media. Anonymous members write press communiqués, media interviews, and publish content that makes propaganda, videos, and information on social causes publicly accessible (Coleman, 2020). Individual members are running hundreds of Anonymous Twitter accounts, using social media to broker and connect individuals and social movements, using bots to boost visibility, and influence greater support for a cause (Beraldo, 2022; Jones *et al.,* 2022). Anonymous values are also

extracted through an analysis of the content produced on social media. For example, an analysis of hashtag usage found that male and female members focused on animal rights, conspiracy theories, and ISIS (McGovern, Fortin, 2019). The hacks themselves are often evaluated by the media, citing the Anonymous-affiliated tweets to best understand their motivations and goals (Bonifacic, 2022; Kika, 2022; Papadopoulos, 2022). The tactical use of both social and mass media forces discourse by presenting a contrasting vision of justices and freedom, challenging these notions for the purposes of changing longstanding control by governments and other institutions of powers. As such, their use of assertion both implicitly and explicitly reveals the values that motivate their target selection.

2.1 Collective Identity

What makes Anonymous enigmatic is its unparalleled ability to launch hundreds of online campaigns, despites its lack of defined shape and its imprecise, nebulous structure. This makes it hard to identify how it shapes the collective identity of its members (Machado, 2015; Mansfield-Devine, 2011). As one author notes, "Even under the discrete umbrella of hacktivism, […] Anonymous has a distinct makeup: a decentralised (almost nonexistent) structure, unabashed moralistic/political motivations, and a proclivity to a couple online cyberattacks and offline protests" (Kelly, 2012, p. 1678). It is possible the fluid nature of the group's structure contributes to the continued life of the movement, even after the arrests of its leaders (the infamous Hector "Sabu" Monsegur) and the subsequent dissolution of Anonymous's affinity groups: LulzSec and AntiSec in 2011 (Anderson, 2012). Anonymous members (self-proclaimed "Anons") do not operate within a formal hierarchical power structure but instead create many small, horizontally structured groups, which allowed the movement to remain active even when faced with potential arrests and the loss of one or more of its more influential participants (Beran, 2020).

2.2 Freedom of Expression

Anonymous has a long history of targeting individuals and corporations who would place limitations on individual and collective freedoms. Initially, the members of Anonymous were seen as online pranksters (otherwise known as trolls) and their actions were viewed as disruptive by its victims and amusing by its members. For example, one of their first operations known as *Habbo Raid*, involved organising 4chan users to perform a virtual sit-in the virtual world game Habbo Hotel (Bardeau, Danet, 2011). This operation was a performative prank aimed simply to block access to other users of the game — disruption for the sake of disruption. In 2008, in what came to be known as Project Chanology, attacks against the Church of Scientology increased the group's visibility outside the message boards, and led to the evolution of the group as hacktivists, beginning to take on more social, political, economic and technological issues spanning several years (Caldwell, 2015; Coleman, 2011, 2014). Since that time, Anonymous members have used DDoS attacks and the leaking of confidential information against targets such as the America Israel Public Affairs Committee, the CIA, the FBI, the Vatican, the White House and the Westboro Baptist Church (Bodó, 2014; Kenney, 2015; Ludlow, 2010). Anonymous has been credited with publicly leading the hacktivist movement (*movement* being defined as the concept of hacktivism, not an organised social movement in

itself), utilising legal and illegal digital tools to pursue political actions and influence public opinion on a wide range of issues (Kelly, 2012; Pendergrass, 2013).

The quasi-homogenous group of targets chosen by Anonymous campaigns over the years are representative of their commitment to freedom of expression as a core value. Between 2008 to 2011, during the height of Anonymous's popularity, Anonymous's operations and members adhered to a specific philosophy, which englobed free access of information, ensuring that information remains both free and decentralised (Ludlow, 2010). Congruent with hacktivist goals as defined by Gunkel (2005) and Renzi (2015), the core values of Anons places them in opposition to those who try to curb freedom of expression and information sharing and defend the principles and values of anti-globalisation (Bardeau, Danet, 2011). Most recently, Anonymous pursued Russian governmental infrastructure, disfiguring websites affiliated to Russian State TV, Russia's space research institute, energy companies and the Center for the Protection of Monuments in response to perceived illegitimate invasion of the Ukraine by Russian forces (Everington, 2022; Faife, 2022). In each case, Anonymous targeted institutions and corporations who would place limitations on the individual and/or collective freedoms, particularly that of freedom of expression.

2.3 Immunity of the media

At its simplest, the tactical use of media and other hacking methods is crucial to the movement: hacktivism is a way of gaining visibility and causing harm (Caldwell, 2015; West, 2017). The use of these tactics suggests the willingness to garner attention to a social-political issue, raise awareness (due perhaps to waning or neglecting attention), create public pressures, question established systems and, in a sense, resist the legitimisation of such institutions (Gunkel, 2005; Kelly, 2012; Renzi, 2015). As Renzi (2015) suggests, hacktivism creates a terrain for forced discourse by presenting a contrasting vision of justice and freedom, challenging these notions for the purpose of changing the longstanding, standardized control over those discourse by governments and other institutional forms of power. For example, Anonymous aided in publicizing rape cases in Ohio at an international level as well as aiding the Arab Spring protests when the government banned Twitter to its citizens (Coleman, 2020). As is the case with other social movements, hacktivism relies on mass media and social media to reach greater audiences and support, that overcome geographic limitations and suppressive means of the government. As such, the media, both traditional forms of media (e.g.: news sources) as well as social media, are imperative tools for hacktivist groups such as Anonymous, granting a certain immunity from hacktivist groups.

3. Aim of the study

There exist contradictions regarding Anonymous' organisational structure and its impact in the target selection process. Since the arrests of Anonymous leaders in late 2011 and early 2012, Anonymous has been deemed as weak and less effective than its past. Social movement researchers have noted campaigns rife with constant dissent over messages and operation targets, which is a direct consequence of its informal, decentralised structure (Caldwell, 2015; Kelly, 2012). Consequently, this has caused a blur in the target selection process, and the values which motivate certain operations such as minority-led projects and hacks, with no minimum approval,

and almost no justification between members (Kelly, 2012). For example, a lone anti-abortion hacker targeted Britain's largest abortion clinic under the banner of Anonymous (Coleman, 2020). While the campaign was disavowed by other Anonymous members and social media accounts, it is indicative of contradicting values motivating hackers during the target selection process due to the decentralise structure.

Yet the group has continued to mount kindred operations across the world, indicative of Anonymous' commitment to various freedoms and values, such as free access to information, freedom of expression and information sharing, and defending the principle and values of anti-globalisation against repressive regimes (Bardeau, Danet, 2011; Ludlow, 2010; Mansfield-Devine, 2011). For example, #OperationParis saw the hacking of hundreds of ISIS websites, shutting them down in an effort to quell the spread of false information and extremism online (McCrow-Young, Mortensen, 2021). During #OperationMinneapolis, Anons began hacking police services, publishing police officers' personal information on social media for harassment (known as *doxing)* and shutting down the Minneapolis Police Department websites after the death of George Floyd, a black Minneapolis man, at the hands of several police officers in 2020 (Castrodale, 2020; Franceschi-Bicchierai, 2020; Molloy, Tidy, 2020). Most recently, #OperationRussia included hacking several government websites as a response to the Russia- Ukraine war, to which Anonymous social media accounts deem as an illegal invasion (Everington, 2022; Faife, 2022).

The objectives of the present study are firstly, to assess mentions of a value system attributed to the hacktivists, and secondly to analyse communication in Anon internet relay chatrooms (IRC) to determine the ways in which Anonymous hackers choose their targets. In doing so, this study is contextualising itself during the 2012 Québec Maple Spring, as the timeline places the events post-Sabu, when Anonymous was characterised as more disorganised, and rife with dissent and confusion over messages, values, operations and target selections (Caldwell, 2015; Kelly, 2012). This study therefore will present the communications amongst Anonymous Québec members to determine if a congruency between Anonymous social media promoted values and those discussed in the chatrooms. This qualitative analysis has been used in the past to evaluate message posted on social media, looking at their official communications (via social networking sites like Twitter) as a way to better understand what is important to the movement (McGovern, Fortin, 2019). However, those communications are generally among Anonymous social media administrators and their social media followers, not all of which are active participants in hacking or target selection process. A post-hoc interpretation of the targets attacked, as well as values promoted by individuals who may not have participated in target selection creates a disconnect in our understanding of Anonymous' values at both stages of hacktivism: the hack and assertion.

While the data of Anonymous IRC has to be nuanced within its temporal context, its impact regarding our fundamental understanding of Anonymous' values, and hacktivism is not to be underestimated. Firstly, this is due to the limited data regarding the target selection process prior to the cyberattacks. According to Coleman (2020), Anonymous operations are often reactive, making it difficult to obtain conversations in IRC, granting

greater significance to the limited data that is available for analysis. Secondly, the consistent targets chosen in Anonymous campaigns suggests the continued relevance of the data. Given this perennial stability in targets chosen, we remain confident that the results derived from the forums can be generalised to other campaigns even those that have recently taken place.

Analyzing the ways Anonymous' values function in operation and target selection is vitally important in understanding the continued relevance of hacktivism worldwide. Since 2012, cybersecurity experts have warned of the increase in hacktivist operations around the world (AFP, 2017; Caldwell, 2015; Canadian Centre for Cyber Security, 2018). While the Maple Spring was one of the first Anonymous operations on Canadian soil, it was not the last. During the 2015 federal elections, Anonymous was the subject of controversy as they were credited for a number of hacks, having leaked confidential government documents from the Canadian Treasury Board with several news outlets (MacLellan, 2018). The documents revealed information regarding foreign spy stations, and Canadian government secrets of varying levels of importance in order to disparage the Canadian Conservative government, under the leadership of Canadian Prime Minister Steven Harper (AFP, 2017; MacLellan, 2018). These examples, among others, demonstrates the importance of ongoing research on Anonymous operations, as both Anonymous and hacktivist operations are not a thing of the past.

4. Methodology

4.1 Data

The main source of data for the present research derives from the content of two public chatrooms used by the Anonymous collective for approximately two months in 2012. Anonymous chatrooms were open access, making it possible for anyone to monitor them and collect data that is made available as timestamp log files. An account was connected to both chatrooms 24/7 and kept all the logs on a daily basis. Conversations took place on an online network called Internet Relay Chat (IRC) where chatrooms allow Internet users to share files, play games, or work with other users, no matter where they are in the world and whether they are in private or public chatrooms. These chatrooms offer the advantage of anonymity through services such as proxies that hide users' IP addresses (Décary-Hétu, Leppänen, 2013).

We focused on two chatrooms during a time where individuals connected with Anonymous Québec were particularly active, analyzing 447 files that contained a total of 21 megabytes of data. The conversations studied consist of 259,668 lines of text. The sixty most active individuals on both chatrooms accounted for, on average, 1,011 messages. If all those who used the chatroom are counted, including people who messaged only once, and the use of pseudonyms is taken into account (a single individual can send a message several times under a particular pseudonym, change to another pseudonym to send other messages, and then return to using the first pseudonym[2]), the number of most active individuals drops to 41. However, even this reduced number is not representative, as a small number of these individuals were very active, while others seldom participated.

The first chatroom analyzed presented a large amount of information about Anonymous' philosophy and preferred type of attack. The second

[2] A police officer, affected to the case, was met to help the understanding the use of nicknames and some slang and hacking terms.

chatroom was dedicated to the major operations in Québec during the Maple Spring events and not only provided information about Anonymous's philosophy, choice of targets, and attack techniques but also provided useful information about the context in which they were discussing many topics. The police officer who oversaw the investigation was interviewed on several occasions and provided additional information on technical terms as well as the meaning of certain comments. The investigation report for this case was also consulted. While there were many technical discussions and ask-for-help messages, the focus of this paper has been put on the social aspect of the movement.

4.2 Method

Analysis of conversations was performed using QDA Miner software. This qualitative analysis tool simplifies the processing of a large quantity of texts and made it possible to develop a coding system for vertical analysis of conversations. Each message was coded under a particular theme according to the subject of the conversation[3]. If participants posted on a particular topic in a continuing conversation, each message was coded. A message could also be coded under more than one topic. For example, part of a conversation could be about a potential target while part was about government corruption. Codes/themes were developed to capture the beliefs and motivations of individuals and specific events, or disputes were coded to allow for a synthesis of events. These steps made it possible to develop a more complete description of events and of the perceptions of individuals in the chatroom.

After the initial coding, we recoded specific topics to identify larger themes that characterized the discussions. This type of data processing has considerable advantages, including the ability to immerse oneself in the context of that time. Reading and analyzing the daily conversations of particular individuals in the Anonymous movement gave the researchers a chance to see them in their "natural" environment, while conversations between participants contained information that would not have been available through other methods (for example, through a survey). Our method provided an opportunity to access unique and privileged information, essential for the purposes of this work.

5. Results

In this section, we present the important themes that emerged from the analysis of the most prevalent topics discussed, as well as themes that provide insight into the Anonymous movement during the Maple Spring. In analyzing data derived from the chatrooms, five important themes emerged characterized by reoccurring discussions. They discussed the identity of the hacktivist collective, values such as freedom of expression, the media-centric immunity of mass media outlets, their target selection, and the aftermath of the attacks. The themes are explored and described in the following sections, using quotes from the data collected when appropriate.

5.1 Collective Identity

Previous studies have described Anonymous as a movement, a group, and a collective (Mansfield-Devine, 2011; McGovern, Fortin, 2019), demonstrating that there is no consensus on how Anonymous is defined and that discussing the movement's identity requires a great deal of interpretation. This may be due, in part, to the

[3] The logs in our sample were bilingual with a majority of messages in French, all text excerpts presented in this paper were translate in English and validated by authors.

decentralized nature of the group, with different definitions provided by different members, who may be influenced by the image of Anonymous depicted in the media. Similarly to that of prior research, our data included several attempts by Anonymous members to describe the movement, which involved both correcting others and justifying the group's existence:

> [04:17] <UserA> anonymous doesn't really have any 'rules'.
> [04:17] <UserA> just an ideology
> [04:21] <UserB> Anonymous is an idea ... a collective consciousness ... but certainly not an ideology
> […]
> [10:06] <UserC> anonymous is a group
> [16:34] <UserD> we're not a group ...

These excerpts indicate dissent but also show that seldomly a better answer is provided when the description of the group's identity is rejected by others. Anons seem to be providing a personal vision of the group rather than attempting to establish a unified identity for the whole movement. The lack of agreement and lack of negotiation over a particular identity suggests that at least the Anons in this chatroom were not bothered by the lack of a clearly stated collective identity. Other excerpts illustrate that coming up with a strict definition of Anonymous is problematic. Attempts in which the definition is more abstract are generally met with less dissent:

> [19:18] <UsersE> anonymous it's an idea ... a way of thinkin[g]
> […]
> [19:18] <UserF> anonymous its a cyber culture
> […]
> [06:22] <UserG> Anonymous is freedom of expression
> […]
> [16:45] <UserH> Anonymous is ideas, and people who want to help those ideas.
> […]
> [12:19] <UserI> It is a voice for the people that provides the opportunity to speak against what we think is outdated.

As these excerpts illustrate, Anonymous participants see the movement as many things – an idea, a cyberculture, even a voice for the people. Congruent with Coleman's (2020) perspective on Anonymous collective identity, the inclusive and participatory nature of the collective allows for a cohesive identity to exist in a more abstract way than with the collective identity of other movements There appears to be room for multiple definitions of its identity to coexist within the movement with the condition that they do not create fundamental conflicts. The discussions of identity also suggest that participants have larger goals – a vision in which may be important than the identity of the collective.

5.2 Freedom of Expression

The computer attacks by Anonymous during the Maple Spring were launched in response to Bill 78, the Québec government's attempt to control the student demonstrations that followed their announcement of a tuition increase. Anonymous saw the bill as an attack on citizens' freedom of expression and encouraged Anons to carry out a series of attacks against the government. These

attacks included disabling more than a dozen websites, including those of the Education Department, the Québec liberal party, The Ministry of Public Security of Québec and the Montreal police force as well as publicizing the possibility of online attacks against hotels and guests during the Montreal Grand Prix (Daudens, 2012; Montpetit, 2012). The analysis notes conversations frequently discussed the infringement of students' rights by the Québec government, suggesting that freedom of expression is an essential value for those who identify as Anonymous.

> [21:48] <UserS> Anonymous supports freedom of expression
> […]
> [10:15] <UserJ> Yeah, but let's remember that the student conflict it not really the subject here, Anon, it's more freedom of expression

It appears that, for some participants, the tuition increase was not the main reason for Anonymous involvement, suggesting a lack of interest in certain types of socio-economic debates. They weren't helping the student movement so much as fighting for individual and collective rights, suppressed by the government. As such, the UserJ's comment highlights how important freedom of expression is for the participants.

Free circulation of information is also among the values defended by participants in the chatrooms. Anonymous has targeted institutions that have attempted to control, limit, or monopolize public information. UserK succinctly summarizes this point:

> [16:44] <UserK> We are fighting for freedom of expression in all its forms and without censorship
> […]
> [21:07] <UserK> Actions on the Internet = the sole and broad purpose of fighting censorship and defending freedom of expression

We should probably note that censorship as presented above is probably indicative of the limits placed on protestors. It seems that UserK was seeing the limitations as describes in bill 78 was, in a way, censoring the students' messages by limiting protests.

5.3 Immunity of the media

Surprisingly, one topic that surfaced during analysis was that the media must be "protected" or, at the very least, should be immune from target selection. Indeed, not attacking the media seems to be one of their few clearly articulated rules (Olsen, 2012). Discussions suggest that the media should be protected from attacks because they agree with Anonymous about the value of freedom of information, which includes protecting the sources that disseminate such information:

> [20:32] <UserL> I am in favor of making the information about failures, faults, leaks, injustice ... etc. as widely [known] as possible.
> […]
> [17:05] <UserM> Attacking the media goes against the anonymous idea
> […]
> [19:05] <UserN we don't attack media, anonymous rule

[…]

[17:42] <UserO> if it's censorship, we should give them a message right? ... we don't attack the media ok ... but if it's censorship... it's not the same debate anymore, right?

Several Anons proposed launching attacks on a telecommunication provider and an important TV station, but other individuals quickly pointed out that one of the rules of Anonymous is that the media structure should not be attacked. This rule prompted questions in the chatroom when members realized that some of the media were censoring information.

[17:06] <UserP> and what happens when the media censors the people?

[…]

[16:59] <UserQ> [Telecommunication provider company] controls the pouting people who are little informed ... propaganda, disinformation, censorship, this provider is unworthy of having a news network!!!

Censorship by the media is at odds with Anonymous philosophy, which is based in part on supporting the free flow of information. The comments show that two core values of Anonymous – freedom of information (through the abolition of censorship) and protection of the media, which can be useful in making their activities visible and disseminating their message – were sometimes in conflict. In the end, protecting the media seems to be more important to Anonymous than their desire to fight censorship, as no hacking acts targeting any media outlets were recorded.

One possible hypothesis which could explain the importance of traditional media is that Anonymous depends on the media in fulfilling their goal: an attack that is presented in the media is seen as a proof of a successful attack, as it gives the movement greater impact on the political level by reaching the general population rather than just members. For example, UserTT reported to the group that their promotional video had been shown by a TV news station.

[14:33] <UserTT> our video is now playing on [TV news station]

[14:33] <UserTT> Victory!

For Anons, dissemination of their work in the media is an important reward as it provides them with a wider audience for their message and also creates a sense of belonging and excitement among participants in the movement.

5.4 Target Selection

Target selection was a recurring topic of discussion in the chatrooms and there were many brainstorming sessions of variable lengths. These sessions were characterized by conversations about ideas for potential targets, sometimes in response to current events.

[12:07:28] <UserR > Why not attack the government server?

[…]

[12:14:50] <UserR> Would you attack all government sites (and including AFE [the Student Financial Aid Service of Quebec]) or just some government sites?

[…]

[14:12] <UserS> Should we first decide on the target for a new attack: [prime minister], [minister of education], or [name of a popular event in Montreal]?

[…]

[18:41] <UserRR> It is necessary to attack good targets to send the right message

The process of selecting a target in the chatrooms seemed to be that hackers would suggest a good potential target to other users, who would then offer their opinions. The term "good target" was commonly used to designate a target that is in line with the philosophy and values of the movement (i.e., launching computer attacks to defend values such as freedom of expression and freedom of information) by targeting those they believe were contravening individual and collective freedoms. As mentioned in the previous excerpts, it was frequently observed that Anons were against the actions of the ruling political party at the time, making proposals to attack government websites an obvious "good target" to Anons in the chats. The opinions of other participants in the chatroom were solicited and some form of acknowledgement was sought before taking action. After discussion and informal approval, participants seem to reach a consensus on their next target fairly quickly:

[12:09:42] <UserT> Okay What's the attack today?

[12:09:45] <UserU> [police dept.] is a good target

[12:09:56] <UserV> I would say [police dept.]

[12:10:30] <UserV> Same tactic for weeks, they don't want to try anything. [police dept.] must go down.

[…]

[12:09:40] <UserW> Okay, what about the [opposition political party] then?

[12:09:43] <UserX> it's a good target

[12:09:58] <UserY> it's true

While participants provided opinions about which target should be selected and why, certain emotional responses to the events were observed to impact the selection of certain targets, particularly, when government entities were the subject of the discussion:

[21:08] < UserWA> fuck law 78

[21:08] < UserX > That's why it must be dropped

[18:56] <UserYQ> [UserED], anonymous is a symbol, we prove to the world that we can attack the government

[18:56] <UserYC> and the government is attacking the people

[…]

[09:33] < UserY> that we let a rotten government ... tell us what to do and what not to do ... disgust Ccharest and accolytes of this world that believes itself themselves gods when .... they are nothing more than worms

[10:52] <UserXA> I wish someone would take down the canadian conservative party website. Yesterday #DenounceHarper was trending on twitter, I was so happy

[17:09] < UserQRT> anyway... it's not the media [that's] the problem

[17:09] < UserQRT> it's government

The quoted excerpts suggest that Anonymous participants were consistent in carrying out their attacks according to an underlying ideological cause

and in defending the collective values of the movement even when emotions such as anger were present. However, when we compared these collective values with the individual values expressed by some chatroom users, we observed some discrepancies: some individuals proposed targets that were not related to the movement or carried out attacks without consulting others in the chat room:

> [19:03] <UserV> HACKED [Municipality A - adjacent to Montreal site URL]]
> [19:04] <UserZ> Seriously... why [[Municipality A]]?
> [19:05] <UserAA> [[Municipality A]] is a seriously bad target

By hacking into a municipality's website, rather than into targets that fit the group's philosophy, this user created a conflict between his/her actions and Anonymous principles. The interventions and actions suggest that he/she might have been hacking out of excitement rather than as a protest. Such cases were not common but illustrates that the personal values of some individuals occasionally clashed with the collective values of the movement.

> [23:08] <UserBB> No one understands why [[Municipality B]] was targeted ..... even we don't understand
> […]
> [14:25] <UserCC> Yesterday I hacked into a holiday camp site, the camp [name of the summer camp] xD joy!
> [14:26] <UserDD> Who cares?
> [14:26] <UserEE> I hope you're not proud of it
> [14:28] <UserFF> Yeah, it's not great ...
> […]
> [12:20] <UserRR> we should all attack FB for no particular reason >_>

It should be noted that Municipality B was located in the north part of the province and there was no obvious link to the events. Also, Facebook was also suggested as a target, despite UserRR's clear indication that attacking Facebook was not a part of the Maple Spring events, suggesting that the motivations of some participants may be incongruent with the general objectives of the Anonymous chatroom.

5.5 Reception and Perception of the Aftermath of Attacks

In the chatrooms, a few individuals posted about how they had managed to break into various unidentified systems, obtained personal information about police officers, government officials, or consumers, and then disseminated this information. Some mentioned that they had hacked into the servers of the Québec National Institute for Public Health (*Institute National de Santé Publique du Québec* (INSPQ)) and the Montreal Police Service (*Service de Police de la Ville de Montréal* (SPVM)). Anons were proud of their successes and happy to share them. A collective sense of joy and pride was visible in the chatroom after a success was reported through the use of emoticons (xD, :D) which illustrate a sideways smiley face indicative of happiness/joy.

> [20:47] <UserCC> I AM ENTERING IN http://www.inspq.qc.ca
> [20:48] <UserCC> and I AM AMDIN
> […]
> [21:03] <UserCC> I AM IN SERVER xD

[21:03] <UserQQ> How did you do all this with cmd

[21:04] <UserRR > Are you telling me that you are in the spvm server?

[21:04] <UserSS> I have all the files on the server: D

In addition to reporting intrusions into unidentified servers, participants claimed they had obtained information about the identities and banking data of ticket buyers for a popular event in Montreal, had identified clients of a bank that had many police officers as clients, and had obtained contact information for senior executives of a police department. It was not possible to confirm whether the intrusions and dissemination of confidential information boasted about in chatrooms had actually occurred. While the government website hacks discussed in the chatrooms were reported in the media; such as in the Toronto sun, the Globe and Mail and Radio-Canada, (Daudens, 2012; Montpetit, 2012; QMI Agency, 2012), others may have been invented to gain recognition from those in the chatroom.

6. Discussion

The present study describes the topics that were discussed in Anonymous' chatrooms during Maple Spring. While some studies (Kelly, 2012) argue that collective identity is important in creating a cohesive membership and helping determine the identity of individual members, others suggest that collective identity is often only the acknowledgement of a shared willingness to fight for a common cause rather than the embodiment of a particular identity held by members (Bennett, 2005). For Anonymous, how each member defines the group appears to be less important than the opportunities it provides for positive interactions with other members. Social movements are often formed not by individuals who identify only with a single group but by those who identify with various groups, creating a mosaic of protest identities operating under a single banner (Treré, 2015). This benefits groups such as Anonymous because, as participants are able to create their own meanings within a broad collective, the group as a whole is not limited to the types of campaigns in which it can engage (Machado, 2015). It is this fluidity and collection of coexisting identities which allow Anonymous to continue to organize, contrary to the characterisation of Anonymous as ineffective and rife with dissent (Caldwell, 2015; Kelly, 2012). Both the literature and our data support the view that Anonymous does not have one collective identity but rather collective identities, created through positive communication, particularly within the chat rooms. The excerpts have shown that the movement can encompass its values (through userG), its goals (UserH) its ability for change (UserI) and other abstract features. Given the number of cyberattacks undertaken but those on the chat during the Maple Spring, it seems the ways in which members define the group's identity is of little consequence in practice, having demonstrated their ability to carry out hacking operations. This seems more like a simple exercise than a fundamental requirement for participation.

An analysis of conversations between Anonymous members suggests that the philosophy of the hackers at this time was based on few, generally accepted, values. The emphasis on freedom of expression extracted from our data is in line with that of previous studies which suggest that freedom of expression is a central value for Anonymous members (Ludlow, 2010). The conversations

analyzed also demonstrate an interplay between ideas of freedom of expression, freedom of speech, and freedom of information, to which members sometimes seem to see as overlapping. This made it difficult to discern nuanced distinctions between said concepts presented by those using the chatroom. While students began their demonstrations as protesting tuition hikes, Anonymous only mobilized once Bill 78 was introduced, an act they saw as a limitation on protestors' freedom of expression. This mobilization was consistent with other actions by Anonymous, which have targeted traditional institutions of power that attempt to limit freedom of expression (Mansfield-Devine, 2011).

Our study highlights the importance of the media to the hackers as well. As mentioned earlier, suggestions targeting the media were easily ruled out, particularly those that suggested attacks on traditional media (media outlets). Anons in the chatrooms seemed to agree that traditional media should be protected and any dissent over this position was quickly and forcibly shut down, although this did not stop Anons from criticizing the media and questioning the role of telecommunication company providers and the control they have over the media. Participants in the chatrooms seemed aware that the concepts of freedom of information and censorship were closely linked. It must be noted, however, that other campaigns contradict this interpretation, as media outlets under state control have been the target of cyberattacks. RT, a Russian stat-sponsored media outlet was hacked during the early weeks of the Ukrainian invasion (Bonifacic, 2022). In this case, it can be suggested that the media outlets are not operating under a value of freedom of information, but an agent of the state, such as police forces, pushing government propaganda and misleading citizens. It is not surprising that Anonymous aligns those media outlets as another arm of government repression.

Protecting the media suggests that those in the chatrooms recognize that traditional media acts as a third-party broker between Anonymous and the public and any attack on the media could affect Anonymous's public image. As the movement is a political entity, the opinion of the general public matters. Losing public approval could have devastating implications for Anonymous, delegitimizing their campaigns, their actions, and their general cause. Another possibility is that Anons recognize the greater need for traditional media to spread their message to a larger audience. The conversations analyzed in our study show that Anonymous's goal is to use electronic civil disobedience techniques to denounce those who attempt to stifle freedom of expression. Such acts work best when they are disseminated to a large audience, encouraging the public to hold a particular opinion about the transgressor. This reflection among participants in the chat room is indicative of the importance of assertion, as described by George and Leidner (2019), even though these participants may not be involved in the social media aspect. While Anonymous discusses successful campaigns on their social media pages, these publications reach only those who follow Anonymous, many of whom presumably already support their message. Recognizing that the media is key to publicizing their actions to a wider audience suggests that Anonymous is aware that denouncing transgressors is most effective if the denunciation reaches the socio-political sphere, making everyday people aware of the abuses committed by traditional institutions of power.

The reaction to events carried out by Anonymous also demonstrated the importance of the media as an indicator of success. Anons in the chatrooms were excited about announcing that their actions had been mentioned on the news, because it meant that they had reached a larger audience. Recognition in the media validates actions against a chosen target, providing tangible proof of a successful operation and leading to validation from other members, as well as indicates a greater socio-political impact of an attack outside of solely the group and its targets. Anons celebrated news broadcasts about a successful operation, creating positive interactions between members. As Treré (2015) suggests, such interactions are important for a collective unity among members. While the individual motivations of each Anon in the chatroom cannot be determined, the data show that a successful operation had the secondary effect of promoting continued identification with other Anonymous members when the success was celebrated in the same chatrooms where targets had been selected.

Regarding consensus on target selection, few arguments or pushbacks were observed, demonstrating a sense of teamwork between Anons online. There seemed to be informal leaders who dominated the conversation and proposed potential targets, in line with the descriptions of the group by Coleman (2014) and Mansfield-Devine (2011). Two types of targets were observed in the present study: targets that were unanimously agreed upon good and bad targets. The good targets proposed in the chatrooms were largely traditional institutions of power: government, police, and political parties. Anonymous has focused on such targets in the past, which may explain why consensus was so easily reached (see Thackray, McAlaney, 2018). Proposing traditionally "safe" targets that are likely to incite positive reactions from other Anons also ensures positive interactions between members (Treré, 2015). Suggested targets that were quickly denounced included a children's camp, municipal governments, and the media. Those who proposed targets that were rejected were apparently either unaware that the proposed targets were considered out of bounds by the group or were motivated by individual interests (e.g.: for fun, the need to prove themselves, etc.). The instances of bad targets being attacked without the approval of others in the chatrooms, suggested that bad targets are considered those in which an attack would not send the appropriate message. This demonstrates that hacking is not the finality, but that target selection process is about sending the right message based on the same Anonymous values as those on social media. For that reason, targets such as distant municipalities and summer camps were considered outside the context of fighting for freedom of expression, and therefore a bad target.

There are a couple of limitations to this study that should be addressed. Its results are congruent with a decade of recent research arguing Anonymous, cyberattack targets are infringing on individual freedom of expression and social issues (Bardeau, Danet, 2011; Beran, 2020; Coleman, 2020; Ludlow, 2010). Regardless, in order to validate the results of the present study, an analysis of multiple target selection conversations among multiple Anonymous campaigns is needed. Future research should attempt to diversify the sampled population to achieve a greater level of generalisability. We also found that much of the conversation was dominated by a few participants. This affects the results as the largest number of Anons in the chatrooms took a more observational role, rarely

engaging in conversation. Results might have been different had all the participants participated equally. While this may not have had an effect on the values of the group, it might have affected the target selection process in particular, as it can be assumed that the more people engage in a discussion, the greater the chance of miscommunication and debate. Greater discussion could also demonstrate a wider variety of targets proposed which could have shown how other members in the chat rooms deal with targets that are not traditionally good targets frequently chosen by Anons.

7. Conclusion

The present study argues that Anonymous values have remained steady over the course of a dozen years in both the hacker and social media contingents of the group. The few values Anonymous members hold, particularly freedom of expression, freedom of speech and freedom of information are held in high regard and include rules as infallible values during the target selection process (particularly traditional media's immunity). Most notably, the media's importance cannot be understated, as it acts as a third-party broker between Anonymous's message and the general public. While more recent hacks against Russian TV would suggest otherwise, the context to which the media in Russia exists reinforces the impunity of the media (Bonifacic, 2022). The media itself is not protected, but for the freedoms of expression and information it represents. With the inclusion of social media for assertion, traditional forms of media are no longer the sole gatekeeper for wider audiences. Thusly, the media remains immune to cyberattacks so long as it remains an active proponent of these freedoms. This suggests the target selection process of future campaign will continue to evaluate the media's involvement and relationship to the state, as to ensure it reinforces the same values as the collective. As Operation Russia indicates, any deviation for the promotion of freedom of information can make a bad target a suitable target for cyberattacks.

The media also acts as a barometer for successful operations, as it shows proof of an attack having taken place, which in turn offers Anons the opportunity to gloat, feel joy, and interact positively with one another. Possibly, due to the search for positive interactions among members, which may explain why we observed mainly traditional Anonymous targets being suggested as suitable targets. Contrary to literature suggesting Anonymous is characterised by confusion or infighting amongst members, Anonymous seemingly thrives on a lack of identity, or rather, a collection of multiple personal identities to co-exist. These findings must remain in the context of both space and time, as 2012 is now in the past. However, Anonymous has mounted many similar campaigns; most recently in 2020, against U.S. police forces and 2022, against the Russian government, as proof of Anonymous' continued relevance (Everington, 2022; Franceschi-Bicchierai, 2020). For this reason, research must continue to analyse and understand this unique and impactful form of social activism.

References

1. Auty C., «Political Hacktivism: Tool of the Underdog or Scourge of Cyberspace?», *Aslib Proceeding*, vol. 56, issue 4, 2004, pp. 212-221.
2. Bardeau F., Danet N., *Anonymous : Pirates informatiques ou altermondialistes numériques ? : Peuvent-ils changer le monde ?* Éditions FYP, 2011.

3. Bégin-Caouette O., Jones G., «Student organizations in Canada and Quebec's "Maple Spring"», *Studies in Higher Education*, vol. 39, 2014, pp. 412-425.
4. Bennett L., «Social Movements Beyond Borders: Organization, Communication, and Political Capacity in two Eras of Transnational Activism», *Transnational Protest and Global Activism*, 2005, pp. 203-226.
5. Beraldo D., «Unfolding #Anonymous on Twitter: The Networks Behind the Mask», *First Monday*, vol. 27, n. 1, 2022.
6. Bergeron A., Delle Donne J., Fortin F., «Une Publication pour Dénoncer, Sans Plus : Description des Activités des Groupes Facebook S'identifiant au Mouvement Anonymous au Canada», *La Criminologie de L'information : État des Lieux et Perspectives*, vol. 52, n. 2, 2019, pp. 35-62.
7. Beyer, J., *Expect Us: Online Communities and Political Mobilization*, Oxford University Press, New York, 2014.
8. Bodó, B., «Hacktivism 1-2-3: How Privacy Enhancing Technologies Change the Face of Anonymous Hacktivism», *Internet Policy Review*, vol. 3, n. 4, 2014, pp. 1-13.
9. Caldwell T., «Hacktivism goes hardcore», *Network Security*, vol. 5, 2015, pp. 12-17.
10. Coleman, E. G., «Logics and Legacy of Anonymous», in Hunsinger, J., Allen, M., Klastrup, M., (Eds.), *Second International Handbook of Internet Research*, Springer, 2020, pp. 145-166.
11. Coleman, E. G., «Hacker politics and publics», *Public Culture*, vol. 23, n. 3, 2011, pp. 511-516.
12. Coleman, E. G., *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, Verso, 2014.
13. Conway, M., «Hackers as terrorists? Why it doesn't compute », *Computer Fraud and Security*, vol. 12, 2003, pp. 10-13.
14. Décary-Hétu D., Leppänen A., «Criminals and Signals: An assessment of criminal performance in the carding underworld», *Security*, vol. 29, n. 3, 2013, pp. 442-460.
15. Denning D. E., «Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy», in Arquilla, J., Ronfeldt, D., (Eds.), *Networks and netwars: The future of terror, crime, and militancy*, RAND, 2001, pp. 239-288.
16. George J. J., Leidner D. E., «From Clicktivism to Hacktivism: Understanding Digital Activism», *Information and Organization*, vol. 29, n. 3, 2019, pp. 1-45.
17. Guiton A., *Hackers : Au Cœur de la Résistance Numérique*, Éditions Au diable Vauvert, 2013.
18. Gunkel D. J., «Editorial: Introduction to hacking and hacktivism», *New Media & Society*, vol. 7, n. 5, 2005, pp. 595-597.
19. Hampson N. C. N., «Hacktivism: A New Breed of Protest in a Networked World», *Boston College International and Comparative Law Review*, vol. 35, n. 2, 2012, pp. 511-542. https://heinonline.org/HOL/P?h=hein.journals/bcic35&i=515
20. Jones K., Nurse J. R. C., Li S., «Behind the Mask: A Computational Study of Anonymous' Presence on Twitter», *Proceedings of the Fourteenth International AAAI Conference on Web and Social Media (ICWSM 2020)*, vol. 14, 2020, pp. 327-338.
21. Jones K., Nurse J. R. C., Li S., «Out of the Shadows: Analyzing Anonymous' Twitter Resurgence during the 2020 Black Lives Matter Protests», *Proceedings of the International AAAI Conference on Web and Social Media,* vol. 16, 2022, pp. 417-428.
22. Kahn R., Kellner D., "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging", *New Media & Society*, vol 6, n. 1, 2004, pp. 87-95.
23. Karatzogianni, A., *Hackers during cyber conflict. Violence and war in culture and the media. Five disciplinary lenses*, Routledge, New York, 2013.
24. Kelly B. B., «Investing in a Centralized Cybersecurity Infrastructure: Why Hacktivism Can and Should Influence Cybersecurity Reform Note», *Boston University Law Review*, vol. 92, n. 5, 2012, pp. 1663-1712.
25. Kenney M., «Cyber-Terrorism in a Post-Stuxnet World», *Orbis*, vol. 59, 2015, pp. 111-128.
26. Li X., «Hacktivism and the first amendment: Drawing the line between

cyber protests and crime», *Harvard Journal of Law & Technology*, vol. 27, issue 1, 2013, pp. 302-329.
27. Ludlow P., «WikiLeaks and Hacktivist Culture», *The Nation*, vol. 4, 2010, pp. 25-26.
28. Machado M. B., «Between Control and Hacker Activism: The Political Actions of Anonymous Brazil», *Historia, Ciencias, Saude—Manguinhos*, vol. 22, 2015, pp. 1531-1549.
29. Manion M., Goodrum A., «The Ethics of Hacktivism», *Journal of Information Ethics, suppl. Special Issue: New Challenges to Ethics and Law; Jefferson*, vol. 9, n. 2, 2000, pp. 51-59.
30. Mansfield-Devine S., «Anonymous: Serious Threat or Mere Annoyance?», *Network Security*, vol. 1, 2011, pp. 4-10.
31. McCrow-Young A., Mortensen M., «Countering Spectacles of Fear: Anonymous' Meme War' Against ISIS», *European Journal of Cultural Studies*, vol. 24, n. 4, 2021, pp. 832-849.
32. McGovern V., Fortin F., «The Anonymous Collective: Operations and Gender Differences», *Women & Criminal Justice*, vol. 30, n. 2, 2019, p. 1-15.
33. McKelvey F., «Digital Media and Democracy Tactics in Hard Times», *Canadian Journal of Communication*, vol. 35, n. 2, 2010.
34. Pendergrass W. S., «What is anonymous? A case study of an information systems hacker activist collective movement», [Doctoral Dissertation], Robert Morris University, 2013.
35. Raynauld V., Lalancette M., Tourigny-Koné S., «Political Protest 2.0: Social Media and the 2012 Student Strike in the Province of Quebec, Canada», *French Politics*, vol. 14, n. 1, 2016, pp. 1-29.
36. Renzi A., "Info-capitalism and resistance: How information shapes social movements", *Interface: A Journal for and about Social Movements*, vol. 7, issue 2, 2015, pp. 98-119.
37. Romagna M., "Hacktivism: Conceptualization, Techniques, and Historical View", *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp. 743-769.
38. Thackray H., McAlaney J., «Groups Online: Hacktivism and Social Protest», in McAlaney J., Frumkin L. A., Benson V. (Eds.), *Psychological and Behavioral Examinations in Cyber Security*, IGI Global, Hershey, 2018, pp. 194-209.
39. Treré, E., «Reclaiming, Proclaiming, and Maintaining collective identity in the #YoSoy132 movement in Mexico: An examination of digital frontstage and backstage activism through social media and instant messaging platforms», *Information, Communication & Society*, vol. 18, n. 8, 2015, pp. 901-915.
40. West, S. M., *Ambivalence in the (Private) Public Sphere: How Global Digital Activists Navigate Risk*. 7th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 17), 2017.

Sitography

1. AFP, «Canada: Hackers Targeted Country's 2015 Election, May Try Again», *SecurityWeek.Com,* 2017, June 18, [News Media], available on the internet site: https://www.securityweek.com/canada-hackers-targeted-countrys-2015-election-may-try-again
2. Anderson N., «"Literally" the day he was arrested, hacker "Sabu" helped the FBI", *Ars Technica*, 2012, May 4, [News Blog], available on the internet site: https://arstechnica.com/tech-policy/news/2012/05/literally-the-day-of-his-arrest-hacker-sabu-helped-the-fbi.ars
3. Beran D., «The Return of Anonymous», *The Atlantic*, 2020, August 11, [News Blog], available on the internet site: https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/
4. Bonifacic I., «Anonymous claims responsibility for Russian government website outages», *Yahoo!Finance*, 2022, February 26, [News Blog], available on the internet site:

https://finance.yahoo.com/news/anonymous-hacks-russia-websites-190045299.html
5. Canadian Centre for Cyber Security, *Cyber Threats to Canada's Democratic Process*, 2018, [Report], available on the internet site: https://cyber.gc.ca/en/
6. Castrodale J., «Hackers Jammed Chicago Police Scanners With Internet Classic "Chocolate Rain"», *Vice,* 2020, June 1, [Blog], available on the internet site: https://www.vice.com/en_us/article/889nw4/hackers-jammed-chicago-police-scanners-with-internet-classic-chocolate-rain
7. Daudens, F., «Les Anonymous piratent plusieurs sites du gouvernement du Québec», *Radio* Canada, 2012, May 21, [Blog], available on the internet site : https://web.archive.org/web/20130822085752/http://blogues.radio-canada.ca/surleweb/2012/05/21/anonymous-operation-quebec/
8. de la Hamaide, S., «Timeline of Paris Attacks According to Public Prosecutor», *Reuters*, 2015, November 14, [News Media], available on the internet site: https://www.reuters.com/article/us-france-shooting-timeline-idUSKCN0T31BS20151114
9. Everington, K., «Anonymous hacks into Russian firm running Ukrainian nuclear plant», *Taiwan News*, 2022, March 15, [News Media], available on the internet site: https://www.taiwannews.com.tw/en/news/4474025
10. Faife, C., «Anonymous-linked group hacks Russian space research site, claims to leak mission files», *The Verge*, 2022, March 3, [News Blog], available on the internet site: https://www.theverge.com/2022/3/3/22960183/anonymous-hack-russian-space-research-roscosmos-ukraine
11. Franceschi-Bicchierai, L., «"Anonymous" Is Going Viral Again, But Is It Really Back?», *Vice*, 2020, June 1, [Blog], available on the internet site: https://www.vice.com/en_us/article/wxq5mm/anonymous-minneapolis-george-floyd-protests
12. Jul C., «Hacktivism & Anonymous», *Calum Stuart*, 2013, July 30, [News Blog], available on the internet site: http://calumstuart.com/hacktivism-anonymous/
13. Kika T., «Anonymous hacks into Russian printers to deliver resistance information», *Newsweek*, 2022, March 21, [News Media], available on the internet site: https://www.newsweek.com/anonymous-hacks-russian-printers-deliver-resistance-information-1690269
14. Levesque C., «Grève Étudiante : Un vidéo d'Anonymous dénonce la loi 78 et lance l'Opération Québec», *HuffPost Québec*, 2012, May 20, [News Media], available on the internet site: https://quebec.huffingtonpost.ca/2012/05/20/anonymous-operation-quebec_n_1531489.html
15. MacLellan S., «Canada's Voting System Isn't Immune to Interference», *Centre for International Governance Innovation*, 2018, November 5. [News Media], available on the internet site: https://www.cigionline.org/articles/canadas-voting-system-isnt-immune-interference
16. Molloy D., Tidy J., «George Floyd: Anonymous hackers re-emerge amid US unrest», *BBC News*, 2020, June 1, [News Media], available on the internet site: https://www.bbc.com/news/technology-52879000
17. Montpetit J., «Anonymous hacking campaign in Quebec draws attention of Montreal police», *The Globe and Mail,* 2012, May 31, [News Media], available on the internet site: https://www.theglobeandmail.com/news/national/anonymous-hacking-campaign-in-quebec-draws-attention-of-montreal-police/article4224869/
18. Papadopoulos L., «Anonymous says Russia's spy satellites are now hacked. But the nation denies everything», *Interesting Engineering*, 2022, March 3, [News Blog], available on the internet site: https://interestingengineering.com/says-russia-denies-anonymous-hack-claims

19. Purtill J., «Anonymous takes down Kremlin, Russian-controlled media site in cyber attacks», *ABC News*, 2022, February 24, [News Media], available on the internet site: https://www.abc.net.au/news/science/2022-02-25/hacker-collective-anonymous-declares-cyber-war-against-russia/100861160
20. QMI Agency, «Quebec Liberal, government sites hacked», *Toronto Sun*, 2012, May 19, [News Media], available on the internet site: https://torontosun.com/2012/05/19/quebec-liberal-government-sites-hacked

doi: 10.14664/rcvs/243

Le aggressioni all'immagine in Turchia: un caso di studio di un fenomeno digitale preoccupante

Les atteintes à l'image en Turquie : étude de cas d'un fléau numérique ravageur

Tarnishing Reputation in Turkey: A case study of a devastating digital scourge

Julie Alev Dilmaç et Verda Irtiş***

Riassunto
La letteratura scientifica e i casi mediatici segnalano l'esistenza di comportamenti criminali sempre più diversificati legati all'uso delle tecnologie digitali.
Questi attacchi alla persona, che mettono in discussione la dignità e la reputazione dell'individuo, stanno assumendo sempre più importanza in Turchia. Si constata una recrudescenza degli attacchi online (es. furto di dati...), ma anche delle aggressioni all'immagine in cui le rappresentazioni del corpo della vittima sono condivise, in modo non consensuale, con una folla di utenti anonimi. Nonostante l'assenza di "fisicità" nello spazio digitale, le cyberviolenze sembrano ricondurre sistematicamente al corpo e mirano a rimettere in discussione non solo la reputazione, ma anche la dignità umana della persona. In questo articolo, si presenterà innanzitutto una rassegna della letteratura scientifica in Turchia e si tenterà di evidenziare come le cyberviolenze sono state trattate in questo contesto. In seguito, a partire dall'analisi di casi giornalistici, si offrirà una panoramica relativa alle condotte a danno dell'immagine registrate in Turchia tra il 2017 e il 2022. Si cercherà di individuare le ricorrenze legate alla violenza digitale che rientrano tra gli attacchi all'immagine sociale. Infine, si esamineranno le risposte giuridiche e giudiziarie proposte dalle autorità turche per combattere questi fenomeni.

Résumé
La littérature scientifique, mais également les cas médiatiques font aujourd'hui état de pratiques délinquantes toujours plus variées liées à l'utilisation des technologies numériques.
Ces atteintes à la personne, qui remettent en question la dignité et la réputation de l'individu, prennent de l'ampleur en Turquie. On constate une recrudescence des agressions en ligne (ex. vol de données…) mais aussi des atteintes à l'image par lesquelles les représentations du corps de la victime se voient partagées, de manière non consentie, avec une foule d'anonymes. Ainsi, malgré l'inexistence d'une quelconque « corporalité » dans l'espace numérique, les cyberviolences semblent systématiquement porter sur le corps et par là, visent à remettre en question non seulement l'image sociale (la réputation) mais aussi l'image personnelle (la dignité humaine) de la personne.
Dans cet article, il s'agira tout d'abord de rendre compte de la littérature scientifique en Turquie et de voir comment les cyberviolences ont été appréhendées dans ce contexte. Puis, dans un deuxième temps, à partir de cas journalistiques, nous proposerons une vue d'ensemble des cas d'atteinte à l'image recensés en Turquie entre 2017-2022. Nous tenterons de dégager les récurrences liées aux violences numériques relevant des atteintes à l'image sociale. Enfin, nous nous pencherons sur les réponses juridiques et judiciaires proposées par les instances turques en vue de combattre ces phénomènes.

Abstract
The scientific literature and media report today on varied delinquent practices linked to digital technologies.
These attacks towards the person, which offend the dignity and tarnish the individual's reputation, seem on the rise in Turkey. There is an upsurge in online attacks and damages to the image by sharing representations of the victim's body, without his-her consent, with a crowd of anonymous people. Thus, despite the non-existence of any « corporality » in the digital world, cyber violence seems to be linked to the body and thereby aims to challenge not only the social image (reputation) but also the personal image (human dignity) of the individual.
In this article, first, we will describe the scientific literature to explain how cyber violence has been analyzed in the Turkish context. Then, in a second part, based on journalistic cases, we will offer an overview of the cases of image damage recorded in Turkey between 2017-2022. We will try to identify the recurrences linked to digital violence related to social image attacks. Finally, we will look at the legal and judicial responses proposed by the Turkish authorities to combat these phenomena.

Key words: cyberviolences, Turquie, atteintes à l'image, corps, monde numérique

* Enseignante-Chercheuse en Sociologie, Université Galatasaray Département de sociologie, Centre pour la recherche sociale (TAM). Membre Associé au centre PHILéPOL, Paris Descartes, Sorbonne Cité.
** Enseignante-Chercheuse en Sociologie, Université Galatasaray Département de sociologie.

1. Introduction[1]

La littérature scientifique mais également les cas médiatiques font aujourd'hui état de pratiques délinquantes toujours plus variées liées à l'utilisation des technologies numériques. Par exemple, il suffit de taper « danger snapchat » sur Google pour obtenir pas moins de 899 000 résultats, alertant sur les risques auxquels s'exposent les internautes en utilisant cette application (Déage, 2018). Outre le piratage, le vol et le partage de données volées (appelé aussi *doxing*) (Douglas, 2016), on observe de plus en plus d'atteintes aux personnes et à leur image (que celle-ci soit personnelle, virtuelle ou sociale…) dans l'espace numérique : parmi les cyberviolences (Blaya, 2013) désormais communes et théorisées, on retrouve par exemple le harcèlement numérique (Girot, 2005), le *happy slapping*, le *bashing* (Bernard Barbeau, 2012), le *revenge porn*, le « sexting secondaire » (Robitaille-Froidure, 2014 ; Desfachelles, Fortin, 2019), « le bifflage[2] », le harcèlement ou l'humiliation en ligne ; à celles-ci viennent s'ajouter d'autres formes d'incivilités telles que l'intimidation et les menaces, les rumeurs, la diffusion de scènes d'agression en ligne, la sollicitation répétée de photographies intimes, les violences verbales (moquerie, insulte), psychologiques ou morales (dénigrement), l'imposture et le vol d'identité...

L'utilisation des réseaux sociaux génère un phénomène de panique morale (Boyd, 2014, p. 211) et notamment chez les adultes qui dénoncent les dangers de ces technologies de communication menaçant les nouvelles générations. Or, bien qu'un grand nombre d'études se soient plus particulièrement concentrées sur le cas des adolescents et des *digitales natives* (grands consommateurs de réseaux sociaux et par conséquent, plus vulnérables aux risques liés à l'utilisation d'Internet), ces agressions numériques semblent toucher toutes les populations, et ce, quel que soit leur âge.

Les nouvelles technologies ne serviraient plus alors uniquement à communiquer ou à s'informer, mais seraient aussi utilisées pour humilier, divulguer des informations, dévoiler des détails compromettants, caricaturer, trier et classifier les individus en vue de les stigmatiser. Internet et ses dispositifs permettraient également aux personnes de faire voir à autrui ce qu'elles ne pourraient pas lui montrer dans la vie réelle, ou de le forcer à regarder ce qu'il ne consent pas à voir.

Dans le cyberespace, trois modalités spécifiques au monde numérique semblent favoriser ces incivilités. Tout d'abord, il semblerait qu'Internet ait modifié les manières de « regarder ». Les dispositifs technologiques proposés donnent à l'Internaute la possibilité d'analyser, de découper, de recadrer, de « saisir » les images de l'Autre dans les moindres détails. Les imperfections d'Autrui ainsi que ses « secrets entraperçus » (Vincent-Buffault, 2004, p. 43) peuvent par la suite être dévoilés à une foule d'anonymes, groupe d'inconnus qui les jaugeront à leur tour. Dans les « régimes de visibilité » (Mongin, 2004, p. 220), les clichés sont ainsi « consommés » par des individus mus par une insatiable « voracité oculaire » (Vincent-Buffault, 2004, p. 43). Il va sans dire que ces nouvelles manières de regarder peuvent présenter un danger : l'image, qui déjà réifie la personne, est alors « regardée » sans que son histoire ne soit prise en compte. Sur Internet, l'individu n'est *que* ce qu'il est représenté.

[1] Nous tenons à exprimer nos remerciements à Zeynep Karahasanoğlu pour son engagement soutenu dans cette recherche et pour son aide quant à la collecte d'informations.

[2] Être giflé avec le sexe d'un tiers pendant que d'autres filment. Les images ont été diffusées sur les portables des lycéens (exemple disponible sur le site Internet : http://www.ouest-france.fr/2012/11/30/pays-de-loir/Un-lycéen-poursuivi-pour-bifflage).

Or, si les moindres détails du corps peuvent être révélés et partagés par un tiers sans l'obtention au préalable du consentement de la personne concernée par l'atteinte, on constate aussi que divers moyens sont employés par les acteurs eux-mêmes en vue de « divulguer » des aspects de leur propre vie privée et de susciter le regard de leurs pairs : partage de photographies intimes, mise en ligne de films personnels, utilisation de webcams… Internet est alors un espace où l'on regarde l'Autre et où l'on souhaite être vu. Ceci semble d'ailleurs être une prérogative : sur la Toile, le corps doit être mis en scène, s'exhiber et doit chercher à tout prix à attirer les regards (Dilmaç, 2015) en vue de ne pas tomber dans l'oubli.

La deuxième modalité spécifique à la Toile qui favoriserait les cyberviolences relèverait des formes de sociabilité singulières aux réseaux sociaux. Dans le monde numérique, les frontières entre le privé et le public tendent ainsi à se brouiller, entraînant un bousculement des codes de conduite censés régir ces deux domaines. Le secret et le caché qui relevaient jusqu'ici de la vie privée, sont sur Internet, exposés et dévoilés. L'anonymat, l'invisibilité, la rapidité et la déshumanisation entraînés par Internet auraient pour effet de provoquer une « désinhibition en ligne » (Suler, 2004 ; Valkenburg, Peter, 2011) : clivée d'une partie de leur individualité dans le cyberespace, les individus seraient plus à même de manifester leur intimité ou de tenir des propos qu'ils ne tiendraient pas dans le monde physique. Desfachelles et Fortin (2019, p. 337) soulignent par exemple que « les adolescent·e·s reconnaissent être plus entreprenants et agressifs dans leur utilisation virtuelle d'images et de mots suggestifs que dans les communications en personne ».

Il n'est donc pas étonnant de constater qu'avec le développement des technologies, on assiste également à un nouveau rapport à la sexualité : derrière les écrans, les individus seraient plus enclins à « contourner la norme de réserve relationnelle » (Clair, 2008, p. 35-38) et à s'engager dans la recherche de plaisirs plus subtils (Casilli, 2010) tels que la « cybersexualité » ; celle-ci leur permettrait de nourrir des fantasmes, tout en les dispensant de la rencontre (Breton, 2001) dans la vie réelle. Les conversations sur les réseaux se voudraient désormais plus « sexualisées » : la pratique du « sexting », à savoir l'envoi de « contenu sexuellement explicite visuel ou non, envoyé par SMS, « smartphone » ou en ligne comme sur les réseaux sociaux » (Ringrose *et al.*, 2012, 9), semble ainsi s'être répandue sur la Toile. Certaines études montrent que parler de sexualité à des inconnus sur Facebook, d'évoquer des sujets intimes comme l'amour ou le sexe (Davis, 2010 ; Schouten *et al.*, 2007) entre amis, ou encore de partager des contenus suggestifs serait des pratiques plutôt banalisées aujourd'hui ; elles relèveraient d'une activité « amusante ou de flirt » (Cooper *et al.*, 2016). Les adolescents utiliseraient les réseaux en vue d'échanger avec le sexe opposé, de révéler leurs sentiments, bref d'expérimenter la séduction (Metton, 2004). Lachance (2012) va d'ailleurs jusqu'à affirmer qu'une partie de la sexualité des jeunes se vivrait désormais sur Internet.

Enfin la troisième modalité qui se doit d'être notée : Internet favoriserait un nouveau rapport au corps qui augmenterait le risque d'atteintes dans le cyberespace. Ainsi, bien qu'absent physiquement, le corps va de même être sollicité et être placé au cœur de la sociabilité en ligne : celui-ci va être constamment mis en scène à travers l'image en vue de créer du lien et de prouver que l'on existe ; il aide

les acteurs à faire acte de « présence » sur Internet (Casilli, 2010). Autrement dit, l'informatique engage les corps des utilisateurs (Flichy, 2009, p. 163). De nombreux stratagèmes sont également employés pour l'exhiber : on le dénude, on en partage des représentations visuelles, on l'embellit par des filtres, on le met en scène dans des vidéos, on change son portrait, on rend compte de ses performances, on choisit un Avatar (à savoir une « incarnation »), on le montre sous toutes ses formes… Dans son analyse effectuée auprès d'adolescentes, Huerre (Huerre *et al.*, 2013) montre que celles-ci se mettent en scène dans des tenues légères dans le but d'être rassurées sur leurs corps par leurs pairs. Ainsi, c'est en laissant des « traces corporelles » sur les réseaux que l'individu prouve qu'il *existe* sur la Toile et qu'il peut espérer obtenir une certaine reconnaissance sociale. Rien de pire dans le monde numérique que de refuser « l'injonction à la visibilité » (Haroche, 2011, p. 80) et risquer de tomber dans l'oubli.

1.1 Le cadre conceptuel

Ces modalités du monde numérique seraient ainsi susceptibles de faciliter la tenue et la dissémination d'actes de violence (Blaya, 2013), désignés désormais de « cyberviolences » : celles-ci relèveraient de « l'usage des différents outils de connexion en ligne ou par téléphone mobile dans le but d'insulter, harceler, humilier, répandre des rumeurs, ostraciser, exercer une coercition externe sur un individu qui ne peut pas facilement se défendre seul ou qui subit une domination » (Blaya, 2013, p. 33). Ces persécutions différeraient des autres types de violence et notamment du harcèlement numérique, car elles ne s'inscrivaient pas forcément dans la durée et ne seraient pas répétitives.

La littérature scientifique fait d'ailleurs état de termes variés en vue de désigner ces agressions : on retrouve par exemple le cyber sexisme qui renvoie à « des faits qui font violence aux individus, se déploient à travers le cyberespace, contaminent l'espace présentiel ou réciproquement et qui visent à réitérer les normes de genre ciblant distinctement garçons et filles ; bref, à mettre ou à remettre chacune et chacun à la "place" qui lui est assignée dans le système de genre » (Couchot-Schiex *et al.*, 2016, p. 57).

Or encore, le cyberharcèlement : ce phénomène théorisé pour la première fois en 1975 par le psychologue suédois Anatol Pikas sous l'appellation de *mobbing*, fut par la suite rendu populaire par Dan Olweus en 1978 ; ce dernier s'attacha à décrire les modalités du « bullying » dans le milieu scolaire, autrement dit un lynchage (Blaya, 2018) individuel ou collectif à caractère itératif qui établirait un rapport asymétrique entre la victime et son agresseur. De nombreuses autres analyses prendront appui sur ces études pionnières (ex. Hinduja, Patchin, 2008 ; Grigg, 2010) et certaines introduiront une logique de continuité entre harcèlement en ligne et hors-ligne (Macilotti, 2019 ; Stassin, 2019 ; Baldry *et al.*, 2015 ; Livingstone *et al.* 2011 ; Kowalski *et al.*, 2008 ; Willard, 2007) alors que d'autres se focaliseront sur l'impact psychologique de ces violences, et notamment le sentiment de colère, de confusion, et de tristesse (Carlson, 1987) provoqué par ces agressions chez l'individu visé.

Au vu du développement de ces types d'incivilités numériques, on constate également l'émergence de termes plus spécifiques, comme par exemple celui de cybertraque (attaque par laquelle le harceleur suit sans relâche les moindres faits et gestes de sa victime sur Internet, en lui faisant savoir par l'envoi

répété de messages injurieux par exemple que celle-ci est épiée) ou encore celui de cyberhumiliation. Ce dernier renvoie au fait de faire « tomber de son piédestal » la victime, de fragiliser sa position sociale, bref de salir son « image » publique ; ici, c'est la réputation qui tente d'être bafouée et pour ce faire, un seul acte infamant suffit. L'envoi de messages incendiaires désigné en anglais de *flaming* (Vrooman, 2002 ; O'Sullivan, 2003 ; Jane, 2015), l'usurpation d'identité (*impersonation*), la révélation de l'orientation sexuelle (*outing*) représentent ainsi des exemples concrets de cyberhumiliation. Dans ces cas, l'éreintement répété n'est pas de mise (et donc ne peut être défini comme la modalité phare de la cyberhumiliation), ce qui la différencie du harcèlement numérique.

D'autres vocables vont être aussi usités en vue de désigner les atteintes particulières portant majoritairement sur le corps, et ce, malgré l'inexistence d'une quelconque « corporalité » dans le monde numérique : en effet, dans le cas où celui-ci serait dénigré, on pourra parler de grossophobie, de « *body-shaming* » ou encore de « *slut shaming* ». Le corps sur Internet peut également être, mis en scène (on lui fait « prendre la pose »), divulgué (on dévoile l'intimité de la victime, on partage des images prises en dessous des jupes des jeunes filles – « *upskirting* »), stigmatisé (et notamment celui de la communauté LGBT+ ou des individus en situation de handicap) détourné, ridiculisé, partagé… Ainsi, c'est à travers le corps (et ses représentations virtuelles) que les atteintes à l'image semblent s'opérer. Par ces actes humiliants et dégradants effectués en ligne, les agresseurs remettraient en question non seulement l'image virtuelle, mais aussi l'image sociale (la réputation) et l'image personnelle (la dignité humaine) de la personne.

La pornodivulgation (désignée aussi sous le terme de « *revenge porn* ») est d'ailleurs un exemple probant de ce type d'atteinte : l'acteur, pour se venger de son partenaire ou lui faire du mal, va l'humilier en diffusant, à son insu, des contenus privés en révélant son nom et ses coordonnées pour que des messages dégradants d'inconnus lui soient envoyés et que sa réputation soit détruite (Hall, Hearn, 2019). Le terme « *revenge porn* », pourtant banalisé dans la littérature pour décrire ces atteintes à l'intégrité, est cependant problématique : ce concept évoque une vengeance qui supposerait qu'un acte réprobateur et humiliant ait été commis par la victime au préalable, encourageant l'individu blessé par cette action à répliquer en diffusant des images intimes et à devenir agresseur à son tour. Cette appellation fait donc implicitement de la violence perpétrée une action pleinement « justifiée » (Aksoy Retornaz, 2021), marquant au passage un transfert de responsabilité. De plus, par ce terme, la « revanche » semble être le seul motif sous-jacent au comportement : or, on le sait, les cyberattaques ont aussi pour objectif d'humilier, de salir la réputation, de blesser, d'intimider, et peuvent même dans certaines circonstances être commises par pur amusement ou être totalement gratuites (Bartow, 2009). En outre, l'allusion à la pornographie pour désigner ce type de violence pose, elle aussi, un problème : en effet, cela suppose que les images mettent en scène un rapport sexuel consenti entre adultes qui ne supposent aucune intimité devant être soustraire au regard des autres ; la diffusion massive de ces matériaux visuels serait même souhaitée, car l'image ici est monnayée (Beyens, Lievens, p. 33). Pour remédier à ce problème de conceptualisation, Citron et Franks (2014, p. 346) proposent de parler de « pornographie non consensuelle », alors que d'autres auteurs

(Desfachelles, Fortin, 2019) affirment qu'il serait plus approprié de parler de « sexting secondaire », et notamment lorsque nous serions en présence d'un individu qui aurait consenti à la relation en pensant que celle-ci resterait privée, mais qui n'aurait nullement donné son aval pour le dévoilement de cette intimité.

1.2 Le cas turc

Ces atteintes à la personne, qui remettent en question la dignité et la réputation de l'individu, semblent prendre de l'ampleur en Turquie. On constate en effet une recrudescence des agressions en ligne (ex. usurpation d'identité, discours de haine, vol de données…) mais plus particulièrement des atteintes à l'image où les représentations du corps de la victime se voient partagées, de manière non consentie, avec une foule d'anonymes sans que la personne persécutée ne puisse répliquer. D'après le rapport de l'Association de la connaissance sociale et de la communication (*Toplumsal Bilgi ve İletişim Derneği*) (2021) une personne sur cinq en Turquie se dit avoir déjà été victime de cyberviolences ; la catégorie des 18-32 ans serait la plus touchée avec une personne sur trois s'étant déjà fait agresser dans le monde numérique. L'étude rapporte également des différences entre les sexes : pour les femmes, l'atteinte porterait plus sur leur image et leur apparence physique ; 51% d'entre elles se feraient harceler dans le monde numérique par le biais de messages écrits, vocaux, mais aussi vidéos et 46% seraient victimes de traque en ligne (*stalking*). Pour les hommes, c'est leur orientation politique qui serait plus prise pour cible. En outre, trois plateformes seraient privilégiées par les persécuteurs : Instagram (53%), Facebook (35%) et Twitter (19%), poussant les individus à réagir en bloquant l'accès à leur profil (65%) ou en formulant une plainte au site hébergeur (39%)[3].

Dans le cas turc, on observe là aussi beaucoup de termes relevant des atteintes à l'image évoquant les attaques liées au corps : on parle par exemple de « dévoilement » (*ifşa*), « de contenus à caractère sexuel » (*cinsel içerikli*), de harcèlement sexuel (*cinsel taciz*), d'obscénité (*müstehcenlik*), de maltraitante en ligne (*siber istismar*), de flirt violent (*flört şiddeti*), de violences digitales (*dijital şiddet*), de maltraitance d'enfant en ligne (*çevrimiçi çocuk istismarı*) (Çalışkan, 2019). Bien que ces termes soient nombreux, on constate que ceux-ci sont moins spécifiques que les concepts d'autres sociétés, et notamment les pays anglophones où le fléau des cyberviolences est bien plus développé et théorisé. Or, cela ne remet pas en question l'impact de ces agressions sur l'image sociale des personnes : les cyberviolences portent atteinte à ce que l'individu représente, à savoir au nom, au statut, à la réputation, la dignité de la personne.

La place du corps en Turquie doit également ici être explicitée : celui-ci est en Turquie au cœur de nombreux débats aussi bien sociaux que politiques et a une place particulière. Le corps des femmes est ainsi souvent considéré comme LE cheval de bataille des discours et des controverses politiques : on questionne son revêtement, à savoir si le corps doit être voilé ou dévoilé, et ce, en quelles circonstances. Le corps est de même très présent dans les discours médiatiques turcs : les faits divers mentionnent ainsi diverses formes de violences faites aux femmes (violences conjugales, violences de flirt, harcèlement, viols, féminicides…) et où le corps est victime de maltraitance. Dans un autre cas de figure, on relève aussi des atteintes au corps

[3] Digital Şiddet.org [En ligne], disponible sur le site Internet : https://dijitalsiddet.org/wp-content/uploads/2021/09/konda-rapor-8eylul.pdf

féminin à travers les crimes d'honneurs, homicides visant à punir les acteurs perçus comme ayant agi de manière transgressive (adultère, relation sexuelle avant le mariage, flirt…). Bien entendu, le corps des hommes peut aussi se voir mutiler suite à la souillure des femmes qui leur sont attachées. Ils se doivent ainsi de répliquer aux affronts, réaction qui leur permet de prouver, mais surtout « d'exhiber » leur virilité.

Le corps des femmes et sa protection sont d'ailleurs des sujets qui ont été amplement évoqués, et notamment après la décision des autorités turques de se retirer de la convention d'Istanbul qui jusqu'ici protégeait plus qu'aujourd'hui la population féminine quant aux diverses atteintes au corps dont elles pouvaient être victimes[4] (ex. féminicide, sanction des crimes d'honneurs…). D'autres populations, quant à elles, dont le corps et la présence dans la société seraient totalement niés : c'est le cas par exemple des membres de la communauté LGBT+ qui, selon les autorités turques, « n'existeraient pas ».

À un niveau plus global, un contrôle des corps semble de même s'être instauré avec le nouveau gouvernement en place qui remet en cause toute expression de la subjectivité des acteurs dans l'espace public ; le corps se doit alors d'être discipliné, contenu, passif.

La littérature turque fait aussi état de la pression de quartier (*mahalle baskısı*) qui impose aux individus une autocontrainte des corps afin d'éviter les rumeurs et les ont-dits pouvant mettre à mal leur réputation, leur image sociale et dans certains cas, les empêcheraient d'intégrer le marché matrimonial. L'individu doit alors constamment jouer sur le caché, le voilé, prouvant ainsi qu'il connaît la honte (*ayıp*) ; il doit éviter les comportements inappropriés (*uygunsuz*) et esquiver le dévoilement (*ifşa*) de ses secrets.

Le corps en Turquie est donc à la fois un support de valeur, de retenue, d'une morale qui peut être contrôlé, sanctionné par des individus extérieurs. Les violences numériques qui mettent à mal l'image des personnes et dévoilent leur corps ont alors un impact dévastateur qui peut entraîner la déchéance sociale non seulement de la personne, mais aussi de toute sa famille. Ces contraintes qui imposent aux individus une retenue de leur corps peuvent expliquer, en partie, pourquoi de plus en plus de personnes en Turquie usent des réseaux sociaux pour faire des rencontres. Ces espaces semblent ainsi favoriser l'émancipation des conduites, mais aussi d'entretenir des relations sous couvert d'anonymat.

L'« image » telle qu'elle sera traitée dans cet article ne doit donc pas être uniquement envisagée comme la « représentation réifiée » de l'individu, mais comme l'ensemble des éléments de la personnalité, des informations personnelles et intimes qui s'incorporent dans la notion de vie privée, et qui, s'ils sont divulgués sans consentement préalable, portent atteinte à l'intégrité. Les cyberviolences s'établissent ainsi par un regard oblique posé sur la personne et son corps, et correspondent à une manière toxique de regarder (Mongin, 2004, p. 225).

Le fléau des violences numériques semble d'ailleurs avoir attiré l'attention des chercheurs turcs de diverses disciplines, ce qui explique le nombre important d'études effectuées ces dernières années en Turquie visant à cerner les modalités de ces

[4] Pour les experts, concernant les crimes d'honneur, la situation était d'autant plus préoccupante que les sanctions pénales proposées ne leur semblaient pas assez dissuasifs. Cf. https://www.ohchr.org/fr/press-releases/2022/06/experts-committee-elimination-discrimination-against-women-commend-turkiye
(Nations Unies, Droits de l'Homme, Haut-Commissariat, « Le retrait de la Türkiye de la Convention d'Istanbul préoccupe particulièrement les membres du Comité pour l'élimination de la discrimination à l'égard des femmes », 15 juin 2022).

atteintes à l'image. En outre, ces agressions numériques auraient augmenté de 20% avec la pandémie du Covid-19 (Milliyet, 30.09.21) et l'âge du premier usage d'Internet aurait chuté exposant ainsi les enfants à ces risques potentiels dès l'âge de deux ans (*Istiklal*, 14.04.22). Or, malgré les prises de conscience face aux dangers des plateformes communicationnelles, les réponses judiciaires censées sanctionner les cyberintimidations sont quasi inexistantes, ce qui plonge les victimes dans un flou juridique venant renforcer leur désarroi.

Dans cet article, dans un premier temps, nous évoquerons en détail la littérature scientifique turque concernant les violences numériques et évoquerons le cas particulier de l'application Potinss, téléchargée par les adolescents et dont l'utilisation souleva des débats et mis la lumière sur des actes malveillants relatifs aux nouvelles technologies. Puis dans un second temps, il s'agira, à partir de cas journalistiques de deux journaux à grand tirage (*Hürriyet* et *Birgün*) identifiés pour la période 2017-2022, de proposer une vue d'ensemble des cas d'atteinte à l'image recensés par les médias en Turquie. Nous tenterons, à partir de ces matériaux de dégager les récurrences liées à ces cyberviolences spécifiques et de cerner les modalités propres de ces phénomènes : quels outils communicationnels sont utilisés ? Quels supports de l'image sont privilégiés dans ces attaques ? Qui sont les victimes et les agresseurs ? Comment s'opère l'agression ? Existe-t-il une continuité observable entre l'expérience en ligne et hors ligne ? Ces violences numériques sont-elles spécifiques aux mineurs et touchent-elles essentiellement les femmes, par exemple ?

2. État des lieux des recherches en Turquie

Beaucoup de recherches sur les cyberviolences ont été conduites ses dernières années[5] en Turquie, démontrant encore une fois l'urgence à cerner ce phénomène : ces études portent aussi bien sur les visions sociétales et globales de la cyberintimidation (Tamer, Vatanartıran, 2016), que sur les perceptions particulières des jeunes (Arsoy, Ersoy, 2015), qu'il s'agisse d'enfants (Arslan *et al.*, 2012) ou d'adolescents (Beyazit *et al.*, 2017). L'une des premières études réalisées a mené Erdur-Baker et Kavşut (2007) à interroger 228 lycéens âgés de 14 à 19 ans en vue de cerner leurs éventuelles expériences de cyberintimidation. Les chercheurs ont ainsi pu démontrer que les étudiants de sexe masculin étaient à la fois les plus impliqués dans l'agression, mais aussi les plus exposés ce type d'attaques que leurs pairs féminins. L'étude a également révélé une relation positive entre la fréquence d'utilisation d'Internet et le fait d'être un persécuteur ou une victime, alors que d'autres variables telles que le type d'école, le revenu économique familial, l'âge et la classe sociale n'avaient pas d'impact sur l'expérience des violences numériques.

Certains chercheurs ont de même tenté de voir s'il existait une corrélation entre la fréquence des usages d'Internet et le cyberharcèlement (Akça *et al.*, 2015 ; Özdemir**,** Akar, 2011). Des divergences dans la littérature existent en outre quant à savoir si

[5] Parmi lesquelles par exemple : Önay Doğan B., Ertürk Y. D., Aslan P., « Facebook Kullanıcısı Kız Çocuklarına Yönelen Zorbalık Odaklı Siber Tacizin Cinsel Tacize Dönüşümü: Gazete Haberleri Üzerinden Betimsel Bir Değerlendirme », *Etkileşim*, nº 2, 2018, p. 36-55; Şener M. T., Set T., Dursun O. B., « Güvensiz İnternet Kullanımı İle İlgili Bir Olgu Sunumu: Sanal Taciz », *Türk Aile Hekimleri Dergisi*, vol. 16, nº 3, 2012, p. 127-129. Aksaray S., « Siber Zorbalık », *Çukurova Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi*, vol. 20, nº 2, 2011, p. 405-432.

l'humiliation réelle se distingue de celle effectuée dans le monde numérique (Dilmaç, 2017) ou si la cyberviolence n'est autre qu'un prolongement des intimidations entre pairs prenant forme dans le milieu scolaire (Erdur-Baker, Kavşut, 2007 ; Uçanok *et al.*, 2011). Des différences de genre aussi seraient à reporter : dans son analyse effectuée avec 717 participants de 16-17 ans, Topçu (2008) montre par exemple que sur les 47.6% d'individus se disant à avoir déjà été intimidé numériquement, les garçons endosseraient plus le rôle d'agresseurs que les filles ; pour l'auteur, cela s'expliquerait par le fait que ces dernières seraient plus empathiques que leurs pairs masculins et donc, moins enclines à humilier un tiers. Çifçi (2010, p. 114) va plus loin en affirmant que la violence provoquée des actes d'humiliation, de harcèlement et de traque sur le Web permettrait aux garçons de démontrer leur force et leur courage mais aussi de conserver leur statut ; bref, en dénigrant l'Autre, ils affirmeraient leur virilité.

L'application « Potinss » et les problèmes engendrés par son utilisation massive ont dû encourager ces recherches ciblées sur les adolescents. Créée par deux lycéens, cette application visait à transposer dans le cyberespace les conversations entre les jeunes pouvant avoir lieu dans les cours de récréation. Cette plateforme communicationnelle anonyme interlycées va d'ailleurs avoir un succès considérable : on ne compte pas moins de 1034 noms d'écoles en Turquie inscrits sur Potinss, à savoir 250.000 d'abonnés[6], donnant ainsi à cette plateforme et aux données qui y sont postées un rayonnement considérable. Peu à peu, l'application va devenir téléchargeable par Google Play et App Store. En cliquant sur le nom des établissements, les utilisateurs vont pouvoir avoir accès aux noms des étudiants inscrits dans ces lycées, de consulter leurs messages mais aussi les photographies que d'autres utilisateurs avaient postées. Les individus avaient également la possibilité de commenter, et ce, anonymement, les profils qu'ils consultaient. Il était donc impossible de savoir qui était l'auteur des discours, donnant ainsi lieu à des échanges incontrôlés augmentant les risques d'humiliation. Les études effectuées sur cette application ont d'ailleurs montré que celle-ci regorgeait de divers types d'atteintes à la personne dénigrant le corps des individus. Aslan et Önay Doğan (2017) évoquent notamment :

- **Les insultes** : Des stratégies sont utilisées pour contourner les régulations du site : par exemple, lorsque les individus échangent des insultes, ils le font en mobilisant des étoiles (*) pour que le mot ne soit pas détecté et éviter que le message ne soit effacé. L'insulte reste donc visible et comprise par tous, sans qu'aucune action ne vienne la sanctionner.
- **L'attribution de surnoms** en lien avec le physique (ex. « Saumon », « Doberman ») ;
- **La moquerie** : là aussi l'image est utilisée pour railler le corps. On dénigre par exemple « les chauves de l'école » (*Okulun Kelleri*), catégorie sous laquelle des photographies de personnes sont partagées ; ou encore « Les plus belles filles de l'école » avec pour illustration des noms de garçons ou encore « une liste des individus qui sentent le plus ».
- **Le dévoilement** (*ifşa*) : on dénonce ceux qui ont copié aux examens ou qui fument ; on révèle des informations intimes relatives à la relation amoureuse telle que « qui sort avec qui ».
- **Insultes et menaces.**

[6] https://twitter.com/search?src=hash&q=%23potinss

- **Le partage de vidéos ou matériel visuel** : Mais aussi des photographies commentées : comme c'est le cas par exemple de cette jeune fille assise sur une balançoire dont une photographie de son entrejambe est montrée en gros plan, laquelle est accompagnée de la légende suivante : « la p*te avec la performance de lit (sexuelle) la plus longue de l'école ? Je fais une réservation… ».
- **L'exclusion**, qui elle s'établit à partir de cinq particularités : l'identité ethnique ; l'orientation sexuelle ; les différences socio-économiques ; les orientations politiques. Ainsi, sur l'application les individus sont « fichés » selon ces catégories où on échange pour savoir qui est homosexuel ou Alévis, par exemple.

Potinss sera peu à peu considérée comme une application dangereuse non seulement pour les étudiants et leur image, mais aussi pour les enseignants. De nombreuses plaintes seront adressées au Centre de communication présidentiel de la République de Turquie (CIMER) par la population mais aussi par les médias pour en dénoncer les dérives et notamment celle d'inciter les lycéens à la violence entre pairs. Une annonce est même publiée sur le site de l'éducation nationale visant à informer les responsables des écoles ainsi que les enseignants sur les possibles dangers provoqués par cette application ; il est d'ailleurs conseillé, en cas de criminalité engendrée par Potinss, de s'en référer aux forces de l'ordre[7]. L'application sera désactivée suite à la décision de ses créateurs qui souhaitent travailler sur une version plus aboutie[8]. Il donnera aussi lieu à de nombreux articles de journaux (Ülkütekin, 2017) pour se voir retirer de la circulation.

Ainsi, vu la manière dont ont été problématisées les recherches sur les cyberviolences, on constate alors que les scientifiques turcs ont plutôt privilégié ces dix dernières années les analyses portant sur les populations juvéniles (Peker, 2012). Cependant, il nous faut souligner que toutes personnes, quel que soit leur âge, peuvent être impliquées en tant que victimes ou persécuteurs dans la cyberhumiliation (Dilmaç, Kocadal, 2019). Un article du journal *Sözcü* (Atam H., Sözcü, 17.01.2019) montre par exemple que la police aurait appréhendé un gang qui sévissait sur les réseaux sociaux. En utilisant des images volées d'une agence de mannequins et se faisant passer pour des femmes, les criminels faisaient chanter des hommes de plus de 40 ans après avoir obtenu de leur part des enregistrements vocaux obscènes, censés être adressés aux profils imaginaires. Les enquêtes de la police ont révélé que le réseau a piégé au moins 2 000 personnes et a réalisé un bénéfice de 500 000 lires. En outre, en 2019, le journal *Yeni Şafak* daté du 22.03.2019 rapporte que les personnes de plus de 65 ans, qui seraient désormais plus actives sur les réseaux, seraient, elles aussi, vulnérables aux attaques en ligne du fait de leur croyance aveugle en des personnes se présentant comme étant une autorité institutionnelle.

Cependant, malgré ces cas, force est de constater que la population juvénile reste LA catégorie la plus touchée par ces attaques. D'ailleurs, on note que la condition sine qua non pour qu'un acte soit considéré comme du cyberharcèlement en Turquie serait qu'une des personnes impliquées (agresseur ou victime) soit un enfant ou un jeune individu et

[7] Décision du 10.04.17, [en ligne], disponible sur le site Internet : https://mus.meb.gov.tr/meb_iys_dosyalar/2017_04/11084606_Potinss_UygulamasY.pdf

[8] https://twitter.com/search?src=hash&q=%23potinss

que l'agression implique l'utilisation des technologies de l'information. La cyberintimidation consisterait alors à blesser ou à intimider un individu en utilisant Internet. Le but de l'action viserait à humilier la personne, à l'insulter, à la menacer ou à la faire chanter.

Les études turques insistent aussi sur une des distinctions fondamentales entre la cyberhumiliation et le dénigrement traditionnel : dans le cas d'une agression dans la vie réelle, la répétition de l'acte (Doğan *et al.*, 2018) ne serait pas une prérogative contrairement aux atteintes numériques : en effet, la propagation rapide des images dans les réseaux sociaux viendrait redoubler le tourment provoqué chez la victime. Une autre différence est que sur le Net, le persécuteur peut rester anonyme, situation venant renforcer le désarroi du bouc émissaire qui ne peut dans la majorité des cas identifier son agresseur (Arıcak, 2015).

La cyberhumiliation aurait pour but de déstabiliser un tiers, de s'amuser en le blessant et quelques fois même de se venger de lui (Aksaray, 2011, p. 407). Yetim (2015) souligne cependant que les termes peuvent varier selon les cas : ainsi, si l'agresseur est un adulte, on parlera plus de « cyberharcèlement » (*siber-taciz*) ou de « cybertraque » (*siber-takip*) que de « tyrannie » numérique (*siber-zorbalık*). D'ailleurs, ce terme est celui qui est le plus souvent employé dans les recherches effectuées : il signifie littéralement « cyber-tyrannie ». En turc, outre la tyrannie, « *zorbalık* » renvoi de même au despotisme, à l'oppression. Il a pour synonyme le terme « impérieux ». Le « *zorba* » est celui « qui fait confiance en sa force ; c'est la personne qui n'accorde aucune liberté d'action ni de parole à ceux qui se trouvent sous son autorité ». C'est un despote, un dictateur (Türk Dil Kurumu - Organisme de la Langue Turque)[9]. Dans cette optique, le persécuteur *décide* donc du sort de sa victime : il est dans une position de toute puissance et cette situation plonge les protagonistes dans une relation déséquilibrée. On comprend ici pourquoi les chercheurs ont choisi ce terme plutôt qu'un autre en turc, puisqu'il semble être l'équivalent parfait de *bullying* en anglais : l'acte comprend un agresseur ou un groupe d'agresseurs et peut être engendré sur la mise en circulation de rumeurs, d'informations diffamatoires ou sur la manipulation de tiers contre le bouc émissaire, pratiques entraînant l'isolement de la victime. Dans la littérature turque, on rencontre également d'autres termes tels que « *siber istismar* » (la maltraitance en ligne, équivalent de grooming), « *siber mağduriyet* » (cybervictimisation), « *siber takip* » (traque). L'emploi des concepts en langue étrangère peut également être de vigueur à diverses occasions ; tel est le cas du vocable « Revenge porn » (Aksoy Retornaz, 2021) ou de celui de « mobbing » (Demirtaş, Karaca, 2018) par exemple.

Enfin, à un niveau plus macrosociologique, on constate l'existence de deux analyses portant sur la manière dont la presse écrite turque a jusqu'ici rapporté les cas de cyberhumiliation (Narin, Ünal, 2016). Cette recherche tentait à travers 27 journaux nationaux de cerner la fréquence à laquelle l'intimidation en ligne était traitée, mais aussi en quels termes (linguistiquement, politiquement, le contenu utilisé) cette question était abordée. Parmi les résultats les plus probants, on apprend que parmi les 27 journaux analysés pour la période janvier 2015 - juillet 2016, 93 nouvelles en rapport avec ce type d'agression numérique ont été

[9] TDK : https://sozluk.gov.tr/ *« Zorba » : « Gücüne güvenerek hükmü altında bulunanlara söz hakkı ve davranış özgürlüğü tanımayan (kimse) (...)* » (consulté le 9 Avril 2022)

recensées. Les auteurs soulignent qu'une grande majorité des matériaux trouvés (93,5%) portaient sur la sensibilisation des lecteurs au sujet de l'existence d'un tel phénomène dans la société contemporaine. Les cas particuliers de violence, eux, ne représentent que 4,3% des données collectées. Les chercheurs remarquent aussi que lorsqu'il est question de cyberintimidation, les nouvelles sont systématiquement traitées en rapport avec les thèmes de la technologie (100%), des enfants (82,8%) et de l'éducation (49,5%); les solutions pour lutter contre ce fléau, quant à elles, ne sont présentes que dans 39.8% des nouvelles et les campagnes de prévention uniquement dans 10% des cas. Linguistiquement, les auteurs relèvent que le langage employé dans le traitement de ces situations est en grande majorité technique (67,7%). En outre, les nouvelles analysées pointeraient la famille (à 46,2%) et le système scolaire (30,1%) comme principaux responsables de ces agressions. La dégénérescence sociétale et l'insuffisance des peines juridiques ne seraient, quant à elles, blâmées que dans 4% des actualités de la presse turque.

La deuxième étude de cas journalistiques (Doğan *et al.*, 2018), quant à elle, s'attachait à décrire des cas de cyberintimidation, dont ont été victimes des mineures de 11-13 ans, usagères de Facebook. L'originalité de cette étude est qu'elle montre comment ces agressions qui au départ s'apparentaient à du *cyber*harcèlement, vont peu à peu se transformer en « harcèlement sexuel » et intégrer le monde réel : les auteurs mettent ainsi en lumière les répercussions *hors ligne* des persécutions ayant débuté *en ligne*. Parmi les modalités d'actions des agresseurs décrites par les auteurs, certaines nous ont semblé intéressantes à souligner, car elles corroborent nos propres résultats :

- Certains harceleurs se font passer pour des femmes ou pour une autorité (un enseignant par exemple) afin de créer un lien de confiance avec les adolescentes.
- Beaucoup mentent également sur leur âge et leur statut, et se font passer pour des pairs.
- L'intimidation exercée sur le Net peut engendrer des menaces et persécutions dans la vie réelle : on demande à la victime de la voir ou d'avoir une relation avec elle dans la vraie vie... Dans ces cas-là, Internet semble être utilisé comme un biais à la « rencontre amoureuse forcée » ou à la « prédation sexuelle », et non uniquement comme un outil servant à humilier.
- Dans les faits relatés, l'agresseur agit seul, dans son propre intérêt ; il n'existe pas d'effet de groupe.
- Le corps est dans la majorité des cas le support par lequel va s'effectuer l'atteinte : on demande par exemple à la victime de se dénuder, mais l'agresseur peut lui aussi envoyer des photographies de lui, forçant l'individu à voir ce qu'elle ne souhaite pas regarder. Divers scénarios se dégagent : on *montre* quelque chose de soi ; on *demande à voir* le corps de l'autre ; on *l'oblige* à regarder quelque chose ; on *partage* une image du corps de quelqu'un.

3. Méthodologie

Dans cette partie, il s'agira, à partir de cas journalistiques de deux journaux grands tirages (*Hürriyet* et *Birgün*) identifiés pour la période 2017-2022 (5 ans), de proposer une vue d'ensemble des cas d'atteinte à l'image recensés en Turquie. Pour effectuer la collecte d'information à travers les

supports médiatiques, divers mots clefs relatifs aux cyberviolences ont tout d'abord été déterminés, parmi lesquels « cyberharcèlement » (*siber taciz*), « harcèlement numérique » (*sanal taciz*), « tyrannie virtuelle » (*sanal/siber zorbalık*), « violence de flirt » (*flört şiddeti*), « traque » (*ısrarlı takip*), « tyrannie des pairs » (*akran zorbalığı*), « menace » (*tehdit*), « humiliation » (*aşağılama*), « photographies/vidéos non appropriées » (*uygunsuz fotoğraf/ video*), « obscénité/ images obscènes » (*müstehcenlik/ müstehcen görüntü*). A ces termes, ont été ajouté ceux de la « réputation » (*haysiyet*), de la « remise en question de la dignité », (*onur kırıcı*) ou encore de « la souillure de l'honneur » (*onur/şeref zedelenmesi*) qui pourraient avoir fait émerger des cas de discrédits numériques. Ces vocables ont été choisis, car ils correspondent aux termes susceptibles d'être employés en Turquie pour désigner les atteintes à l'image. À la suite de la découverte des cas répertoriés dans les archives numériques de ces journaux accessibles en ligne, une étude minutieuse des faits relatés a été effectuée. Pour cela, une grille d'analyse a été mise en place, permettant ainsi de relever des informations liées aux modalités des cyberviolences lorsque celles-ci étaient données. Cette exploration avait ainsi pour but de collecter des renseignements sur :

- Le profil des victimes des agresseurs : informations démographiques, âge, statut, profession.
- Les types de relation (amical, marital, sentimental, ex-partenaire, connaissance, inconnu…) entre les protagonistes.
- L'agression même, son déroulement et voir si celle-ci était effectuée en ligne, mais aussi hors ligne.
- Les termes utilisés dans l'article pour nommer l'agression : parle-t-on de « harcèlement », d' « humiliation », de « traque », de « tyrannie » en ligne.... ?
- Les moyens utilisés pour l'agression : téléphone portable ? Internet ? Réseaux sociaux précis ? Sites de rencontre ? Plusieurs moyens combinés ?
- Les informations sur les données partagées : s'agissait-il de photographies personnelles, intimes, dénudées, partage de bribes de conversations privées, photographies détournées ou caricaturées ?
- Les individus avec lesquels ces images ont été partagées (famille, proches, avec des anonymes sur des réseaux, les amis de la victime, les amis des agresseurs…)
- Les discours de victimisation : Que dit la victime de cette agression ? Existe-il un discours de celle-ci se dégage-t-elle de l'article ? (discours sur les sentiments, sur la honte, sur l'image et réputation remise en question, demande de réparation ou de justice…)
- Les sanctions juridiques appliquées ou passibles d'être appliquées (observe-t-on par exemple une référence explicite aux codes ou articles pénaux ? Par quels moyens l'agresseur a-t-il été appréhendé ou identifié ?).

Cette recherche nous a permis de récolter au total 23 cas (tous rapportés par la presse) sur la période des cinq ans étudiés. Au terme de cette analyse qualitative, certaines récurrences dans les modalités des agressions en Turquie ont été identifiées.

4. Présentation et interprétation des résultats

Tout d'abord, dans tous les cas d'atteintes à l'image collectés où il a été possible de cerner l'identité des persécuteurs[10], on constate que les agresseurs sont des hommes adultes qui agissent seuls et tentent d'intimider des victimes du sexe féminin.

Cela va d'ailleurs dans le sens des propos de Kırık (NTV.com.tr, 2020), chercheur en communication numérique, qui montre qu'avec la pandémie, l'intérêt pour les médias sociaux aurait augmenté, entraînant de nouvelles problématiques, et notamment de la violence à l'encontre des femmes. En effet, ce type d'agression prend plus particulièrement forme sur les réseaux sociaux. Les menaces à caractères sexuels et les discours de haine se seraient même généralisés au cours de cette période. Pour le chercheur, ces violences numériques sexistes devraient être combattues d'une manière plus soutenue (Baş, 2020). Dans le cas de notre étude, s'il est vrai que les agressions touchent essentiellement les jeunes femmes, aussi bien adultes que mineures, on constate cependant que ces sévices étaient déjà pratiqués avant la pandémie, puisque nous recensons des cas dès 2017 (5 cas), mais aussi en 2018 (5 cas), en 2019 (3 cas), en 2020 (3 cas) et 3 cas également pour l'année 2021 et 4 cas pour 2022.

Cependant, lorsqu'il est question d'atteinte à l'image effectuée en groupe, on constate que les hommes vont plus prendre pour cible des enfants : c'est le cas notamment dans le partage, l'échange ou la vente d'images pédopornographiques et d'abus sexuels perpétrés sur des mineurs que l'on retrouve dans deux cas (Hürriyet, 11.01.22 et Hürriyet, 15.10.20), l'un impliquant 46 personnes et l'autre, 22 suspects. Fait intéressant, on observe que le terme « obscène »[11] (*müstehcen*), utilisé en vue de qualifier les matériaux visuels diffusés, est essentiellement usité dans les journaux pour désigner les images liées aux mineurs, alors que dans les cas impliquant des adultes, on parlera plus de photographies « non convenables » ou « non appropriées » (*uygunsuz*), créant ainsi une sorte de hiérarchie dans la gravité des actes. Ainsi, l'obscène est ce qui « offense ouvertement la pudeur dans le domaine de la sexualité », ce « qui est choquant par son caractère inconvenant »[12], alors que l'inapproprié, se veut gênant, « déplacé » ; ce dernier ne devrait pas être exposé, il n'a pas sa place dans l'espace public. En outre, le terme récurrent « inapproprié » que l'on retrouve dans les discours médiatiques pour qualifier les vidéos ou images d'adultes dénudés est à nos yeux de même significatif : il est à la fois très subjectif, quasi moralisateur, et marque une non-conformité, une déviation par rapport au normatif et peut-être même une certaine déviance des comportements qui sont représentés sur les images désignées de la sorte.

Ainsi, on constate que dans les situations identifiées, les adolescents et notamment ceux agissant en compagnie de leurs pairs sont sous-représentés (à l'opposé de ce qui est reflété dans la littérature scientifique). Les agresseurs sont dans une majorité des cas des individus que nous pourrions qualifier de « jeunes adultes » ou adultes qui agissent seuls, sauf dans le cas de la pédopornographie. Dans un des faits, la mère d'une victime de cyberintimidation

[10] Deux cas font cependant exception : l'un car il traite de l'utilisation abusive par une banque d'une photographie d'une de ses clientes sur un panneau publicitaire. Or, cette situation ne relevant pas à proprement parler de cyberharcèlement, il n'a pas été pris en compte. L'autre cas, ne mentionnant pas le sexe de l'agresseur, n'a pas pu être comptabilisé dans cette section.

[11] Tous les termes, les expressions et extraits présentés entre guillemets (et commentés) correspondent aux discours repérés dans les articles analysés.

[12] CNRTL : https://www.cnrtl.fr/definition/obscene

va même jusqu'à avouer avoir été surprise lorsqu'elle apprit que l'agresseur de sa fille de 13 ans n'était autre que son petit ami adolescent ; celui-ci lui aurait demandé des photographies d'elle, images qu'elle refusa, dans un premier temps, de lui transmettre, mais qu'elle finira par lui envoyer plus tard, intimidée par les menaces. Les images seront ensuite récupérées par un groupe de collégiennes et qui chercheront à humilier la victime dans la vie réelle. La mère de la persécutée affirmera avoir été choquée par ces pratiques, qui d'après elle, seraient plus communément commises par des adultes plutôt que par des mineurs (Hürriyet, 13.03.19). Ainsi, dans les représentations mais aussi dans les cas identifiés, les agressions en ligne seraient plus perpétrées par des individus majeurs agissant seuls.

D'ailleurs, force est de constater que dans plus de la moitié des cas collectés, les hommes agresseurs étaient plus âgés que leurs victimes (dont la plupart étaient même mineures). Le rapport de domination entre les protagonistes est donc systématiquement de mise : dans les cas les plus récurrents, on constate que l'agresseur force la victime à se dénuder, lui demande des faveurs sexuelles, essaye de lui extorquer de l'argent. Nous sommes là dans un cas de « grooming » en ligne, autrement dit une situation de leurre d'enfants. Le désarroi ressenti par la victime qui s'est fait humilier est donc décuplé par la différence d'âge qui sépare les protagonistes, et exerce sur elle une pression de plus. On constate de même que les agresseurs aiment à mentir sur leur statut social soit pour susciter chez leurs interlocuteurs la curiosité et provoquer la discussion, soit pour pouvoir soutirer des images visuelles de la victime contactée : ainsi, les persécuteurs peuvent aussi bien se faire passer pour un policier que pour un ingénieur maritime ou un officier pour gagner la confiance des femmes (Hürriyet, 13.05.21).

On constate également une différence entre le traitement médiatique de ces violences : par exemple, lorsqu'il est question de faits concernant les mineurs, les journalistes auront tendance à insister sur le statut (âge et profession) des agresseurs, quitte à les évoquer trois fois dans la même rubrique. Ainsi, un des faits récoltés relate l'opération effectuée par la police permettant d'arrêter 44 individus impliqués dans la vente et l'achat de photographies et vidéos d'enfants victimes d'abus sexuels. Les malfaiteurs sévissaient sur l'application Telegram (Hürriyet, 11.01.22). À travers cette nouvelle, nous apprenons que parmi les personnes appréhendées se trouvaient un policier, un docteur des soldats contractuels, un sous-officier spécialisé et quatre fonctionnaires. Un autre fait (Hürriyet, 15.10.20) rapporte l'implication de 22 suspects (dont 13 seront arrêtés) dans la diffusion et l'archivage d'images d'abus sexuels sur mineurs, parmi lesquels se trouve un homme handicapé de 72 ans. Dans ce cas précis, les journalistes vont jusqu'à évoquer le passé de cet offenseur, dévoilant par exemple que celui-ci aurait été exclu de sa famille qui le soupçonnait d'avoir abusé de son petit.e. fils/fille, bannissement qui le poussa à se réfugier dans une maison de retraite. Tous ces détails sur les antécédents de l'agresseur n'apparaissent pas dans les autres cas. Il semblerait ainsi que les atteintes à l'image effectuées à l'encontre des mineurs soient plus naturellement décriées que les agressions de cyberhumiliation impliquant des victimes adultes.

4.1 La séparation acrimonieuse

Lorsque l'on se penche sur le rapport qui lie la victime à son agresseur, deux grandes tendances se

dégagent de notre étude : on constate que les cas les plus récurrents menant à la cyberhumiliation relèvent soit de la « rupture sentimentale mal-acceptée » soit de la « mauvaise rencontre » sur Internet. La plupart des victimes connaissaient en effet leur persécuteur : celui-ci est dans la majorité des cas un ex-partenaire qui refuse la rupture et s'en prend à son ancienne compagne en diffusant des images d'elles dégradantes dans le cyberespace. Ces images peuvent d'ailleurs être réelles, à savoir avoir été partagé en toute confiance et lors de la relation par la victime lors de la relation, ou avoir être créée de toute pièce : le photomontage ou la création de faux profils sur lequel l'agresseur partage, au nom de la victime, des photos sexy est de même un moyen usité ; les images sont ainsi partagées dans le cyberespace avec des inconnus. En outre, il est de même possible que l'ex-compagnon envoie les matériaux visuels dégradant à ses propres connaissances depuis la plateforme Whatsapp en leur demandant de contribuer à leur diffusion (Birgün, 21.01.20). Dans d'autres cas, l'amoureux éconduit va envoyer des photographies a contenu sexuel de son ex-partenaire à un ami O. (22 ans), qui à son tour, harcèlera la victime pour obtenir plus de vidéos et la menacera de diffuser les images qu'il a déjà d'elle sur les réseaux sociaux (Hürriyet, 13.11.17).

Ainsi, il semblerait que les victimes d'infraction envoient, dans la majorité des cas, des contenus suggestifs à des destinataires qu'ils connaissent et auxquels ils font confiance (Huerre *et al.*, 2013). Penser contrôler le destin de son image, sa diffusion et l'attachement vis-à-vis du récepteur, encourageraient les individus à partager des informations personnelles sur les réseaux (Velten, Arif, Moehring, 2017, p. 243). Or, on constate que c'est justement lorsque ce lien de confiance est remis en question que les cyberattaques ont lieu : en effet, les jeunes seraient de plus en plus victimes de personnes avec lesquelles ils entretenaient une relation amoureuse ou amicale (Lenhart, 2009). Ceci vient remettre en question la croyance selon laquelle les Internautes ne seraient victimes que de personnes malveillantes qui leur sont totalement inconnues. Bien entendu, cela dépend du type d'infractions puisque cela n'est pas le cas par exemple dans les affaires de leurre d'enfants ou de pédopornographie. Dans la même logique, les sujets peuvent aussi être contactés par des inconnus et recevoir des sollicitations sexuelles agressives ou se voir envoyer des vidéos pornographiques qu'ils ne souhaitaient pas voir, actes relevant aussi du harcèlement.

Ce type d'intimidation est d'ailleurs désigné dans la littérature par le terme controversé « porno-vengeance » (*revenge porn*) : il correspond à la diffusion d'un contenu sexuellement explicite partagé en ligne sans le consentement de la ou des personnes apparaissant sur le contenu, dans le but d'en faire une forme de vengeance (İkiz, 2018). L'objectif est ainsi de salir la réputation (et donc l'image sociale) de la personne en dévoilant des contenus mettant en scène son corps et en espérant provoquer des répercussions à la fois dans le monde numérique et dans le monde réel. Si la revanche pornographique est observable dans diverses sociétés, pour nous, celle-ci prend une autre dimension dans le cas de la Turquie. En effet, la remise en question de la réputation et par là, celle de l'honneur dans la société turque ne soulève pas tout à fait les mêmes enjeux que dans les autres contextes nationaux : bien entendu, ces attaques ont des conséquences effroyables sur tous les individus qu'elles touchent et ce, quelques soit leur pays. Cependant, il nous semble que le contexte culturel

se doit aussi d'être pris en considération dans la compréhension de ces violences car le corps et la remise en question de la réputation n'ont pas la même résonnance dans toutes les sociétés, et notamment dans celles où les crimes d'honneur existent encore (tel qu'il en est le cas en Turquie). Ainsi, il n'est pas étonnant de constater par exemple que les cyberviolences dans le cas turc peuvent avoir pour but non seulement d'offenser la dignité de la personne mais également de souiller l'honneur de la famille de la victime.

La diffusion de rumeurs par le Net est ainsi un autre moyen de dénigrer non seulement l'image sociale de l'individu mais aussi son corps : dans ce dernier cas, on parle de rumeurs « visuelles » (Froissart, 2002, p. 189) qui désignent les « images rumorales » associées au corps de la victime et circulant d'une boîte mail à l'autre ou postées sur les sites Web personnels. Edgar Morin (1969) décrit d'ailleurs les rumeurs comme des « métastases » qui incubent et prolifèrent sur un corps inerte et sans défense. Elles diffusent ainsi « le virus de l'hostilité » (Allport et Postman, 1965) et peuvent remettre en question la réputation de toute une famille. Le cas de Merve Gürbüz[13] en est d'ailleurs un exemple probant : celle-ci se verra victime de son ex-partenaire qui créera en son nom et en celui de son ex-belle-mère, des profils d'escorte (Milliyet, 30.05.21). La réputation et sa remise en question se veulent alors réticulaires. Quelques fois même, les proches du persécuté subissent également des violences dans la vie réelle : comme dans le cas d'E.U. qui entame une relation avec H.I.G. rencontré dans un supermarché (Hürriyet, 11.03.18). Celui-ci prendra des photographies d'elle dénuée qu'il utilisera pour la faire chanter et lui faire subir des pressions. Refusant de céder, E.U. porte plainte, ce qui n'arrête pas l'agresseur qui viendra importuner les autres membres de la famille et de s'en prendre à eux aussi bien par des violences physiques que verbales. H.I.G. ira jusqu'à lancer un cocktail Molotov dans le bus dans lequel se trouve le père de E.U. et tirera sur son frère, assis sur un balcon. En dénigrant non seulement l'image personnelle de la victime mais aussi la réputation de sa famille, ces attaques qui visent à se venger d'un amour déçu, ôtent au persécuté toute possibilité de trouver un autre partenaire, et même un futur conjoint.

4.2 La « mauvaise » rencontre

Les résultats de notre étude montrent également que les individus ont tendance à être victimes de personnes malveillantes rencontrées sur Internet. Le monde numérique semble être devenu un espace utilisé par les individus pour créer du lien, mais aussi pour entrer en contact avec des partenaires en vue d'entamer une relation amoureuse (Rosen *et al.*, 2008). D'ailleurs, les sites de rencontres par exemple mettent en relation des personnes qui ne se connaissent pas, tout en leur permettant de nouer des contacts avec des individus ciblés, répondant à leurs critères (par exemple, en affinant les recherches ou en filtrant les résultats), maximisant ainsi les chances de trouver son âme-sœur. Ces rencontres en ligne seraient d'ailleurs amenées à se développer encore plus dans les années à venir et à s'imposer comme une vraie alternative aux rencontres traditionnelles (Chenavaz, Paraschiv, 2011). Il semblerait ainsi que le cyberespace soit envisagé pour certains individus comme un cadre « intimiste » leur permettant de discuter plus librement de sujets très personnels (Moon, 2000) et d'engager des interactions suivies, avant de se rencontrer dans la vie réelle. En effet, comme le montre Sautter *et al.*, (2010), certains utilisateurs

[13] Les noms, prénoms et initiales cités tout au long de l'article sont ceux mentionnés dans les articles de presse analysés.

acceptent de se rencontrer rapidement dans la sphère réelle, sans beaucoup d'information sur le partenaire potentiel. Ils s'exposent donc à certains risques dont ils sont conscients en révélant « des attributs identitaires au-delà de la sphère restreinte à laquelle ils sont habituellement réservés » (Déage, 2018, p. 149). Şener (Şener *et al.*, 2012, p. 128) va jusqu'à affirmer que le fait qu'il soit plus facile sur Internet de discuter avec des inconnus et de les accepter comme amis encouragerait les individus à parler de sexe ou à s'insulter plus librement. Les atteintes dans ce cas de figure semblent suivre le même processus : un contact est établi par l'une des personnes, celles-ci conversent et après un certain temps, l'une d'elles se voit demander des images intimes qui constitueront un matériel utilisé par l'agresseur soit pour la faire chanter et lui soutirer de l'argent, soit pour la menacer en vue d'obtenir d'autres avantages (des faveurs sexuelles, par exemple).

Nous pouvons par exemple nous référer au cas d'E.A. qui n'a que 14 ans lorsqu'elle rencontre C.K. en 2014 sur Internet. Après avoir gagné la confiance de la victime, celui-ci commence à la faire chanter avec les photos dénudées que lui avait envoyées la jeune fille. Par peur que C.K. mette à exécution ses menaces, et notamment celles d'envoyer ces images à d'autres mais aussi à sa propre famille, E.A. accepte sous la contrainte d'avoir des rapports avec lui. À 16 ans, suivant le même procédé, C.K. obtient d'elle qu'elle ait des rapports avec Y.Ç. et N.S. La victime finira par signaler la situation à la police (Hürriyet, 19.02.18). On constate ainsi ici que nous sommes sur un cas de leurre d'enfants, et donc d'abus sexuel de mineur.

Si les victimes, qui sont très souvent mineures, se confient plus aisément à leur famille, on constate que certaines d'elles vont aussi porter plainte aux autorités. Or, au vu des cas relatés dans les médias turcs, on constate que la police, pour appréhender les agresseurs, passe systématiquement par l'organisation d'une rencontre fictive dans le monde réel : il est ainsi demandé aux victimes de chantage par exemple de donner rendez-vous à leurs harceleurs, lieu dans lequel ils seront arrêtés par les autorités. On note ainsi que les cyberviolences en Turquie ne semblent pas faire l'objet d'une réponse répréhensive dans le monde numérique, poussant ainsi les forces de police à mettre en place des « opérations » (mots que l'on retrouve aussi dans les cas) dans le monde réel en vue d'arrêter les cyberharceleurs. C'est le cas par exemple de N.K., 30 ans (Hürriyet, 25.06.21) qui se fera appréhender sur le lieu de rendez-vous où celui-ci attendait la rançon qu'il avait sollicitée de son ex Y.D. (38 ans, rencontrée sur les réseaux sociaux) et qui s'élevait à 50.000 livres turques, afin de ne pas diffuser les photographies intimes qu'elle lui avait transmises.

Les cas de cyberharcèlement, à savoir les attaques qui seraient réitérées, sont sous-représentés dans notre échantillon : E.Ç., 29 ans, envoie des demandes d'amitié a des femmes sur les réseaux sociaux ; celles qui lui refusent l'accès ou le bloquent sont menacées de voir leur avatar volé et dénudé par l'usage du programme de retouche Photoshop (Hürriyet, 12.04.19).

En outre, il ressort de notre analyse que dans le cas de la mauvaise rencontre, là aussi, beaucoup d'agresseurs mentent sur leur statut ou sur leur sexe en vue de gagner la confiance de leur victime et de lui soutirer des informations plus facilement. Ainsi, le malfaiteur pourra se faire passer :

- pour un policier (Birgün, 4.08.17), comme dans le cas de H.K., qui appela A.U. et se présenta comme un représentant des forces de l'ordre pour que la mineure lui fournisse

des images d'elle dénudées. Les malfrats réussiront à soutirer de la jeune fille à peu près deux mille cinquante euros, mille livres turques, dix bracelets torsadés, une boucle d'oreille, une montre en or et une alliance ;

- une jeune fille à la recherche d'hommes (ex. d'un entraîneur de basket qui utilisa les photographies d'une des joueuses de son équipe pour créer un faux profil d'Escorte et appâter des hommes pour leur soutirer de l'argent) ;
- ou encore pour des femmes (dans deux cas notamment) : comme dans le cas de C.O. (Birgün, 16.03.17), propriétaire d'un cybercafé, qui crée deux faux profils sur Facebook au nom de femmes prénommées « Melek Sonmaz » et « Ebru Yaşar », et envoie deux invitations d'amitié à deux mineures. Ne se méfiant pas, B.K. accepte la demande et commence à converser avec C.O., caméra allumée, sans pour autant que celui-ci ne se dévoile lors de la visio. L'adulte va alors encourager la petite fille à se déshabiller et à enregistrer les images. Se faisant de plus en plus pressante, la victime prendra peur et mettra fin à la conversation, pour ensuite aller reporter la situation à sa sœur. Le deuxième cas est celui d'E.K. (Hürriyet, 15.04.22) qui créa de nombreux comptes sur Telegram en utilisant des noms et des images de femmes. Ce stratagème lui permit d'entretenir des conversations à caractère sexuel avec plusieurs victimes. Il menaça de partager les captures d'écrans de ces dialogues et fit chanter ses interlocuteurs.

L'aspect traumatique de ces attaques en ligne est de même reflété dans la manière dont sont traitées discursivement les situations par les médias : on parle de « situation cauchemardesque » vécue par les persécutés, de vie devenue « un enfer » ou encore « une prison » pour les victimes.

Comme mentionné précédemment, notre analyse journalistique nous a permis de collecter 23 cas relevant des atteintes à l'image. Ce nombre peut paraître minime, surtout si on considère tous les débats et les enjeux autour de la question traitée. Cependant, on constate que près de la moitié des cas incluent des enfants, des jeunes et des jeunes adultes soit en tant que victimes, soit en tant qu'agresseurs ou encore les deux.

Dans les situations considérées comme relevant de cyberviolences, divers thèmes et vocables ont ainsi surgi de notre analyse. Les cas traitaient par exemple de cyberintimidation, de violence en ligne entre pairs, de victimes menacées, harcelées, dénigrées ou encore ayant subi des abus sexuels. Ces attaques pouvaient, on l'a vu, prendre plusieurs formes : diffusion ou utilisation non consentie de photographie, divulgation d'images de la vie privée, archivage d'images obscènes de mineurs et leur partage, harcèlement sexuel. Ces violences pouvaient de même être accompagnées d'autres sévices, à savoir de chantage, d'insulte, de partage d'images intimes personnelles à des amis. La cyberhumiliation se caractérise donc par son hétérogénéité en termes d'expressions de la violence. Or, il semblerait que les sanctions préconisées à l'encontre de ces agressions à forme multiples soient tout aussi variées.

4.3 À propos du traitement juridique et judiciaire des cyberviolences

Au vu de l'ensemble des sources consultées, nous pouvons affirmer que les définitions juridiques des infractions commises dans l'espace virtuel et leurs

prises en charge judiciaire constituent un domaine vif de débat, aussi bien au niveau international qu'au niveau national.

Tout d'abord, sur le plan international, nous devons évoquer l'existence de la Convention de Budapest (2001) qui traite de la cybercriminalité, incluant à la fois les pays membres de l'Union européenne, mais aussi d'autres États signataires[14] dont fait également partie la Turquie (Aksoy Retornaz, 2021, p. 56-57). La Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (également appelée « la Convention de Lanzarote »), qui impose la criminalisation de tous les types d'infractions à caractère sexuel perpétrés contre des enfants »[15], en constitue une autre (Aksoy Retornaz, 2021, p. 52). Celle-ci, rentrée en vigueur en 2010, a été également signée par la Turquie. Ce texte s'avère de même être le seul pour le moment à aborder la question du sexting chez les enfants (Aksoy Retornaz, 2021, p. 52) : ainsi, « le Comité de Lanzarote est d'avis qu'en cas de divulgation d'images sexuelles prises par des enfants sur la base de leur consentement, des mesures éducatives et thérapeutiques devraient être appliquées pour éliminer ces comportements » (Aksoy Retornaz, 2021, p. 54).

La Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, connue comme la Convention d'Istanbul (2011), demeure une autre référence importante. Elle est considérée comme « le premier instrument en Europe à établir des normes contraignantes visant spécifiquement à prévenir les violences fondées sur le genre, à protéger les victimes de violences et à sanctionner les auteurs » (Jurviste et Shreeves, 2020)[16]. Comme le relate Aksoy Retornaz (2021, p. 3-4), c'est en partant de la définition de la violence existant dans ladite convention que le Conseil de l'Europe a élaboré une définition de la notion de cyberviolence. Dans un contexte plus récent, nous pouvons également mentionner la Recommandation générale n° 1 du GREVIO (2021) sur la violence numérique perpétrée à l'encontre des femmes. Celle-ci indique que : « 11. Si les hommes comme les femmes peuvent être confrontés à des incidents de violence et d'abus, les femmes sont plus susceptibles de subir des formes répétées et graves d'abus, y compris des violences sexuelles. Elles sont également plus susceptibles d'avoir subi des violences physiques, psychologiques ou émotionnelles durables, ou des violences ayant entraîné des blessures ou la mort, y compris de la part d'un partenaire intime. 12. Les formes numériques de la violence à l'égard des femmes peuvent être particulièrement prononcées lorsqu'elles ciblent les femmes et les filles qui sont exposées ou risquent d'être exposées à des formes de discrimination croisée, et peuvent être exacerbées par des facteurs tels que le handicap, l'orientation sexuelle, l'affiliation politique, la religion, les origines sociales, le statut migratoire ou la célébrité »[17].

En ce qui concerne le contexte turc, bien que « les actes de violence à l'encontre d'individus commis au

[14] Conseil de l'Europe, Convention sur la cybercriminalité, Budapest, 23.XI.2001, STE n° 185. Disponible à l'adresse suivante : https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf

[15] Conseil de l'Europe, Droits des Enfants, Convention de Lanzarote. Disponible sur : https://www.coe.int/fr/web/children/lanzarote-convention

[16] Jurviste U. et Shreeves R., Service de recherche pour les députés, PE 659.334, « La Convention d'Istanbul, un outil pour lutter contre les violences à l'encontre des femmes et des filles », novembre 2020, 2 pages. Disponible sur : https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659334/EPRS_ATA(2020)659334_FR.pdf

[17] GREVIO, « Recommandation générale n° 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes adoptée le 20 octobre 2021 », 2021, 34 pages. Rapport disponible sur : https://rm.coe.int/reccomandation-no-du-grevio-sur-la-dimension-numerique-de-la-viomence-/1680a49148

moyen ou facilités par les technologies de l'information et de la communication ('cyberviolence') [soient] devenus une préoccupation majeure pour les sociétés et les individus »[18], on constate qu'en Turquie le champ juridique reste encore « en chantier ». Malgré l'existence de débats afin d'inclure les cyberagressions comme une catégorie à part entière dans le Code pénal, la violence numérique n'est pas à proprement parler un crime défini par la loi (Baş, *Milliyet*, 27.07.20), contrairement à la cybercriminalité (*Bilişim Suçları*)[19]. Autrement dit, les infractions qui sont commises dans l'espace numérique sont punies selon des articles destinés à traiter des infractions qui sont dans la compétence du Code pénal sans une référence spécifique à la violence numérique. Comme l'affirme l'ancienne cheffe de la commission du droit informatique du barreau d'Istanbul, Şebnem Ahi, « la violence numérique n'est pas un crime défini par la loi. Cependant, tout comme dans la vraie vie, commettre certaines actions sur Internet peut constituer un crime et il existe différentes réglementations légales régissant l'application des sanctions dans ces cas précis. Bien sûr, d'autres problèmes demeurent, comme par exemple l'impossibilité d'identifier les persécuteurs ou encore la spoliation des preuves. Ces actions peuvent se manifester sous forme d'insultes, de menaces, d'atteinte à la liberté d'expression, de discours de haine, de harcèlement sexuel, d'atteinte à la vie privée, d'atteinte aux droits et libertés ou sous forme de délits. Par ailleurs, les données personnelles peuvent également faire l'objet de ces actions et de discours menaçants pour lesquels la loi prévoit de sanctions telles que l'emprisonnement, la mise en place de mesures de sécurité et d'amendes judiciaires » (Baş, *Milliyet*, 27.07.20).

Malgré l'impossibilité d'établir une liste exhaustive de tous les types de cyberviolences ainsi que les lois qui les sanctionne, le tableau ci-dessous[20] nous permet d'énumérer une série d'actions considérées comme relevant d'agressions en ligne et leur traitement juridique en Turquie.

Types d'infraction[21]	**Cadre juridique du traitement**	**Sanctions attribuées**[22]
Suivi persistant[23]	Détérioration de la paix et ordre du peuple, article 123 du Code pénal turc	Emprisonnement de trois mois à un an
Divulgation des correspondances et images privées	Violation du secret de la communication, article 132 du Code pénal turc	De un à trois ans d'emprisonnement[24]
	Écoute et enregistrement des	De six mois à cinq ans

[18] Comité de la Convention sur la cybercriminalité (T-CY), Groupe de travail sur la cyberintimidation et les autres formes de violence en ligne, en particulier contre les femmes et les enfants, *Étude cartographique sur la cyberviolence*, 2018, 156 pages, p. 4. Rapport disponible sur : https://rm.coe.int/t-cy-2017-10-cbg-study-fr-v2/1680993e65

[19] Qui se caractérise par toutes atteintes effectuées à l'aide d'outils communicationnels modernes tels que des ordinateurs, des tablettes, des téléphones portables. La cybercriminalité est mentionnée dans le Code pénal turc (no. 5237) et les infractions font l'objet des articles 243 et 245. On y retrouve par exemple l'entrée illégale dans un ordinateur pour détruire le système ou le pirater, le vol de données etc.

[20] Ceci constitue un résumé du tableau se trouvant dans le « Guide pour la lutte contre la violence numérique sexiste » réalisé dans le cadre du Programme « Pense civil » (*Sivil Düşün*) de l'Union européenne par l' « Association de la connaissance sociale et de la communication » (TBİD - *Toplumsal Bilgi ve İletişim Derneği*) et « Informatique alternative » (AltBil - *Alternatif Bilişim*). Cf. Şener G. *et al.*, *Cinsiyetçi Dijital Şiddetle Mücadele Rehberi*, décembre 2019, 62 pages, pp. 22-30. Rapport disponible en ligne sur : https://www.stgm.org.tr/sites/default/files/2020-09/cinsiyetci-dijital-siddetle-mucadele-rehberi.pdf.

[21] Dans le tableau d'origine, celui-ci est désigné sous l'appellation « Acte de violence numérique ».

[22] Pour que ce tableau puisse rester une synthèse, toutes les conditions d'augmentation des peines ne sont pas explicitées.

[23] L'envoi de messages ou appels répétées, obligeant à signaler la localisation ou à envoyer des photographies. Insister en vue d'établir une communication même si la personne déclare qu'elle ne veut pas ou ne répond pas (Şener G. *et al.,* 2019, p. 22).

[24] Violation du secret en enregistrant le contenu d'une communication entre les personnes. La peine peut se voir augmentée. Divulgation illégale du contenu d'une communication entre les personnes sans avoir obtenu leurs consentements. De deux à cinq ans d'emprisonnement (Şener G. *et al.,* 2019, p. 22).

	conversations entre individus, article 133 du Code pénal turc	d'emprisonnement et une amende jusqu'à quatre mille jours
Cyber exploitation / Chantage à caractère sexuel (*cinsel içerikli şantaj*)[25]	Violation de la vie privée, article 134 du Code pénal turc	De un à cinq ans d'emprisonnement
	Menace, article 106 du Code pénal turc	De deux à cinq ans d'emprisonnement[26]
	Insulte, article 125 du Code pénal turc	De trois mois à deux ans d'emprisonnement ou d'une amende
Cyberharcèlement[27]	Harcèlement sexuel, article 105 du Code pénal turc	De trois mois à deux ans d'emprisonnement ou d'une amende ; s'il s'agit d'une infraction contre un enfant : de six mois à trois ans d'emprisonnement
Violation de la vie privée[28]	Enregistrement des données personnelles, article 135 du Code pénal turc	De un à trois ans d'emprisonnement
	Donner ou acquérir des données illégalement, article 136 du Code pénal turc	De deux à quatre ans d'emprisonnement
	Formes qualifiées de délit[29], article 137 du Code pénal turc	Peine à infliger est augmentée de moitié
	Non-Destruction de données, article 138 du Code pénal turc	De un à deux ans d'emprisonnement
	Accès au système de traitement des données informatiques, article 243 du Code pénal turc	Jusqu'à un an d'emprisonnement ou d'amende punitive ou de six mois à trois ans d'emprisonnement
Partage au nom de la personne par la création de faux comptes sur internet	Livraison ou acquisition illégale de données, article 136 du Code pénal turc	De deux à quatre ans d'emprisonnement
Discours de haine[30]	Insulte, article 125 du Code pénal turc	Cf. ci-dessus
	Provoquer les individus à être rancuniers et hostiles, article 216/2 du Code Pénal	De six mois à un an d'emprisonnement
Doxxing[31]	Livraison ou acquisition illégale de données, article 136 du Code pénal turc	Cf. ci-dessus
Diffamation[32]	Indemnisation en cas de violation des droits personnels, article 24 du Code civil ; Concurrence	Les dispositions relatives à l'indemnisation spécifiées dans les lois pertinentes

[25] Filmer des images intimes d'une personne et menacer en les partageant et/ou en les partageant avec d'autres personnes sur Internet, sur les réseaux sociaux ou à travers la messagerie privée (Şener G. *et al.,* 2019, p. 23).

[26] Sauf en cas de menace, de provoquer une grande perte de biens ou d'une autre mauvaise conduite, la sanction peut s'élever à six mois d'emprisonnement ou d'amende punitive. En revanche, s'il s'agit de la commission d'un crime ayant pour objectif de menacer et qui résulte d'un homicide volontaire, d'une blessure ou dommage à la propriété, les peines supplémentaires s'appliqueront à la sanction allant de deux à cinq ans d'emprisonnement (Şener G. *et al.,* 2019, p. 23).

[27] Envoyer à une personne des messages et/ou des images à contenu sexuel sans son consentement. Par ailleurs, comme le souligne Aksoy Retornaz, « En droit turc, le délit de harcèlement sexuel est régi par l'article 105 du Code pénal turc. (...) Il est également possible de commettre un harcèlement sexuel dans le cyberespace. La qualification ajoutée à l'article 105/2-d du Code pénal turc par la loi n° 6545 va également dans ce sens. Dans ce contexte, l'infraction de harcèlement sexuel peut également être commise par le biais d'outils de communication électronique, audio, vidéo, SMS ou toute méthode de messagerie envoyée par voie électronique » (Aksoy Retornaz, 2021, p. 82-83).

[28] Récupération du courrier électronique de la personne et/ou mots de passe de médias sociaux et accéder à ses comptes, vérifier les informations sur ses appareils sans permission. (Şener G. *et al.,* 2019, p. 25).

[29] Si les infractions sont commises a) par un agent public qui abuserait de son pouvoir, b) en exploitant les avantages d'une profession et d'un art (Şener G. *et al.,* 2019, p. 26).

[30] Partager sur internet, sur les réseaux sociaux, dans les jeux numériques, dans les applications de messagerie, des messages humiliants, insultants, sexistes ; cibler des personnes et les exposer à un lynchage virtuel (Şener G. *et al.,* 2019, p. 28).

[31] Recueillir des informations détaillées sur une personne sur internet et diffuser et utiliser ces informations pour lui causer du tort (Şener G. *et al.,* 2019, p. 29).

[32] Partager des messages d'une manière qui porte atteinte à la réputation commerciale d'une personne, révéler des secrets commerciaux (Şener G. *et al.,* 2019, p. 29).

	déloyale, article 56 Code du commerce turc	s'appliquent
	Atteinte au droit des marques, Dispositions de la loi n° 6769	Indemnisation et dispositions pénales spécifiées dans la loi pertinente s'appliquent
	Dispositions de la loi numéro 5651	Blocage de l'accès et la suppression du contenu
Contrôler[33]	Blocage/empêchement de la communication, article 124 du Code pénal turc	De six mois à deux ans d'emprisonnement ou amende punitive ou e un à cinq ans d'emprisonnement
Menace/Chantage[34]	Menace, article 106 du Code pénal turc	Cf. ci-dessus
	Chantage, article 107 du Code pénal turc	De un à trois ans d'emprisonnement et jusqu'à cinq mille jours d'amende punitive
Divulgation de données personnelles	Enregistrement de données à caractère personnel, Livraison ou acquisition illégale de données, Code pénal turc, articles 135, 136, 137 et 138	Cf. ci-dessus
	Loi n° 6698 pour la protection des données personnelles, article 18. Le non-respect des obligations d'informer et de sécurité des données.	Amende punitive allant de 5 000 à 1 000 000 de livres turques[35]

[33] Intervenir dans les partages d'une personne dans les médias, essayer de limiter ses communications dans les médias sociaux (Şener G. *et al.,* 2019, p. 30).

[34] Utiliser des moyens numériques pour menacer d'agression sexuelle et de physique, et menacer à mort (Şener G. *et al.,* 2019, p. 30).

[35] Il convient de rappeler que ces montants ne sont pas actualisés mais représentent les plus récents que nous ayons trouvé.

De plus, la comparaison que nous avons effectuée avec l'état des lieux juridiques fourni par Eylem Aksoy Retornaz nous permet d'inclure les infractions qui s'inscrivent dans « les atteintes à la moralité publique, les actes indécents »[36]. À cet égard, il convient de mentionner les articles 225 et 226. Quand l'article 225 stipule que « Quiconque se livre publiquement à des rapports sexuels ou à l'exhibitionnisme, est puni d'une peine d'emprisonnement de six mois à un an », l'article 226/3 quant à lui indique que « Quiconque utilise des enfants, des images représentatives d'enfants ou de personnes ressemblant à des enfants dans la production de produits contenant des images, des textes ou des propos obscènes, fait l'objet d'une peine d'emprisonnement de cinq ans à dix ans et d'une amende judiciaire pouvant aller jusqu'à cinq mille jours. Est puni d'un emprisonnement de deux ans à cinq ans et d'une amende judiciaire de cinq mille jours au plus, celui qui introduit ces produits dans le pays, les reproduit, les offre à la vente, les vend, les transporte, les stocke, les exporte, les garde ou les met à la disposition d'autrui »[37].

Mis à part les articles mentionnés ci-dessus, nous observons de même que les phénomènes de cyberviolence peuvent être encadrés par d'autres régulations, et notamment par exemple par la Loi n° 5651[38] (concernant le blocage à l'accès et la suppression du contenu) ou encore par la Loi n°

[36] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

[37] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

[38] Loi n° 5651 sur la réglementation des diffusions effectuées sur internet et la lutte contre les délits commis par le biais de ces diffusions *(5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun)*. A côté de cela, nous devons également mentionner la Loi n° 7253 portant sur la modification de la loi concernant l'organisation des diffusions sur internet et la lutte contre les délits commis par le biais de ces diffusions (connue comme la « Loi sur les médias sociaux ») (2020) *(7253 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun (« Sosyal Medya Kanunu »))*.

6284 concernant la Protection de la famille et la prévention de la violence à l'égard des femmes. Par ailleurs, l'article 96 concernant le supplice, l'article 232 renvoyant au crime de mauvais traitement (Aksoy Retornaz, 2021, p. 85 et p. 95) ainsi que l'article 84 (renvoyant à l'incitation au suicide)[39] peuvent être aussi saisi dans certaines situations.

Dans le cadre de notre recherche, si nous tenons compte du fait qu'une partie non négligeable des cas (11 sur 23) concernent les enfants en tant que victime, l'article 103 du Code pénal doit alors être également rappelé. Celui-ci dans son premier paragraphe stipule que : « Quiconque abuse sexuellement d'un enfant est condamné à une peine d'emprisonnement de huit ans à quinze ans. Si l'abus sexuel reste au niveau de l'atteinte à la pudeur (*sarkıntılık*), il est condamné à une peine d'emprisonnement de trois à huit ans. (…) Si la victime n'a pas douze ans révolus, la peine ne peut être inférieure à dix ans en cas d'abus et à cinq ans en cas d'attentat à la pudeur »[40].

Quant aux sanctions prévues à l'encontre de ces infractions, il s'agit plutôt de peines de prison et d'amendes judiciaires. Sans les détailler ici infraction par infraction, nous pouvons dire que les durées d'emprisonnement varient de trois mois à quinze ans[41]. Cette période peut de même se voir allongée selon l'existence ou non de circonstances aggravant la peine (comme par exemple le fait d'être mineur ou d'être dépourvu de la capacité de discernement) ou encore en cas d'accumulation de différentes infractions au sein d'un même cas. Concernant les amendes, nous observons qu'elles peuvent être exprimées directement (en termes de montant) ou en termes de jours d'emprisonnement.

Les plaintes, quant à elles, peuvent être déposées auprès du Parquet général, des commissariats de police ou de gendarmerie, de la Direction générale de la lutte contre la cybercriminalité[42] et du CIMER (à savoir le « Centre de communication présidentiel »). Les tribunaux correctionnels de première instance et les cours d'assises constituent les juridictions qui traitent ces infractions (*Kadim Hukuk ve Danışmanlık*). Cependant, lorsque l'auteur est mineur, on constate que ce sont les cours d'assises pour enfant qui prennent en charge les dossiers.

Par ailleurs, nous tenons à préciser qu'étant donné la non-définition de ces infractions dans le Code pénal, il nous est impossible de les refléter sous forme statistique. En d'autres termes, mis à part les études citées tout au long de l'article, nous ne

[39] Kadim Hukuk ve Danışmanlık, « Bilişim Suçları Nereye Nasıl Şikayet Edilir? », Disponible sur : https://kadimhukuk.com.tr/makale/bilisim-suclari-nereye-nasil-sikayet-edilir/

[40] Disponible sur : https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf Par ailleurs, « par le terme abus sexuel, le Code pénal entend : a) Toutes sortes de comportements sexuels à l'encontre d'enfants qui n'ont pas atteint l'âge de quinze ans ou qui n'ont pas encore développé la capacité de percevoir le sens juridique et les conséquences de l'acte, b) Contre d'autres enfants uniquement les comportements sexuels sur la base de la contrainte, de la menace, de la tromperie ou de toute autre raison affectant la volonté ». Disponible sur : https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

[41] Cette durée est augmentée à travers les modificiations qui ont été apportés en 2014 et 2016 à l'article 103 du Code pénal.

[42] « (…) Afin de lutter efficacement et efficacement contre la cybercriminalité, le Département de la lutte contre la cybercriminalité a été créé au sein de la Direction générale de la sécurité avec la décision du Conseil des ministres n° 2011/2025 ; Conformément à l'autorisation ministérielle du 28/02/2013, le nom de la Direction de la lutte contre les crimes d'information a été changé en Direction de la lutte contre la cybercriminalité. » (Source : « Siber Suçlarla Mücadele Daire Başkanlığı », Disponible sur : https://www.egm.gov.tr/siber/hakkimizda2) Nous constatons que même si avec cette modification la définition de ce qui est considéré comme cybercrime a acquis un contenu plus large (dépassant les infractions liées au hacking), dans les statistiques, c'est l'usage de crimes d'information (*Bilişim Suçları*) qui est maintenu. En lien avec ces réorganisations, il convient aussi de mentionner l'introduction de la « cyber police, également connue sous le nom d'unité de lutte contre les cybercrimes. Cette unité fait partie d'unités telles que l'ordre public, la branche de la circulation, c'est-à-dire qu'elle fait partie intégrante de la police, et non d'une branche ou un groupe professionnel distinct. L'objectif général de la cyberpolice est de traiter les crimes commis sur Internet (…) ». (Source : *Siber Polis Nasıl Olunur ? Siber Polis Nedir ?* Disponible sur : https://polisalimi.net/siber-polis-nasil-olunur-siber-polis-nedir/)

sommes pas en mesure *à ce stade* de fournir au lecteur des données quantifiées. Nos entretiens exploratoires avec deux avocats (et notamment avec un des membres de la Commission de X du Barreau d'Istanbul) nous ont également confirmé cette difficulté à obtenir de telles données.

En outre, d'un point de vue culturel, la honte provoquée par l'exposition d'images dévoilant l'intime peut également pousser les victimes à rester dans le silence et à ne pas parler de ces attaques. Dans ce cas précis, il devient donc plus difficile d'établir des statistiques précises de ces violences numériques. D'ailleurs, force est de constater que dans les cas récoltés, peu de place est faite au ressenti des victimes.

Lorsque nous considérons l'ensemble des cas que nous avons recensés (à cet égard, il convient de rappeler le fait qu'un cas peut contenir plus d'une infraction), les actes les plus fréquents sont l'intimidation, la menace, le harcèlement/harcèlement sexuel, le dénigrement, l'abus sexuel de mineurs, la diffusion de photographies non autorisées, mais aussi l'utilisation non consentie d'images, le partage d'images obscènes et dénudées de mineurs, la divulgation des images de la vie privée, le chantage, l'insulte, le stockage d'images obscènes dans l'ordinateur, la saisie illégale de données personnelles.

En tenant compte des faits relatés, on observe que les agresseurs (à l'exception de deux cas[43]) sont des hommes agissants seuls ou en groupe. Lorsqu'il s'agit des crimes traités dans le cadre de l'article 226/3, les journalistes tendent à fournir plus de précisions, et notamment sur les profils des agresseurs (comme par exemple : « 46 suspects dont 4 fonctionnaires »).

Quand il s'agit des victimes et d'agresseurs de tranches d'âges plutôt proches, les crimes relèvent plus de la violation de la vie privée et du chantage.

La diffusion de « photographies personnelles (dérangeantes, indécentes) », d' « images obscènes », d' « images de la vie privée », de « photographies obscènes », des « images indécentes » (*uygunsuz fotoğraf*), « privées » (*özel fotoğraflar*) ou encore des « photographies d'enfant nu » sont partagées dans la majorité des cas avec des personnes anonymes.

Quant aux prises en charges des affaires par les instances juridiques, dans tous les cas recensés (à l'exception d'un sur lequel nous viendrons), il existe un traitement judiciaire soit sur le point de débuter, soit en cours, soit déjà conclu. Lorsque nous analysons les contenus des nouvelles répondant à la thématique des « sanctions juridiques appliquées », en ce qui concerne les procès conclus, on observe quasi systématiquement (sauf un dont les informations fournies dans le journal restent floues) qu'une sanction est appliquée souvent sous forme d'incarcération (avec ou sans amende pécuniaire) sinon, sous forme de contrôle judiciaire ou amende pécuniaire.

Comme nous pouvons l'imaginer, selon la nature de l'infraction, l'individu peut faire l'objet de sanctions multiples. Dans le cas d'O.A. par exemple, le tribunal décide de lui infliger une amende judiciaire de 3 ans pour le délit de divulgation de la vie privée, 3 ans pour le délit d'obtention illégale de données personnelles, 2 ans, 6 mois et 10 mille lires pour le chantage exercé (Hürriyet, 13.11.17) ; un autre exemple est celui de C.O., condamné à 2 ans, 10 mois de prison et 120 jours d'amende judiciaire pour « harcèlement sexuel contre l'enfant » et « chantage » (Hürriyet, 16.03.17).

Par ailleurs, nous constatons que lorsque la victime est mineure, que l'infraction relève du « harcèlement

[43] Pour l'un, il s'agit d'une banque ayant utilisé la photographie d'une personne sans lui avoir demandé la permission, et pour l'autre, il s'agit d'un auteur non-identifié.

sexuel qualifié » (*nitelikli cinsel taciz*) et qu'il est accompagné de menace et de chantage, la sanction pénale semble devenir plus importante, comme l'illustre la condamnation de C.K. et de ses amis : le premier se verra écoper d'une peine de prison de 132 ans et 6 mois, Y.Ç. de 39 ans et N.S. de 52 ans (Hürriyet, 19.02.18). Il convient également de noter que dans cette affaire, nous sommes face à une infraction répétée. Dans un autre cas où toutes les victimes sont des mineures, nous observons que le tribunal condamne aussi A. à un total de 110 ans et à une amende de 668.000 lires pour harcèlement sexuel, chantage, insultes et stockage d'images obscènes sur son ordinateur (Hürriyet, 20.01.22). L'une des particularités de ce procès est qu'il a duré 11 ans.

En outre, on constate que lorsque les cas d'atteintes faisaient l'objet d'une réponse judiciaire, celle-ci était mentionnée sans pour autant que les lois ou articles[44] auxquels elle répondait ne soient cités.

Quant au seul cas où nous observons une absence de prise en charge judiciaire, il s'agit plutôt *d'une sorte de laisser-aller* qui est lié à la fois au caractère de l'affaire (qui devient plus complexe lorsque l'auteur et la victime sont des enfants) mais aussi au fonctionnement de la justice des mineurs en Turquie. Ainsi, lorsque l'avocat et la police déclarent à la mère de la victime mineure qu'ils ne peuvent pas obtenir une réponse à leur demande parce que l'agresseur est également un enfant (Hürriyet, 13.03.19), ils pointent (d'une manière implicite) le dilemme qui régit les juridictions réservées au traitement des infractions commises par les enfants ; c'est-à-dire que « dans le discours », le système se déclare « protectionnel », alors que dans les pratiques, il s'agit d'un traitement répressif des enfants définis comme étant « en conflit avec la loi » avant tout par le fait d'ignorer que dans la quasi-totalité des cas, il est possible de les traiter en dehors du champ pénal classique (Irtis, 2009 et 2014). Ce qui est exprimé par l'avocat et la police ici, reflète une autre façade (paradoxale) de ces pratiques répressives. Comme nous l'avons très souvent entendu durant nos travaux menés dans le champ de la justice des mineurs, les juges se sentent particulièrement contraints d'agir lorsque l'auteur et la victime sont des enfants. Étant donné qu'ils ont l'habitude de fonctionner, dans la majorité des cas, comme des juges pénaux, ils pensent qu'il faut « sanctionner », alors que la Loi de la protection de l'enfance ainsi que les Conventions internationales leur donne la possibilité de traiter ces mineurs en dehors du filet judiciaire. Dans certains cas – comme dans celui que nous venons d'évoquer – ils ne veulent (pour des raisons et des motifs variés) pas « punir ». Et cette volonté de ne pas « sanctionner » s'exprime par le fait de « laisser tomber » (selon des modalités variées) l'« affaire ».

N'ayant pas accès aux détails de ces traitements judiciaires, il est difficile d'évaluer les conditions d'enquête et celle du processus du jugement pour chacun des cas[45]. Il est certain que ce manque nous oblige à avoir certaines réserves sur ce que nous relatons. Cependant, notre corpus nous permet déjà d'observer *une certaine zone d'incertitude* concernant la prise en charge *équitable* de ces violences numériques. Par exemple, dans l'un des cas, alors que le récit se forme autour du crime de l'abus sexuel d'un enfant, l'enquête juridique se fait conformément à l'article 226/3 (faisant référence au

[44] Il s'agit de 136(1) et 226/3 du Code Pénal.

[45] C'est à cet égard que nous pensons qu'il faudrait effectuer un travail de terrain (en assistant aux procès, en réalisant des entretiens avec les acteurs variés de l'appareil judiciaire ainsi qu'avec les victimes et si possible, avec les inculpés) non seulement pour mieux cerner les enjeux de ces prises en charge judiciaire, mais aussi pour réfléchir sur les règles juridiques qui les régissent afin de voir de plus près ce domaine que nous qualifions « en chantier ».

fait d'apporter, de dupliquer, de vendre, de stocker et d'utiliser des produits obscènes incluant des enfants) du Code pénal. D'ailleurs, si nous suivons l'article 103 du Code pénal, tout acte sexuel envers un enfant de moins de 15 ans pourrait être considéré comme un crime d'abus sexuel et l'acte en question peut être jugé en fonction.

En tenant compte d'autres cas, nous sommes amenés à nous demander s'il n'existe pas de différences au niveau des peines infligées (pour un même type de transgression) selon la taille et/ou caractéristiques des villes dans lesquelles sont situées les juridictions.

Mis à part ces incertitudes, il existe d'autres facteurs au sens plus large (et qui ne sont pas forcément observables dans notre corpus) qui semblent intervenir d'une manière directe ou indirecte dans la prise en charge *ou non* juridique et judiciaire de ces violences telles que : la définition « en chantier » de ce que les instances juridiques nomment les « crimes numériques » ou les « cyber crimes » ; la complexité des affaires et leurs particularités qui exigent de trouver des peines adaptées à chaque type d'agressions ; les difficultés émanant de l'espace numérique (ex. anonymat des agresseurs, problème pour récupérer les preuves) ; le manque de connaissance des individus de l'utilisation des outils technologiques, mais surtout de leurs droits ; la possibilité pour les agresseurs d'obtenir une réduction de peine s'ils se repentent (*Etkin pişmanlık ceza indirimi*) et la possibilité de convertir la peine en amende.

5. Conclusion

Internet est ainsi une « arène de réputation » : c'est un « espace au sein duquel se nouent des relations d'échange, de coopération et de compétition en vue de l'obtention de trophées » (Ragouet, 2000, p. 329), récompenses qui se cristallisent sous forme de « likes », de commentaires, d'augmentation du nombre de vues. Pour élaborer leur e-réputation, les individus vont ainsi mettre à contribution leur corps en le mettant en scène à travers les images. Or, dans cette recherche de reconnaissance, ils s'exposent malgré eux à des risques qui aujourd'hui semblent prendre de l'ampleur. Le destin de leurs propres images (et par là, celui de leur image sociale, véhiculée sur les réseaux) peut ainsi, on l'a vu, leur échapper. Les réseaux sociaux sont alors devenus peu à peu des « terrains de chasse pour les prédateurs » qui profitent des modalités du Net pour agir sous couvert d'anonymat, mais aussi en toute impunité. Se servant des traces laissées par les individus ou des informations que ces derniers ont eux-mêmes partagées avec eux, les agresseurs font preuve d'une rigueur certaine dans leurs méfaits : on observe ainsi une large variété de formes d'humiliations mais aussi d'abus sexuels dans l'espace médiatique. Peut être cité par exemple les discours de dévalorisation (Breton, 2001), les ordalies (Lachance, 2016), les « Fauxtography », (Froissard, 2009), le harcèlement…

Ainsi, même si le corps n'est pas la cible principale des rumeurs visuelles, il reste pourtant un objet d'attaque privilégié : comme le montre Fine (1986), l'image partagée en ligne peut être diffusée dans d'autres sphères, à travers des canaux réputationnels plus traditionnels, tels que les commérages ou les rumeurs. Nous sommes ainsi bien loin de ce que Casilli (2010, p. 136) nomme « l'invulnérabilité du corps » sur Internet, et notamment dans les communautés virtuelles telles que Seconde Life : l'auteur montre notamment que dans ces espaces, les corps par leur représentation graphique (Flichy, 2009, p. 168) peuvent « mourir », « ressusciter », sauter d'un gratte-ciel… Or, dans le cas des

cyberviolences, lorsque le corps est dénigré, c'est bien l'image sociale (et donc la réputation) de l'individu qui se voit souillée, et ce, pour de bon.

L'inexistence de corporalité sur le Net semble ainsi jouer un rôle non négligeable dans la perpétuation de ces agressions : l'invisibilité des corps tend à faire oublier aux internautes que derrière l'écran, se trouve bel et bien une personne. Ainsi, le corps dans le monde numérique est victime d'un stratagème de dématérialisation.

Malgré la persistance des cyberviolences, force est de constater que les individus sont loin d'ignorer les risques auxquels ils s'exposent dans l'espace numérique. Blaya (2016) montre par exemple que les jeunes craignent qu'un inconnu mal intentionné profite de l'anonymat de la Toile pour venir les espionner. Peu à peu, on voit d'ailleurs se développer des stratégies individuelles en vue de contourner ces agressions : Déage (2018) évoque la création de faux comptes par certaines adolescentes, qui vont jusqu'à utiliser des photos d'inconnues récupérées sur Instagram, en vue d'éviter de tomber sur des garçons « pas sérieux » qui dégraderaient leur image. Ainsi, « sous cette fausse identité, elles essaient de séduire le garçon pour vérifier s'il est vraiment sincère avec leur amie ou si c'est un « player » qui salirait sa réputation » (p. 168). Une autre stratégie consisterait à partager de son propre chef des images dégradantes de soi-même (des « photos fichas[46] ») afin de divertir ses amis, mais en camouflant avec des filtres et autocollants son visage ou des parties de son corps. Cette tactique offre à la personne une certaine liberté dans la diffusion de ses informations tout en lui permettant de maintenir un contrôle relatif sur le contenu partagé (p. 158).

Les cyberviolences, si elles sont de plus en plus combattues par les institutions au niveau international, tendent cependant à perdurer. Dans certains contextes, comme en Turquie, ces atteintes représentent un fléau auquel les autorités cherchent encore les moyens d'y répondre. Or, on l'a vu, la réponse juridique et judiciaire telle qu'elle est préconisée dans la société turque n'est, à ce jour, pas adaptée à ces types de violences spécifiques : il semblerait ainsi qu'en Turquie le monde numérique demeure encore aujourd'hui un espace où l'élaboration des lois et leurs applications demeurent en chantier et se doivent d'être améliorées.

Références

1. Akça E. B., Sayımer I., Ergül S., « Ortaokul Öğrencilerinin Sosyal Medya Kullanımları ve Siber Zorbalık Deneyimleri », *Global Media Journal Turkish Edition*, Spring, vol. 5, n. 10, 2015, pp. 71-86.
2. Aksaray S., « Siber Zorbalık », *Çukurova Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi*, vol. 20, n. 2, 2011, pp. 405-432.
3. Aksoy Retornaz, E. *Bir Siber Taciz Biçimi : Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deep Fake),* 2021, onikilevha.
4. Allport G. W. et Postman L. J., *The Psychology of Rumor*, New York, Russel & Russel, 1965.
5. Arıcak T., *Siber Alemin Avatar Çocukları*. İstanbul, Remzi Kitabevi, 2015.
6. Arslan S., Savaser S., Hallett V., Balci S., « Cyberbullying among primary school students in Turkey: Self-reported prevalence and associations with home and school life », *Cyberpsychology, Behavior, and Social Networking*, n. 15, 2012, pp. 527-533.
7. Arsoy A., Ersoy M., « Üniversite Öğrencilerinin Sosyal Ağlardaki Siber Zorbalık Tutum ve Davranışları », dans Özgür A.Z., İşman A. (dir.), *İletişim*

[46] De « se taper l'affiche », être humilié publiquement.

Çalışmaları, Sakarya Üniversitesi Yayını, Sakarya, n. 134, 2015, pp. 353-368.
8. Aslan A., Önay Doğan, B., « Çevrimiçi Şiddet: Bir Siber Zorbalık Alanı Olarak "Potinss" Örneği », *Marmara İletişim Dergisi / Marmara Journal of Communication*, n. 27, 2017, pp. 95-119.
9. Baldry A.C., Farrington D.P., Sorrentino A., « "Am I at risk of cyberbullying"? A narrative review and conceptual framework for research on risk of cyberbullying and cybervictimization: The risk and needs assessment approach », *Aggression and Violent Behavior*, vol. 23, 2015, pp. 36-51.
10. Bartow A., « Internet Defamation as Profit Center: The Monetization of Online Harassment », *Harvard Journal of Law and Gender*, vol. 32, n. 2, 2009, pp. 101-147.
11. Bernard Barbeau, G., « Le bashing : forme intensifiée de dénigrement d'un groupe », *Signes, Discours et Sociétés*, n. 8, 2012, [en ligne], disponible à l'adresse suivante : http://www.revue-signes.info/document.php?id=2478 (13 juillet 2019).
12. Beyazit U., Şimşek Ş., Ayhan A. B., « An examination of the predictive factors of cyberbullying in adolescents, *Social Behavior and Personality*, n. 45, 2017, pp. 1511-1522.
13. Beyens J., Lievens E., « A Legal Perspective on the Non-Consensual Dissemination of Sexual Images: Identifying Strengths and Weaknesses of Legislation in the US, UK and Belgium », *International Journal of Law Crime and Justice*, vol. 47, 2016, pp. 31-43
14. Blaya C., « Le cyberharcèlement chez les jeunes », *Enfance*, vol. 3, n. 3, 2018, pp. 421-439.
15. Blaya C., « Cyberviolence : état de la question », in Debarbieux É. (dir.), *L'école face à la violence : décrire, expliquer, agir*, Armand Colin, Paris, 2016, pp. 52-64.
16. Blaya C., *Les ados dans le cyberespace. Prises de risque et cyberviolence*, De Boeck Supérieur, Bruxelles, Paris, 2013.
17. Boyd D., *It's Complicated: The Social Lives of Networked Teens*, Yale University Press, New Haven-London, 2014.
18. Breton P., « Internet. La communication contre la parole ? », *Études*, vol. 394, n. 6, 2001, pp. 775-784.
19. Çalışkan M. « Toplum ve Suç Araştırmalarında Sınırları Aşan Bir Sorun "Çevrimiçi Çocuk İstismarı" », *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, nº 61, 2019, pp. 122-131
20. Carlson B. E., « Dating violence : a research review and comparison with spouse abuse », *Social Casework : The Journal of Contemporary Social Work*, vol. 68, n. 1, 1987, pp. 16-23.
21. Casilli A., *Les liaisons numériques, Vers une nouvelle sociabilité ?,* Éditions du Seuil, Paris, 2010.
22. Chenavaz R., Paraschiv C. « Processus de rencontre sur Internet : une étude empirique de la perception du risque », *Management & Avenir*, vol. 44, n. 4, 2011, pp. 124-146.
23. Çifçi S., « Dokuzuncu sınıf öğrencilerinin sanal zorbalık düzeyleri ile empatik eğilim düzeyleri arasındaki ilişki », Mémoire de Master, Université : Gaziosmanpaşa Üniversitesi, Tokat, 2010.
24. Citron D. K., Franks M. A., « Criminalizing Revenge Porn (May 19, 2014) », *Wake Forest Law Review*, vol. 49, p. 345-391, pp. 346.
25. Clair I., *Les jeunes et l'amour dans les cités*, Armand Colin, Paris, 2008.
26. Cooper K., Quayle E., Jonsson L., Svedin C.G., « Adolescents and self-taken sexual images: A review of the literature », *Computers in human behavior*, n. 55, 2016, pp. 706-716.
27. Couchot-Schiex S., Moignard B., Richard G., *Cybersexisme : Une étude sociologique dans des établissements scolaires franciliens*, Centre Hubertine Auclert, 2016.
28. Davis K., « Coming of age online: The developmental underpinnings of girls' blogs », *Journal of Adolescent Research*, vol. 25, n. 1, 2010, pp. 145-171.
29. Déage M., « S'exposer sur un réseau fantôme. Snapchat et la réputation des collégiens en milieu populaire », *Réseaux*, vol. 208-209, n. 2-3, 2018, pp. 147-172.
30. Debarbieux É., Alessandrin A., Dagorn J., Gaillard O., « Les violences sexistes à

l'école. Une oppression viriliste », *Rapport de l'Observatoire européen de la violence à l'École*, 131 p., 2018, [en ligne], disponible à l'adresse suivante : http://prevenance-asso.fr/wp-content/uploads/2018/06/Les-violences-sexistes-%C3%A0-l%E2%80%99%C3%A9cole-une-oppression-viriliste.pdf

31. Demirtaş Ö., Karaca M, « Siber Mobbing : Kavramsal Çerçeve, Öncülleri ve Sonuçları », *International Journal of Entrepreneurship and Management Inquiries*, vol. 2, 2018, pp. 20-34.
32. Desfachelles M., Fortin F., « Le sexting secondaire chez les adolescent·e·s. Origine et enjeux d'une source de cyberintimidation », *Déviance et Société*, n. 43, 2019, pp. 329-357.
33. Dilmaç J. A., Kocadal Ö., « Prévenir le cyberharcèlement en France et au Royaume-Uni : une tâche impossible ?», *Déviance et Société*, vol. 43, n. 3, 2019, pp. 389-419.
34. Dilmaç J. A., « L'humiliation sur Internet : Une nouvelle forme de cyberdélinquance ? », *Déviance et Société*, n. 41, 2017, pp. 305-330.
35. Dilmaç J. A., « Du regard qui jauge au regard qui juge : De nouvelles manières de regarder sur Internet », *Influxus*, 2015 [en ligne], disponible à l'adresse suivante : http://www.influxus.eu/article925.html.
36. Douglas D. M., « Doxing: a conceptual analysis », *Ethics and Information technology*, vol. 18, n. 3, 2016, pp. 199-210.
37. Dredge R., Gleeson J., Garcia X. P., « Presentation on facebook and risk of cyberbullying victimisation », *Computers in Human Behavior,* n. 40, 2014, pp. 16-22.
38. Erdur-Baker Ö., Kavşut F., « Akran zorbalığının yeni yüzü: Siber zorbalık », *Eurasian Journal of Educational Research*, n. 27, 2007, p. 31-42.
39. Fine G. A., « The Social Organisation of Adolescent Gossip: The Rhetoric of Moral Education », dans Cook-Gumperz J. *et al.* (dir.), *Children's Worlds and Children's Language*, De Gruyter-Mouton, Berlin-Boston, 1986, p. 406-421.
40. Flichy P., « Le corps dans l'espace numérique », *Esprit*, n. 3-4, 2009, pp. 163-174.
41. Froissart P., « Les images rumorales. Une nouvelle imagerie populaire sur internet », *Médiamorphoses*, n. 5, 2002, pp. 27-35.
42. Girot J.-L. (dir.), *Le harcèlement numérique*, Dalloz, Paris, 2005.
43. Grigg D.W., « Cyberaggression: Definition and concept of cyberbullying », *Australian Journal of Guidance and Counselling*, vol. 20, n. 2, 2010, pp. 143-156.
44. Hall M., Hearn J., « Revenge pornography and manhood acts: a discourse analysis of perpetrators' accounts », *Journal of Gender Studies*, vol. 28, n. 2, 2019, pp. 158-170.
45. Haroche C., « L'invisibilité interdite », in Aubert N. et Haroche C. (dir.), *Les tyrannies de la visibilité. Être visible pour exister ?*, Érès, Toulouse, 2011, pp. 77-102.
46. Haroche C., « Des formes et des manières en démocratie », *Raisons politiques*, vol. 1, n. 1, 2001, pp. 89-110.
47. Hinduja S., Patchin J.W., « Cyberbullying: An exploratory analysis of factors related to offending and victimization », *Deviant Behavior*, vol. 29, n. 2, 2008, pp. 129-156.
48. Huerre P., Rubi S., Lanchon A., *Adolescentes, les nouvelles rebelles*, Bayard, Paris, 2013.
49. GREVIO, « Recommandation générale n° 1 du GREVIO sur la dimension numérique de la violence à l'égard des femmes adoptée le 20 octobre 2021 », 2021, disponible à l'adresse suivante : https://rm.coe.int/reccomandation-no-du-grevio-sur-la-dimension-numerique-de-la-viomence-/1680a49148
50. Ikiz, S., « Les violences à l'encontre des femmes sur les réseaux sociaux », *Topique*, n. 143, 2018, pp. 125-138.
51. Irtis, V., « Comprendre la justice pénale des mineurs en Turquie. Une attitude à la fois punitive et laxiste et l'expression d'une volonté solidaire », *Déviance et société*, vol. 33, 2009, pp. 399-424.
52. Irtis, V., « Etre juge de tribunal pour enfants en Turquie. Entre répression pénale et considérations sociales », *Ethnologie française*, XLIV, n. 2, 2014, pp. 227-236.

53. Jane, E. A., « Flaming? What flaming? The pitfalls and potentials of researching online hostility », *Ethics and Information Technology*, vol. 17, n. 1, 2015, pp. 65-87.
54. Jurviste U. et Shreeves R., Service de recherche pour les députés, PE 659.334, « La Convention d'Istanbul, un outil pour lutter contre les violences à l'encontre des femmes et des filles », novembre 2020, disponible à l'adresse : https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/659334/EPRS_ATA(2020)659334_FR.pdf
55. Kowalski R. M., Limber, S. P., Agatston, P. W., *Cyber bullying: bullying in the digital age*, Malden, MA, Blackwell Publishers, 2008.
56. Lachance J., « Internet et sexualité des adolescents : comprendre leurs rituels d'interactions et de séduction », *La santé de l'homme,* Inpes, n. 418, 2012, pp. 19-20.
57. Lachance J., « Reconnaissance, ordalie et sacrifice à l'ère du numérique », in Jeffrey D. (dir.), *Penser l'adolescence*, Presses Universitaires de France, Paris, 2016, pp. 177-189.
58. Lenhart A., *Teens and sexting, A Pew Internet & American Life Project Report*, n. 1, 2009, pp. 1-26.
59. Livingstone S., Haddon L., Görzig A., Ólafsson K., *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*, EU Kids Online, Deliverable D4, EU Kids Online Network, London, UK, 2011.
60. Macilotti G., « Violence et humiliation à l'ère numérique : une étude en milieu scolaire », *Déviance et Société*, vol. 43, 2019, pp. 299-328.
61. Metton C., « Les usages de l'Internet par les collégiens. Explorer les mondes sociaux depuis le domicile », *Réseaux*, n. 123, 2004, pp. 59-84.
62. Mongin O., « La société des écrans », *Communications*, Le sens du regard, n. 75, Seuil, Paris, 2004, p. 219-227.
63. Moon Y., « Intimate exchanges: Using computers to elicit self-disclosure from consumers », *Journal of Consumer Research*, vol. 26, n. 4, 2000, pp. 323-339.
64. Morin E. *et al.*, *La Rumeur d'Orléans*, Paris, Seuil, 1969.
65. Narin B., Ünal S., « Siber Zorbalık İle İlgili Haberlerin Türkiye Yazılı Basınında Çerçevelenişi », *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, n. 26, 2016, pp. 9-23.
66. Olweus D., *Aggression in the schools: Bullies and whipping boys*, Hemisphere, Washington, 1978.
67. Önay Doğan B., Ertürk Y. D., Aslan P., « Facebook Kullanıcısı Kız Çocuklarına Yönelen Zorbalık Odaklı Siber Tacizin Cinsel Tacize Dönüşümü : Gazete Haberleri Üzerinden Betimsel Bir Değerlendirme », *Etkileşim*, n. 2, 2018, pp. 36-55.
68. O'Sullivan P. B., Flanagin A. J., « Reconceptualizing "flaming" and other problematic messages », *New Media & Society*, vol. 5, n. 1, 2003, pp. 69-94.
69. Özdemir M., Akar F., « Lise öğrencilerinin siber zorbalığa ilişkin görüşlerinin bazı değişkenler bakımından incelenmesi », *Kuram ve Uygulamada Eğitim Yönetimi*, vol. 17, n. 4, 2011, pp. 605- 626
70. Peker A., « Ergenlerin saldırganlık ve siber zorbalık davranışları arasındaki ilişkilerin incelenmesi », *Ekev Akademi Dergisi*, vol. 19, n. 61, 2015, pp. 323-336.
71. Pikas A., « Treatment of Mobbing in School: Principles for and the Results of the Work of an Anti-Mobbing Group », *Scandinavian Journal of Educational Research*, vol. 19, n. 1, 1975, pp. 1-12.
72. Ragouet P., 2000, « Notoriété professionnelle et organisation scientifique », *Cahiers internationaux de sociologie*, vol. 109, pp. 317-341.
73. Ringrose J., Gill R., Livingstone S., Harvey L., *A qualitative study of children, young people and "sexting" : A report prepared for the NSPCC*, NSPCC, Londres, 2012.
74. Robitaille-Froidure A., « Sexting : les adolescents victimes (consentantes ?) de la révolution numérique », *La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux*, n. 5, 2014, [en ligne], disponible à l'adresse suivante :

http://journals.openedition.org/revdh/786
Rosen L., Cheever N., Cummings C., Felt J., « The impact of emotionality and self-disclosure on online dating versus traditional dating », *Computers in Human Behavior*, n. 24, 2008, pp. 2124-2157.
75. Rosenbaum A., « Le devoir de regard », *Communication et langages*, n° 117, 3ème trimestre, 1998, pp. 28-34.
76. Sautter J., Tippett R., P. Morgan, « The Social Demography of Internet Dating in the United States », *Social Science Quarterly*, vol. 91, n. 2, 2010, pp. 554-575.
77. Schouten A. P., Valkenburk P.M., Peter J., « Precursors and underlying processes of adolescents' online self-disclosure: Developing and testing an "Internet-attribute-perception" model », *Media Psychology*, vol. 10, n. 2, 2007, pp. 292-315.
78. Şener M. T., Set T., Dursun O. B., « Güvensiz İnternet Kullanımı İle İlgili Bir Olgu Sunumu: Sanal Taciz », *Türk Aile Hekimleri Dergisi*, vol. 16, n. 3, 2012, pp. 127-129.
79. Sentenac M., Pacoricona D., Godeau E., « Comment les élèves handicapés perçoivent-ils le collège ? Un climat scolaire inclusif pour une école plus inclusive », *Agora débats/jeunesses*, hors-série, n. 4, 2016, pp. 79-94.
80. Stassin B., *(Cyber)harcèlement. Sortir de la violence, à l'école et sur les écrans*, C&F Éd., Caen, 2019.
81. Suler J., « The Online Disinhibition Effect », *CyberPsychology & Behavior*, n. 7, 2004, pp. 321-326.
82. Tamer N., Vatanartıran S., « Ergenlerin Teknolojik Zorbalık Algıları ve Buna Yönelik Teknolojik Zorbalık Farkındalığı Eğitimi: Pilot Uygulama », *Yeni Medya Çalışmaları II. Ulusal Kongre Kitabı*, Alternatif Bilişim Derneği, 2016, pp. 54-66.
83. Topçu Ç., « The relationship of cyber bullying to empathy, gender, traditional bullying, internet use and adult monitoring », Mémoire de Master, Université : Ortadoğu Teknik Üniversitesi, Ankara, 2008.
84. Uçanok Z., Karasoy D., Durmuş E., « Yeni Bir Akran Zorbalığı Türü Olarak Sanal Zorbalık: Ergenlerde Yaygınlığı ve Önemi », Projet TÜBİTAK, n. 108K424, 2011.
85. Valkenburg P.M., Peter J., « Online communication among adolescents: An integrated model of its attraction, opportunities, and risks », *Journal of Adolescent Health*, vol. 48, n. 2, 2011, pp. 121-127
86. Velten J., Arif R., Moehring D., « Managing Disclosure through Social Media: How Snapchat is Shaking Boundaries of Perceptions », *The Journal of Social Media in Society*, vol. 6, n. 1, 2017, pp. 220-248.
87. Vincent-Buffault A., « Regards, égards, égarements dans la ville aux XVIIIe et XIXe siècles », *Communications*, Le sens du regard, n. 75, Seuil, Paris, 2004, pp. 39-56.
88. Vrooman S., « The art of invective Performing identity in cyberspace », *New Media Society*, vol. 4, n° 1, 2002, pp. 51-70.
89. Willard N.-E., *Cyberbullying and cyberthreats. Responding to the challenge of online social agression, threats and distress*, Research press, 2007.

Sitographie

1. Atam H., « Sosyal Medyada "manken oyununa" polis dur dedi », *Sözcü Gazetesi*, 17.01.19, disponible à l'adresse suivante : https://www.sozcu.com.tr/2019/gundem/cinsel-taciz-cetesinin-manken-oyunu-polisetakildi-yaklasik-2-bin-magdur-var-3162268/
2. Baş H., « Kadına "dijital" şiddet de arttı », *Milliyet*, 27.07.20, disponible à l'adresse : https://www.milliyet.com.tr/ekonomi/kadina-dijital-siddet-de-artti-6269025
3. *Birgün*, 16.03.17, « Facebook'ta çocuğa cinsel taciz ve şantaja 2 yıl 10 ay hapis », disponible à l'adresse : https://www.birgun.net/haber/facebook-ta-cocuga-cinsel-taciz-ve-santaja-2-yil-10-ay-hapis-151143
4. *Birgün*, 21.01.20, « Eski sevgilisinin fotoğraflarını başklarına göderen erkek, serbest bırakıldı », disponible à l'adresse : https://www.birgun.net/amp/haber/eski-

sevgilisinin-ozel-fotograflarini-baskalarina-gonderen-erkek-serbest-birakildi-284865
5. *Birgün*, 4.08.17, « 14 yaşındaki çocuğa "çıplak fotoğraf" şantajı! », disponible à l'adresse : https://www.birgun.net/amp/haber/14-yasindaki-cocuga-ciplak-fotograf-santaji-173195
6. Boyd D., « Reflections on Lori Drew, bullying, and solutions to helping kids », 30.11.2008, blog consultable en ligne : http://www.zephoria.org/thoughts/archives/2008/11/
7. Centre National de Ressources Textuelles et Lexicales (CNRTL), disponible à l'adresse : https://www.cnrtl.fr/definition/obscene
8. Digital Şiddet.org, disponible à l'adresse suivante : https://dijitalsiddet.org/wp-content/uploads/2021/09/konda-rapor-8eylul.pdf
9. Conseil de l'Europe, Droits des Enfants, Convention de Lanzarote, disponible à l'adresse : https://www.coe.int/fr/web/children/lanzarote-convention
10. Convention de l'Europe, Convention sur la cybercriminalité, Convention sur la cybercriminalité Budapest, 23.XI.2001, STE n° 185, disponible à l'adresse : https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf
11. Décision du 10.04.17, disponible à l'adresse : https://mus.meb.gov.tr/meb_iys_dosyalar/2017_04/11084606_Potinss_UygulamasY.pdf
12. Direction générale de la lutte contre la cybercriminalité, disponible à l'adresse : https://www.egm.gov.tr/siber/hakkimizda2
13. *Hürriyet*, 11.01.22, « Çocuklara ait müstehcen görüntü operasyonu: Aralarında kamu personelinin de olduğu 44 kişi hakkında gözaltı kararı », disponible à l'adresse : https://www.hurriyet.com.tr/gundem/cocuklara-ait-mustehcen-goruntu-operasyonu-aralarinda-kamu-personelinin-de-oldugu-44-kisi-hakkinda-gozalti-karari-41979394
14. *Hürriyet*, 11.03.18, « Hayatını kâbusa çeviren tacizcisinin ses kaydını sosyal medyadan yayınladı » disponible à l'adresse : https://www.hurriyet.com.tr/gundem/hayatini-kabusa-ceviren-tacizcisinin-ses-kaydi-sosyal-medyadan-yayinladi-40768305
15. *Hürriyet*, 12.04.19, « Sosyal medya üzerinden kadınlara şantaj şüphelisi yakalandı », disponible à l'adresse : https://www.hurriyet.com.tr/gundem/sosyal-medya-uzerinden-kadinlara-santaj-suphelisi-yakalandi-41170063
16. *Hürriyet*, 13.03.19, « Sanal dünyada kötülük yalnızca yetişkinlerden gelmiyor », disponible à l'adresse : https://www.hurriyet.com.tr/teknoloji/sanal-dunyada-kotuluk-yalnizca-yetiskinlerden-gelmiyor-41147753
17. *Hürriyet*, 13.05.21, « Tanıştığı kişi genç kadına kâbusu yaşattı! Gizlice fotoğraflarını çekmiş », disponible à l'adresse : https://www.hurriyet.com.tr/gundem/tanistigi-kisi-genc-kadina-kabusu-yasatti-gizlice-fotograflarini-cekmis-41810107
18. *Hürriyet*, 13.11.17, « Ünlü oyuncunun kızına çıplak fotoğraf şantajı! », disponible à l'adresse : https://www.hurriyet.com.tr/gundem/unlu-oyuncunun-kizina-ciplak-fotograf-santaji-40643010
19. *Hürriyet*, 15.04.22, « Kadınların fotoğrafları ile hesap açtı, şantaj yaptı: Böyle yakalandı » disponible à l'adresse : https://www.hurriyet.com.tr/gundem/kadinlarin-fotograflari-ile-hesap-acti-santaj-yapti-boyle-yakalandi-42044086
20. *Hürriyet*, 15.10.20, « Çocukların müstehcen görüntülerini paylaşıyorlardı… », disponible à l'adresse : https://www.hurriyet.com.tr/gundem/son-dakika-haberler-cocuklarin-mustehcen-goruntulerini-paylasiyorlardi-flas-gelisme-41636794
21. *Hürriyet*, 16. 03.17 « Facebook'ta çocuğa cinsel taciz ve şantaja 2 yıl 10 ay hapis », disponible à l'adresse : https://www.birgun.net/haber/facebook-

ta-cocuga-cinsel-taciz-ve-santaja-2-yil-10-ay-hapis-151143
22. *Hürriyet*, 19.02.18, « Çıplak fotoğraflarla şantaj yaptı! Kararını duyunca bayıldı », disponible à l'adresse : https://www.hurriyet.com.tr/gundem/ciplak-fotograflarla-santaj-yapti-kararini-duyunca-bayildi-40746250
23. *Hürriyet*, 20.01.22, « Çocukların müstehcen görüntülerini çekiyordu: Rekor ceza », disponible à l'adresse : https://www.hurriyet.com.tr/gundem/cocuklarin-mustehcen-goruntulerini-cekiyordu-rekor-ceza-41986113
24. *Hürriyet,* 25.06.21, « Sosyal medyadan tanıştı! Hayatı kâbusa döndü... İğrenç şantaj böyle son buldu », disponible à l'adresse : https://www.hurriyet.com.tr/gundem/sosyal-medyadan-tanisti-hayati-kabusa-dondu-igrenc-santaj-boyle-son-buldu-41839514
25. *Istiklal*, 14.04.22, « İnternet kullanımı yaşı düştü, çocuklara karşı siber zorbalık arttı », disponible à l'adresse : https://www.istiklal.com.tr/haber/internet-kullanimi-yasi-dustu-cocuklara-karsi-siber-zorbalik-artti/684935
26. Kadim Hukuk ve Danışmanlık, « Bilişim Suçları Nereye Nasıl Şikayet Edilir? », disponible à l'adresse : https://kadimhukuk.com.tr/makale/bilisim-suclari-nereye-nasil-sikayet-edilir/
27. *Milliyet*, 30.05.21, « Son dakika : Hayatını zindana çevirdi! Sosyal medyada eskort hesabı », disponible à l'adresse suivante : https://www.milliyet.com.tr/gundem/son-dakika-hayatini-zindana-cevirdi-sosyal-medyada-eskort-hesabi-6518200
28. *Milliyet*, 30.09.21, « Kabusu yaşıyorlar ! Yüzde 20 artış siber zorbalığı patlattı », disponible à l'adresse : https://www.milliyet.com.tr/gundem/kabusu-yasiyorlar-yuzde-20-artis-siber-zorbaligi-patlatti-6609404
29. Nations Unies, Droits de l'Homme, Haut-Commissariat, « Le retrait de la Türkiye de la Convention d'Istanbul préoccupe particulièrement les membres du Comité pour l'élimination de la discrimination à l'égard des femmes », 15 juin 2022, disponible à l'adresse : https://www.ohchr.org/fr/press-releases/2022/06/experts-committee-elimination-discrimination-against-women-commend-turkiye
30. NTV.com.tr, « Pandemi döneminde kadına dijital şiddet de arttı », 27.07.2020, disponible à l'adresse : https://www.ntv.com.tr/kadina-siddet/pandemi-doneminde-kadina-dijital-siddet-de-artti,0ecEWbew-0eDWem_R4kvVw
31. Ouest-France, « Un lycéen poursuivi pour "bifflage" », 29.11.2012, disponible à l'adresse : http://www.ouest-france.fr/2012/11/30/pays-de-loir/Un-lycéen-poursuivi-pour-bifflage
32. Potinss : https://twitter.com/search?src=hash&q=%23potinss
33. Şener G. *et al.*, *Cinsiyetçi dijital Şiddetle Mücadele Rehberi*, Décembre 2019, disponible à l'adresse : https://www.stgm.org.tr/sites/default/files/2020-09/cinsiyetci-dijital-siddetle-mucadele-rehberi.pdf
34. *Siber Polis Nasıl Olunur ? Siber Polis Nedir ?*, : disponible à l'adresse : https://polisalimi.net/siber-polis-nasil-olunur-siber-polis-nedir/)
35. TDK, *« Zorba » : « Gücüne güvenerek hükmü altında bulunanlara söz hakkı ve davranış özgürlüğü tanımayan (kimse) (…) »* (consulté le 9 Avril 2022), disponible à l'adresse suivante : https://sozluk.gov.tr/
36. Ülkütekin D., « Potinss alarmı... Yakışıklı bulduğunuz erkekler var mı? », *Cumhuriyet*, 14.03.17, disponible à l'adresse : https://www.cumhuriyet.com.tr/haber/potinss-alarmi-yakisikli-bulduginuz-erkekler-var-mi-698821
37. *Yeni Şafak*, 22.03.19, « Yaşlılar da siber zorbalık mağduru », disponible à l'adresse : https://www.yenisafak.com/teknoloji/yaslilar-da-siber-zorbalik-magduru-3452673
38. Yetim S., « Siber Zorbalık, Türkiye ve ABD Karşılaştırması (ABD V. Drew Dosyası) », *TBB Dergisi*, nº 120, 2015, [en ligne], disponible à l'adresse : http://tbbdergisi.barobirlik.org.tr/m2015-120-1516. Mayıs 2017.

doi: 10.14664/rcvs/244

L'intelligence criminale nel contrasto alla cybercriminalità: l'esempio francese della gendarmeria nazionale

Le renseignement criminel au service de la lutte contre la cybercriminalité : l'exemple français de la gendarmerie nationale

Criminal intelligence in the fight against cybercrime: the French example of the national gendarmerie

*Jérôme Barlatier**

Riassunto
Questo articolo propone un'analisi sintetica della cybercriminalità a partire dallo stato della minaccia cibernetica realizzato dalla gendarmeria nazionale. La portata di questa forma di delinquenza è oggi tale che l'azione degli investigatori e dei magistrati, caso per caso, in una logica procedurale di individualizzazione, non può, da sola, avere ragione di un fenomeno così esteso. Recentemente riformulata secondo la prospettiva dell'*intelligence-led policing* (ILP), l'*intelligence* criminale propone un nuovo approccio alla delinquenza, proattivo, orientato a una comprensione preliminare delle situazioni al fine di proporre soluzioni adeguate, diversificate e innovative. L'ecosistema digitale si presta particolarmente ai metodi di analisi e alle strategie proposte da tale approccio. L'individuazione e la comprensione delle minacce sono facilitate dalla cyber *threat intelligence* (CTI) e le soluzioni adottate dalle forze di sicurezza interna non si limitano più alla sola repressione penale, ma si avvalgono di dispositivi sempre più sofisticati.

Résumé
Cet article propose une analyse synthétique de la cybercriminalité au travers de l'état de la menace cyber réalisé par la gendarmerie nationale. L'ampleur de cette forme de délinquance est aujourd'hui telle que l'action des enquêteurs et des magistrats, au cas-par-cas, dans une logique procédurale d'individualisation, ne saurait, à elle seule, avoir raison d'un phénomène aussi massif. Récemment reformulé sous l'angle de l'*intelligence-led policing* (ILP), le renseignement criminel propose une nouvelle approche de la délinquance, proactive, orientée sur une compréhension préalable des situations afin de proposer des solutions adaptées, diversifiées et innovantes. L'écosystème cyber se prête particulièrement aux méthodes d'analyse et aux stratégies proposées par le renseignement criminel. La détection et la compréhension des menaces y sont autorisées par *la cyber threat intelligence* (CTI) et les solutions d'entrave pour les forces de sécurité intérieures ne se limitent plus à la répression pénale, mais font appel à des dispositifs toujours plus sophistiqués.

Abstract
This article carries out a synthetic analysis of cybercrime perceived in France through the state of the cyber threat carried out by the gendarmerie nationale. This form of criminality has today such a magnitude that the action of investigators and magistrates, on a case-by-case basis, in a procedural logic of individualization, cannot, on its own, overcome such a massive phenomenon. Recently reformulated from the perspective of intelligence-led policing (ILP), criminal intelligence offers a new approach to delinquency which is proactive and oriented on a prior understanding of the situations in order to propose some adapted, diversified and innovative solutions. The cyber ecosystem lends itself particularly well to the analytical methods and strategies proposed by criminal intelligence. The detection and understanding of threats are authorized by cyber threat intelligence (CTI) and the solutions for the law enforcement forces are no longer limited to criminal repression, but call on elaborate devices with increasing sophistication.

Key words: Internet, cybercriminalité, investigation, *intelligence*, gendarmerie

* Docteur en Criminologie. Chef de la division du renseignement, Service central de renseignement criminel de la Gendarmerie nationale.

1. Introduction

« La révolution de l'An 2000 sera celle de l'information pour tous ». C'est ainsi que débutait le peu clairvoyant rapport de Gérard Théry en 1994 au sujet de ce l'on nommait encore les « autoroutes de l'information » (Théry, 1994).

L'évolution et l'accélération des technologies est telle qu'il est difficile d'imaginer qu'il y a vingt ans à peine l'informatique en réseau et la téléphonie mobile n'en étaient qu'aux balbutiements. Les atteintes aux systèmes de traitement automatisés de données représentaient alors des actes isolés et à portée limitée, réprimés en vertu de la loi Godfrain n° 88-19 du 5 janvier 1988 relative à la fraude informatique.

La prise de conscience des bouleversements induits par la création de l'internet (Wall, 2007) a pour autant été très tôt anticipé par les États Occidentaux. Dans l'enceinte du Conseil de l'Europe, la convention de Budapest sur la cybercriminalité du 23 novembre 2001[1] envisageait une adaptation du droit pénal de fond et de la procédure. Ce texte témoignait d'une conscience et d'une prise en compte rapide des enjeux de délinquance liés à ce nouvel espace. La nécessité de maîtriser la vélocité de l'information et de pouvoir accéder aux traces numériques quels que soient leur lieu de stockage était bien perçue. Certains mésusages de l'internet comme support ou comme vecteur de délinquance étaient déjà identifiés.

Le scénario était écrit, le décor était planté, il ne restait plus qu'aux acteurs de jouer. Moins de deux décennies ont été suffisantes pour ériger la cybercriminalité en la menace criminelle majeure, alors que quarante ans ont été nécessaires au trafic de stupéfiants pour arriver à maturité[2].

Illustrant le lien étroit existant entre la criminalité et les activités humaines, l'essor sans précédent des technologies de communication a corrélé l'évolution des phénomènes cyberdélinquants avec notre addiction aux échanges virtuels. Le netaholisme de nos sociétés et de nos économies rend bien plus difficile la régulation des activités délinquantes, car elles ne se juxtaposent plus seulement aux activités légales. Elles les débordent et s'hybrident, leur volume et leur nature les rendant plus difficiles à identifier, à caractériser et à éradiquer. Elles nécessitent d'envisager des changement de paradigme pour appréhender les évolutions de cette délinquance (Linde, Aebi, 2020).

L'évolution radicale de ce contexte criminologique implique de repenser les modes de régulation qui s'y appliquent. La cybercriminalité est nouvelle et complexe. Elle invite à une démarche où la compréhension précède l'action, remettant en cause le caractère traditionnellement réactif de la répression de la délinquances. Il convient ainsi de s'interroger sur les apports du renseignement criminel, dans une approche issue des théorie de l'*intelligence-led policing* (ILP).

Issu d'une préoccupation ancienne, mais fruit d'une méthodologie nouvelle, le projet d'une police guidée par le renseignement peut être le support d'une réponse composite à la cybercriminalité dans une approche à la fois holistique et casuistique, préventive et répressive, publique et privée. L'ILP ambitionne une compréhension des phénomènes criminels recourant à Internet comme objet ou comme vecteur de délinquance. Elle est parallèlement animée par le souci de trouver des solutions concrètes et actionnables. Par la mise en

[1] Convention on Cybercrime (ETS No. 185), disponible en ligne (consultation le 10 novembre 2022) : https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[2] De la *french connection* au néo-banditisme ; voir, par exemple, l'évolution chez le même auteur : Lalam 2002 et 2017).

cohérence de l'intervention des acteurs publics et privés, une coordination est possible pour mettre en œuvre des techniques d'entrave diversifiées, destinées à apporter une solution stratégique ou opérationnelle à la cybercriminalité.

Au niveau stratégique, le renseignement criminel permet de disposer des éléments d'évaluation et de modélisation des phénomènes, des espaces et des groupes cybercriminels. Cette approche est indispensable pour envisager des moyens de remédiation déjà existants ou susceptibles d'être expérimentés dans une logique *What works ? What doesn't ? What's promising ?*

Au niveau opérationnel, il permet d'envisager des entraves préventives et répressives adaptées à chaque phénomène. Il cherche à cibler les cyber-groupes criminels, tels que les groupes APT, et conçoit des modalités de neutralisation spécifiques à chacun d'entre-eux.

Cette approche proactive constitue, à maints égards, un changement de paradigme en matière de lutte contre la délinquance. Il ne s'agit plus de penser en termes de répression et d'interdit pénal, mais en termes de gestion du risque et de menace. L'enquête n'est plus seulement une source de vérité judiciaire, mais un capteur de savoir au service du renseignement. La plainte formelle de la victime n'est plus le moteur de l'action publique : enrichit, synthétisé et analysé, un simple signalement permet de contribuer à la détection et à la caractérisation des phénomènes, préalables à la définition d'actions de remédiations pertinentes.

Coordonnant les administrations avec le secteur privé et le monde académique, cette approche par le renseignement est susceptible de permettre la compréhension d'un environnement complexe, d'anticiper l'évolution rapide des technologies et de proposer des solutions aussi diversifiées qu'adaptées. En ce sens, les forces de l'ordre se rappellent qu'il est nécessaire de savoir avant d'agir.

Le présent article est nourri par la double expérience de son auteur, praticien au sein des forces de l'ordre spécialisé dans l'exercice de la mission de police judiciaire, et chercheur, auteurs d'une thèse de doctorat interrogeant la performance des processus d'enquête (Barlatier, 2017). Ses constats sont ainsi autant d'ordre académiques qu'opérationnels. Réalisant dans un premier temps un état de la menace de la cybercriminalité (2), il envisage ensuite les conditions de sa régulation et les potentialités offertes par le renseignement criminel (3).

2. État de la menace

La cybercriminalité est souvent abordée de façon autonome par les spécialistes du numérique dans une approche technique et autocentrée qui ne permet pas de rendre compte fidèlement de sa nature. Afin de l'aborder dans ses réalités, il convient de la situer dans l'écosystème plus général de la délinquance.

La question des escroqueries dites « en ligne », par exemple, est souvent envisagée comme une catégorie à part-entière. L'analyse de ce phénomène démontre pourtant une réalité bien plus complexe que ce libellé ne le laisserait présumer : les trois quart des escroqueries intègrent aujourd'hui une composante numérique au sein de leur mode opératoire, que ce soit au niveau de la phase de contact de la victime, de celle de sa manipulation, ou de celle de son paiement[3]. Désormais, distinguer les infractions de l'univers physique et du monde

[3] D'après les analyse du service central de renseignement criminel de la gendarmerie nationale (SCRCGN), à partir d'un suivi permanent de la donnée sur l'ensemble des agrégats de la délinquance en zone de compétence gendarmerie (représentant 95% du territoire national et 52% de la population française).

virtuel constitue une opposition trompeuse. Le numérique se mêle à la vie de chaque citoyen. Il s'intègre à tous les degrés des activités humaines. La délinquance n'y fait pas exception. Son impact en est d'autant plus important.

Augmentant, depuis plus d'une décennie, de 20 points par an[4], la croissance exponentielle de la cybercriminalité est corrélative au développement des accès à l'internet et de l'économie numérique. Plusieurs études considèrent que les atteintes par le vecteur numérique dépassent désormais le volume des infractions constatées dans le monde physique (Europol, 2015 ; Loveday, 2018). Cette estimation est d'autant plus significative que la délinquance recourant au vecteur numérique s'est faite plus discrète pour les systèmes judiciaires. La propension des victimes à rapporter les infractions et celle des institutions à les révéler semble s'être émoussée au regard de la part importante des infractions à faible préjudice, de la technicité de ce contentieux, du faible espoir en termes d'élucidation et de répression, et de l'existence d'autres formes de compensation du préjudice (e.g., indemnisation) (Ghernaouti-Hélie, 2009, p. 59-62). Ainsi, en 2016 la gendarmerie et la police nationales françaises recensaient-elles moins de 10.000 plaintes de fraudes à la cartes bancaires pour plus de 1,9 millions de faits identifiés par les banques et le e-commerçants[5]. S'il mérite d'être adapté à la réalité de chaque phénomène, ce rapport d'une plainte pour 200 faits réellement commis est confirmé par une étude de la gendarmerie nationale évaluant le taux de plainte en matière de rançongiciels à un pour 257 faits commis (Dregoir, Klein, 2017). D'autres études affirment, en revanche, que le taux de reportabilité des infractions numériques serait de 20% environ (Margagliotti *et al.*, 2019 ; Kemp, 2020).

Le vecteur numérique semble ainsi avoir déplacé les opportunités criminelles (Koops, 2011). Il permet, en effet, d'accéder de façon massive à l'intimité des victimes, tout en restant à bonne distance au moyen de garanties d'anonymat, et donc d'impunité. La transmission des modes opératoires est facilitée par la logique de réseaux autorisant la création d'équipes animées par une communauté d'intérêt mais composées de membres se connaissant rarement (Leukfeldt, 2015). Souvent fondés sur la démultiplication de petits préjudices, les bénéfices criminels sont considérables et peu traçables.

Les rapports d'analyse de la gendarmerie nationale identifient le vecteur numérique comme la menace criminelle la plus importante sur les trois axes d'évaluation que sont les phénomènes (2.1), les groupes (2.2) et la géographie (2.3) criminels.

2.1. Les phénomènes cybercriminels

Internet a bouleversé la vie des populations et le fonctionnement de l'économie. Il constitue une rupture technologique décisive plaçant l'information au centre des valeurs. Au terme de vingt ans d'observation, il est possible d'affirmer que ces changements radicaux ont eu un effet considérable sur la délinquance.

Le Web est à la fois le vecteur et l'objet de la délinquance (Wall, 2007, p. 44 et s.) :

- le vecteur car, comme l'apparition de l'automobile en son temps a permis d'agir plus vite et plus loin, internet procure une surface d'attaque plus importante pour la commission d'infraction traditionnelles ;
- l'objet, car internet est composé d'acteurs et

[4] Source : SCRCGN.

[5] Analyse réalisée en 2016 par la SCRCGN lors de la mise en place de la plate-forme PERCEVAL de signalement des escroqueries en ligne à la carte bancaire. Source issues des données opérationnelles de la gendarmerie nationale et de ses partenaires dans le secteur bancaire et du e-commerce.

d'infrastructures eux-mêmes touchés par des infractions de nouvelle nature propres à cet écosystème si particulier.

Les nouvelles technologies de l'information et de la communication représentent donc tout à la fois la transposition d'une délinquance préexistante, l'amplification de celle-ci, et la création de nouvelles formes de criminalité qui n'existaient pas auparavant.

En France, la gendarmerie nationale positionne la cybercriminalité en tête de ses priorités opérationnelles. Son état de la menace cherche à comprendre son organisation, ses modes opératoires, ses dynamiques, ses motivations et son modèle économique. Un bref aperçu des principaux phénomènes peut être réalisé[6].

Intrusions dans un système informatique dans le but de vol, d'altération ou de piratage d'informations, les atteintes au système de traitement automatisé de données (ASTAD)[7] représentent un dixième des infractions constatées par les unités de la gendarmerie dans le cyberespace. Ce chiffre est cependant largement sous-estimé au regard de la faible reportabilité de ces délits auprès des forces de l'ordre, les volumes constatés par d'autres sources (observateurs privés ou publics, tels que le GIP ACYMA) étant bien plus importants[8].

Les rançongiciels (*ransomware*) sont la transposition de l'extorsion de fond traditionnelle par la prise en otage des données informatiques au préjudice des entreprises, mais aussi des personnes publiques et, désormais, des particuliers. Ne se limitant pas à bloquer le système informatique par le chiffrement des données, ce mode opératoire s'accompagne généralement du vol et du remploi des données de la victime, le *business plan* des malfaiteurs cherchant à rentabiliser l'acte par diverses sources de profit. Les procédés d'incitation au paiement sont radicaux et perfectionnés. Cumulant les frais de la rançon, les coûts d'exploitation et l'atteinte à la réputation, le préjudice est considérable et représente souvent un enjeu de survie pour une entreprise, voire une filière économique.

Destinées à neutraliser la disponibilité d'un système informatique, des communications ou d'un site internet par la saturation de ses capacités techniques, les attaques par déni de service (*Denial of Service Attack* - DOS) sont également très couteuses et reposent sur des infrastructures de délinquance évoluées.

D'autres manières d'opérer consistent à mettre à profit les failles informatiques, tel que le *swatting* (fausses alertes aux forces de l'ordre), le *jackpotting* (attaque informatique sur un distributeur automatisé de billet afin d'en retirer l'argent), le *mouse-jacking* (vol électronique de véhicules) ou les actions

[6] Tous les deux ans, la gendarmerie nationale française publie un rapport d'analyse relatif à la criminalité organisée (RACO) procédant à un état de la menace des tendances de la délinquance. Cette analyse constitue une aide à la décision au profit de son commandement et de ses partenaires.
Par ailleurs, un rapport d'analyse des cybermenaces a été publié cette année afin d'approfondir les constats du RACO dans le domaine plus spécifique des atteintes aux systèmes automatisés de données (ASTAD).
Ces rapports sont classifiés et accessibles qu'au regard du droit et du besoin d'en connaître. Toutefois, les éléments pouvant être communiqués au public sont évoqués dans cet article.

[7] Ces infractions sont prévues aux articles 321-1 à 321-8 du code pénal :
- accès, maintient frauduleux ayant, le cas échéant, entrainé la suppression ou la modification des données d'un STAD (art. 321-1 CP) ;
- entrave ou altération du fonctionnement d'un STAD (art. 321-2 CP) ;
- introduction frauduleuse de données dans un STAD, ou extraction, détention, reproduction, transmission, suppression, modification frauduleuse de données (art. 321-3 CP) ;
- détention, offre ou cession d'équipements, instrument, ou programme informatique destiné à commettre les infractions précitées (art. 323-3-1 CP) ;
- participation à un groupement en vue de la commission des infractions précitées (art. 323-4 CP).

[8] Pour le dernier rapport du GIP ACYMA : https://www.cybermalveillance.gouv.fr/medias/2022/03/cybermalveillance-rapport-activite-2021.pdf (consulté le 4 décembre 2022).

malveillantes sur la domotique (serrures électroniques, brouilleurs d'alarmes, *etc.*).

Si ces attaques techniques représentent des préjudices considérables, les trois quarts de la cybercriminalité constatée par les plaintes déposées auprès des unités de la gendarmerie nationale concernent néanmoins les escroqueries[9]. Celles-ci sont particulièrement hétérogènes au niveau de leur modes opératoires, de leur victimologie et de leur préjudice.

Une part importante d'entre-elles concernent les fraudes à la vente et à la livraison d'objets en ligne par des individus à faible capacité criminelle[10] profitant de l'anonymat et des opportunités offertes par la toile.

Les escroqueries dites « à la nigériane » commises par des populations situées en Afrique de l'Ouest représentent une forme plus structurée de délinquance. Commises depuis l'étranger, elles constituent un phénomène socio-économique où des populations pauvres ont une opportunité de gagner facilement de l'argent et contactant *via* internet des populations de pays plus riches. La communauté linguistique avec leur victime et la maîtrise d'un mode opératoire appris et perfectionné sur le tas sont les conditionnants de la réussite des escrocs. La typologie de modes d'action est particulièrement diversifiée, souvent standardisée, parfois innovante : lettre de Jérusalem (dites « *scam* 419 » consistant à solliciter de l'aide par message), fraudes aux sentiments, sextorsions, *pornscam*, fausses locations, fausses annonces, fausses offres d'emploi en ligne, *et cetera*. Ces escroqueries sont d'un faible préjudice économique, mais représentent un bénéfice cumulé important. Elles créent un sentiment d'insécurité chez des internautes vis-à-vis des services proposés sur la toile.

D'autres escroqueries à fort préjudice économique sont commises depuis la France et l'étranger selon des modes d'action bien plus perfectionnés. Qu'il s'agisse de faux ordre de virements internationaux (FOVI), de fausses commandes, de faux investissements, cette criminalité entrepreneuriale repose sur des processus et des modèles économiques planifiés et perfectionnés où le ciblage se fonde sur une collecte préalable des données (*leads*) et un démarchage actif (*via* des *call centers*), prolongé par une phase de manipulation (*social engineering*) et des opérations financières élaborées visant à brouiller les pistes et à blanchir les fonds indûment versés. Commises au préjudice des entreprises ou des particuliers, ces fraudes trouvent également des débouchés en matière de détournement des fonds publics comme cela a pu être observé lors de la captation frauduleuse des aides d'État durant la crise sanitaire (*i.e.*, chômage partiel, prêts garantis par l'État)[11], le détournement

[9] Sont considérées comme des escroqueries numériques l'ensemble des infractions dont au moins un des éléments du mode opératoire est perpétré dans le cyber-espace : identification de la victime (*via* les fuites de données, par exemple), prise de contact (*mail* frauduleux, *spam*, *etc.*), manipulations frauduleuses (procédés de tromperie, recours à des moyens d'anonymisation autorisés par le Web, par exemple) ou versement des sommes indues (virement en ligne ou utilisation de crypto-actifs, par exemple).

[10] La capacité criminelle s'entend du potentiel d'un individu à commettre des infractions d'une certaine gravité, au regard des prédispositions matérielles et psychologiques que celle-ci nécessitent de surmonter. Réaliser des détournements d'argent par ruse en l'absence d'une victime anonyme, par exemple, demande une moindre capacité criminelle que le vol avec violences physiques sur une personne vulnérable.

[11] Cette question a fait l'objet de nombreux écrits de la part des institutions internationales et nationales :

- Interpol : https://www.interpol.int/fr/Infractions/Cybercriminalite/Cybermenaces-liees-au-COVID-19 (consulté le 4 décembre 2022) ;
- Europol : https://www.europol.europa.eu/operations-services-and-innovation/staying-safe-during-covid-19-what-you-need-to-know (consulté le 4 décembre 2022) ;
- Institut des hautes études du ministère de l'intérieur (IHEMI) : https://www.ihemi.fr/articles/evolution-du-crime-et-du-cybercrime-durant-la-pandemie-de-coronavirus (consulté le 4 décembre 2022) ;
- Agence nationale de sécurité des systèmes d'information (ANSSI) : https://www.ssi.gouv.fr/actualite/lanssi-et-le-

du dispositif d'aide à la rénovation énergétique ou de comptes personnels de formation. Cette délinquance témoigne de l'articulation subtile d'actions dans le monde physique et numérique jouant sur l'ignorance ou la crédulités de certains acteurs combinée avec les vulnérabilités et les faiblesse juridiques ou économiques des entreprises et des administrations.

Cette hybridation du physique et du numérique est également bien présente dans les opportunités de trafics offertes à une vaste communauté d'internautes (Ablon *et al.*, 2014) : drogues, médicaments, tabac, armes, documents, données à caractère personnel, moyens de paiement, pièces détachées de véhicules, produits de contrefaçons ou de contrebande, *et cetera*. Ces denrées illicites sont déployées sur un marché libéralisé et anonyme, où l'offre est mise en lien avec la demande sans qu'une régulation spécifique ne soit opérée. Au-delà des échanges de biens illicites, internet facilite également les mouvements de capitaux, chacun se trouvant à un clic de sa banque ou d'un intermédiaire de transfert de fond. L'escroc n'a plus à recevoir le paiement des mains de la victime, les opérations de blanchiment n'emportent plus nécessairement le transport de valises de billets, les mouvements d'argent pouvant se réaliser de façon dispersés par des intermédiaires humains (*money mules*) ou techniques (crypto-actifs, *Non Fungible Token* - NFT) destinés à brouiller les pistes.

Internet crée donc un contexte favorable aux atteintes aux biens. Elle n'empêche pas davantage les atteintes aux personnes, en fournissant un cadre permettant de générer des contenus qui répondent à la curiosité, à la malveillance ou aux pulsions d'un large public d'anonymes (violences, exploitation et contrainte dans la production de contenus pornographiques, *etc.*) (pour une approche de l'influence des facteurs humains, auteur et victime, en termes de cybercriminalité : Leukfeldt, Holt, 2021). Parfois, l'être humain est considéré comme une marchandise dont la commercialisation est amplifiée par les réseaux en contrepartie d'importants profits (proxénétisme, trafic de migrants, atteintes sexuelles sur mineurs en ligne) (Yu, 2014). Brisant les barrières entre la proximité physique et la distance numérique, les réseaux sociaux se sont montrés propices aux violences morales (insultes, menaces, harcèlement), à la désinformation (délits de presse, *fake news*), aux atteintes à la réputation et à la vie privée (diffamation, atteinte au secret des correspondances, *sexting*, *revenge porn*)[12]. Si internet efface les distances, il restaure aussi parfois la proximité. Il existe, à ce titre, une « cyberdélinquance de proximité », où l'auteur agresse anonymement sa victime sur Internet alors même qu'il se situe dans son entourage proche (cyberharcèlement, pédopornographie).

Ces phénomènes accompagnent l'accroissement exponentiel des activités humaines et des enjeux économiques, politiques et sociaux de l'internet. Si la technicité de cet écosystème a impliqué une spécialisation de certains acteurs, la plupart de ces modes opératoires est réalisée par le report de la délinquance traditionnelle vers le *Web*.

2.2 Les acteurs de la cybercriminalité

Ensemble peu homogène, la cybercriminalité relève

bsi-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemagne-dans-le-contexte-de-la-crise-sanitaire/ (consulté le 4 décembre 2022).

[12] A cet effet, le service central de renseignement criminel (SCRC) de la gendarmerie participe à la mise en oeuvre d'un projet de recherche cherchant à comprendre et à entraver le cyberharcèlement (Dulaurans, Fedherbes, 2022). Dénommé CyberNe Tic, ce projet a mis en ligne un site internet destiné à informer le public sur ce phénomène : https://cyberneticproject.eu/projet (consulté le 4 décembre 2022).

d'un biotope d'acteurs diversifiés. A l'évidence, ce sont les groupes cybercriminels organisés qui ont le plus fort impact au regard de leurs actions directes ou indirectes (*i.e.* mise à disposition de services). Leur suivi le plus complet relève paradoxalement non des forces de sécurité intérieures, mais des démarches de renseignement du secteur privée, dénommées *cyber threats intelligence* (CTI). Une typologie générale de ces groupes établie par la gendarmerie nationale française distingue :

- les groupes appartenant à un État et œuvrant en lien avec les services de renseignement de celui-ci afin de mener des cyber-attaques dans un intérêt géopolitique (atteintes aux institutions et à l'économie, désinformation et déstabilisation ayant pour but d'atteindre le moral des populations ou d'influencer un scrutin électoral, *etc.*) ;
- les groupes soutenus ou tolérés par un État, ayant une part d'activités servant les intérêts de celui-ci et une part d'activités autonomes ;
- les groupes indépendants et structurés, à finalité uniquement criminelle et orientés sur le profit ou le pouvoir ;
- les groupes d'activistes en ligne (*hacktivistes*), orientés sur la défense d'une cause politique ;
- les groupes cyber-terroristes, utilisant internet comme vecteur de leur cause (apologie, recrutement, renseignement, communication, attaques informatiques, *etc.*) ;
- les réseaux criminels informels et peu structurés, constitués de membres ne se connaissant pas nécessairement, mais unis par la convergence de leurs actions (trafics de produits illicites, *money mules*, pédopornographie, *etc.*).

Les trois premières catégories sont souvent appelées « groupes APT » (par dérivation de la désignation de leurs attaques discrètes et planifiées, dites « *advanced persistant threats* ») et fait l'objet d'une nomenclature précise[13] permettant leur suivi dans la durée et la réalisation d'attribution en cas de cyber-attaques. Ainsi, le groupe russophone APT 28 (« *Fancy bear* ») est supposément lié aux services de renseignements russes et serait actif depuis 2004, orienté sur le cyber espionnage, la désinformation et la déstabilisation à l'encontre des pays de l'OTAN, des structures sportives internationales et de l'Ukraine. Le groupe russophone REvil est un groupe cybercriminel actif depuis 2019, probablement en reconversion de l'ancien groupe dissout GrandCrab, il utilise et propose en RaaS l'un des rançongiciels les plus utilisés : REvil/Sodinokibi. L'importance de ses actions (dont l'attaque de l'entreprise *colonial pipeline* en 2021) a incité les autorités américaines à avertir fermement leurs homologues russes, ce qui a eu pour effet d'entraîner la suspension des activités de ce groupe. A cet effet, la succession des groupes est courante et impose la réalisation de généalogies : le groupe Egregor a ainsi succédé au groupe Maze, soit par transfert des acteurs, soit par reprise des outils[14]. Paradoxalement, la géographie est fortement conditionnant de l'action de ces groupes dans le choix des cibles (*e.g.*, certains rançongiciels ne fonctionnement pas sur des systèmes d'exploitation en cyrilliques ou dans des langues de pays amis de la Russie) et dans la coopération entre malfaiteurs (la communauté linguistique est un fort conditionnant dans l'association entre développeurs, opérateurs, voire affiliés).

[13] Voir, par exemple, *e.g.,* https://attack.mitre.org/groups/ (consulté le 4 décembre 2022).
[14] *e.g.*, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-012.pdf (consulté le 4 décembre 2022).

Agissant à grande échelle pour la commission de faits susceptibles de déstabiliser une économie ou des organisations, ces groupes cybercriminels sont bien structurés et disposent d'une aptitude à la coopération avec des entités tierces. Ils recourent à des modes d'action sophistiqués et à une forte capacité d'innovation. Leurs revenus sont particulièrement importants et leur donnent une capacité d'investissement susceptible de permettre le développement de leur activité. Le perfectionnement des *modus operandi* impose cependant une spécialisation progressive des acteurs sur le modèle de division du travail existant dans l'économie légale : développeurs, fournisseurs de solutions d'attaque (*initial access broker, loaders, services de test,* vendeurs de kits *webinject* ou de kits de hameçonnage, courtiers en données ou en informations), testeurs (test d'antivirus ou de la validité de données), fournisseurs de service (services criminels en ligne, ou CaaS), pourvoyeurs de solutions d'anonymisation (hébergement *bulletproof*, VPN, *proxy*), vendeurs de matériel physique nécessaire à la commission d'infractions (*skimmers*, dispositifs de détection de réseau, *etc.*), distributeurs (envois de *spams* sur les réseaux sociaux ou par *mail*, mise à disposition de sites piratés), groupes spécialisés dans la mise en oeuvre de certaines attaques (rançongiciels, DDOS), recruteurs (infiltration d'entreprises ou corruption de salariés), groupes utilisant les outils développés par les groupes cybercriminels (affiliés), intermédiaires de paiement (mules, blanchisseurs, mixeurs de cryptomonnaies), *et cetera* (Broadhurst *et al.*, 2014).

Au-delà de ces groupes structurés et disposant de capacités techniques particulières, la cybercriminalité concerne une grande diversité de profils délinquants, d'une criminalité entrepreneuriale (récupération de *leads*, contact avec les victimes par des *call centers* situés à l'étranger, paiements en ligne), à une criminalité sociale (*brouteurs*, *sakawas*, *yahooboys* ou *feymens* procédant par imitation dans les cybercafés d'Afrique de l'Ouest), de pirates informatiques (*hackers*, *script kiddies*) à des individus isolés ou œuvrant en réseau (accès gratuit aux bouquets numériques, téléchargement illégal, promoteurs de haine, producteurs ou collecteurs de contenus pédophiles). Bien moins compétente techniquement, cette catégorie de cyber-malfaiteurs bénéficie de la démocratisation et de la standardisation des outils et des modes opératoires mis en ligne dans le cadre du *crime-as-a-service* (CaaS).

2.3 La géographie et les cybermenaces

Les aspects géo-criminels des cybermenaces comportent plusieurs dimensions. Internet n'est pas seulement un espace dématérialisé. Ses modélisations (modèle OSI en 7 couches, ou modèle TCP/IP en 4 couches) rappellent que des infrastructures physiques et techniques particulièrement lourdes sont nécessaires pour permettre à l'internaute de pénétrer dans un univers d'apparence virtuelle. Le modèle le plus communément utilisé distingue la couche physique (système informatique et réseaux matériels et électromagnétiques), de la couche logique (logiciels permettant de fournir les services attendus), , de la couche applicative (interface démocratisant l'utilisation du Web) et de la couche sémantique (contenu du Web autorisant les interactions sociales) (Douzet, 2014). Entre *data center* et câbles sous-marins, il convient donc de garder à l'esprit les nombreuses vulnérabilités physiques de l'internet, quand bien même l'infrastructure répartie du réseau lui assure une certaine résilience.

La topographie d'internet impose aux individus de

se réorienter dans un écosystème dont les paramètres sont totalement différents du monde physique. Cet univers est, par ailleurs, en rapide mutation et a connu d'importants changements depuis vingt ans entre l'internet des sites (le Web 1.0) mis en œuvre par des acteurs spécialisés, l'internet des réseaux sociaux (le Web 2.0) où chacun est en mesure d'apporter son contenu, et l'Internet des objets (parfois désigné comme Web 3.0) où l'interaction offerte par le numérique investit tous les objets du quotidien.

A cela s'ajoute la plus ou moins grande accessibilité de l'information entre un web référencé et immédiatement accessible, régi par la traçabilité des connexions et le référencement des contenus (*clearweb*), le web non référencé uniquement réservé aux abonnés d'un réseau ou d'un site (*deepweb*), et le web non référencé organisé autour de protocoles destinés à garantir l'anonymat des utilisateurs par le chiffrement et l'intermédiation (*darkweb*) (Rudesill *et al.*, 2015).

Au sein de cette géographie, les acteurs (internautes, fournisseurs d'accès, gestionnaires de sites, *registrar* procurant les noms de domaine et hébergeurs fournissant les capacités de stockage) ont des positionnements et des rôles différents. Ils détiennent chacun une partie des traces nécessaires à l'identification des usagers du réseau.

Cette trop brève description de la géographie de l'internet souligne à quel point le cyberespace fournit des points de repère bien différents qui bouleversent les opportunités criminelles.

Du point de vue criminologique, le cyberespace constitue à maints égard une infrastructure favorable à la délinquance. Il met à disposition des contre-mesures particulièrement nombreuses qui permettent de compliquer l'exploitation des traces par les forces de sécurité intérieure et de favoriser l'anonymat : communications directes (*peer to peer* - P2P), intermédiées (*virtual personnal Network* - VPN, hébergeurs non coopératifs - *Bulletproof hosting*), parcellisées (*Botnet*, mixeurs) ou brouillées (chiffrement, *darkphones*, tels que *Encrochat* et *Sky ECC* ; *darknet*, tels que TOR ou I2P). L'affaiblissement et la mobilité des identités ainsi que les possibilités d'usurpation (pseudos, *dataleaks*, *typosquatting*, *spoofing*) viennent renforcer ces difficultés d'identification. Parallèlement, Internet offre un accès inédit aux victimes par le piratage, la collecte et la valorisation des données des particuliers et des entreprises (fuites de données, ou *dataleaks*). La capacité à prévoir l'action des malfaiteurs est réduite dans un espace ou le mouvement et l'innovation sont la règle : adaptation rapide des modes opératoires existant aux niveaux technique, managérial ou du modèle économique ; identification et exploitation de vulnérabilités techniques (*e.g.*, failles de type *zéro Day*) et humaines (*i.e.,* manipulation par *social engineering*) ; mise à profit de l'évolution technologique (Internet des objet, crypto-actifs, NFT, Métaverse, pour ne citer que ceux-ci).

Du point de vue criminalistique, le numérique renouvelle l'intérêt pour la trace et en transforme les paramètres de sa collecte et de son exploitation. Le principe de déperdition des preuves formulé par le criminaliste français Edmond Locard selon lequel « le temps qui passe, c'est la vérité qui s'enfuie » (Locard, 1934) pourrait être reformulé par « le temps qui passe, c'est la vérité qui persiste », voire même « le temps qui passe, c'est la vérité qui réapparaît ». Les traces laissées sur internet sont, en effet, d'une particulière résilience et présentent tout autant d'une valeur intrinsèque que d'une valeur collective quand la congruence des unes est mise en écho avec les autres. L'internet des objets (*Internet of*

Things - IoT) va accroître la disponibilité et la dispersion des traces, en lien avec le cadre de vie des populations et les habitudes des individus (multimédia, domotique, *smart cities*, véhicules connectés et gérés en flotte, *etc.*) (Bouchaud, 2021).

Du point de vue victimologique, internet bouleverse la façon dont se distribue la criminalité. Il modifie en cela la répartition géographique traditionnelle de la délinquance et la concentration de certains phénomènes dans les centres urbains, plus propices aux violences et aux activités de trafic. L'a-territorialité[15] du cyberespace fait évoluer les modèles de dispersion de la criminalité, les activités en ligne et les vulnérabilités informatiques semblant désormais constituer les variables essentielles. La répartition des infractions paraît ainsi guidée par un critère démographique, plus que géographique[16]. Ce constat est essentiel, car il permet d'envisager que certaines populations relativement épargnées par la délinquance de masse sont aujourd'hui rattrapées par celle-ci au regard des fenêtres numériques qui permettent d'accéder à leur intimité (smartphone, PC, *etc.*). Chaque classe d'âge est différemment exposée : cyberharcèlement et atteintes à la réputation pour les plus jeunes, escroqueries pour les classes d'âge intermédiaires, avec abus de faiblesse pour les plus âgés. La *summa divisio* entre les particuliers et les personnes morales est également pertinente, les typologies de délinquance étant relativement distinctes.

Au terme de cette brève analyse orientée sur les phénomènes, les auteurs et la géographie, la cybercriminalité apparaît comme un enjeu de sécurité essentiel. Son accroissement exponentiel et ses implications majeures en termes politique, économique et social implique de repenser la lutte contre cette menace prioritaire.

3. Réguler la cybercriminalité

Si la cybercriminalité a été anticipée par le législateur, une organisation et des mesures, les effets de ces dispositifs n'ont manifestement pas permis de limiter une forme de délinquance qui est devenue une menace majeure en 20 ans. Cela interroge l'efficacité des moyens de lutte traditionnels, fondés sur un schéma relativement classique consistant à normer (création d'un cadre juridique adapté au niveau national et international), à institutionnaliser (création d'unités et juridictions spécialisées destinées à prendre en charge un contentieux naissant), puis à démocratiser (recherche d'une décentralisation de compétences en vue de faire face à la croissance du contentieux). Cette approche des institutions publiques est essentiellement réactive. Elle ne cherche ni à comprendre, ni à entraver les causes même des phénomènes. Pour autant, aux côtés de cette action axée sur le traitement judiciaire, les acteurs de l'internet se sont souvent eux-mêmes organisés pour tenter de réguler les phénomènes selon des méthodes diversifiées (3.1). Accompagnant cette

[15] Terme évoqué lors d'un colloque au Conseil d'État organisé le 28 septembre 2016 : « L'a-territorialité du droit à l'ère numérique ».

[16] Les analyses du SCRCGN ont établi une typologie relative à la répartition spatiale des phénomènes criminels en fonction de la nature des opportunités criminelles :

- certains ont une répartition criminologique, en ce sens que les déplacement d'un délinquant ou d'une bande criminelle expliquent la localisation des infractions (*e.g.*, sur-représentation des vols avec violence en milieu urbain, vol de fret routier par des modes opératoires perfectionnés) ;
- d'autres ont une répartition géographique, car l'implantation des victimes conditionne la survenance des infractions (*e.g.*, atteintes aux entreprises ou à un secteur économique) ;
- d'autres phénomènes, enfin, ont une répartition démographique, car leur localisation est proportionnelle à l'implantation des populations sur un territoire (*e.g.*, homicides, violences intrafamiliales ou intrafamilières, mais aussi cybercriminalité dont la survenance n'est pas conditionnée par le lieu où se trouve la victime, mais par sa seule présence sur le Web et, parfois, par sa provenance linguistique).

Cette classification empirique est à mettre en lien avec la théorie des activités routinières (Cohen, Felson, 1979)

dynamique, les force de l'ordre ont tout intérêt à mettre en œuvre les principes d'une police guidée par le renseignement, fondée sur une meilleure compréhension de la délinquance (3.2) en vue d'une action plus efficiente (3.3).

3.1 Réprimer ou réguler ?

Le sociologue français Michel Crozier affirmait que, dans tout système, les acteurs investissent les zones indéfinies et utilisent cette incertitude à leur profit (Crozier, Friedberg, 1977). Internet est initialement conçu comme un espace d'échange et de liberté, une a-territorialité vierge et sans frontière qui a été investie diversement par les acteurs au niveau politique, économique, social et légal. Ses zones indéterminées sont particulièrement importantes et la régulation des acteurs privés a bien souvent pris le pas sur la normalisation des États. La tentative de la convention de Budapest de simplifier les échanges entre États afin de mieux prendre en compte un phénomène d'essence transnationale n'a pas produit les effets escomptés. Il est probable que le second protocole additionnel adopté en 2021 ne fasse pas grandement évoluer cette situation.

Orientés sur une logique traditionnelle d'interdit et de répression, les États recourent aux outils habituels offerts par leur arsenal répressif. Destinés à prouver le lien entre un fait infractionnel et son auteur sur la base de garanties procédurales fortes dans le but de répression d'un interdit pénal, ces outils ne sont pas forcément les instruments les plus adaptés pour lutter contre un phénomène massif et permanent. Au regard du faible taux d'élucidation et des difficultés à aborder au cas par cas une délinquance technique et massive, le volume des affaires judiciaires traitées avec succès est sans commune mesure avec l'ampleur du contentieux (Barlatier, 2020b). Elles débouchent sur des peines bien souvent assez peu dissuasives au regard des bénéfices que ces délits génèrent. Au demeurant, l'action judiciaire ne permet souvent qu'une neutralisation ponctuelle et superficielle, l'action policière se concentrant sur les maillons les plus visibles, mais aussi les plus interchangeables des réseaux, les donneurs d'ordre et les gestionnaires d'infrastructure de délinquance étant rarement inquiétés.

Ainsi, après les atteintes aux biens, la délinquance économique et financière et le trafic de stupéfiants, la cybercriminalité porte un nouveau soupçon sur la capacité du système pénal à représenter le seul, sinon le principal, sinon le plus légitime, moyen de lutte contre la délinquance (Barlatier, 2019 et 2020b).

Cette incapacité de soumettre l'internet au droit a très tôt été perçue par les acteurs publics et privés qui ont développé des dispositifs de régulation sectoriels pour instaurer des espaces de stabilité sur la toile.

Ces régulations sont, d'ailleurs, souvent devenues des enjeux de pouvoir et de profit. Le fonctionnement des GAFAM-T en est probablement le plus symbolique. Acteurs structurant du *Web*, ces multinationales sont incontournables et disposent d'une position dominante en termes d'infrastructures physiques et logicielles (Microsoft, Apple), de référencement (Google), de réseaux sociaux (Facebook, Twitter) ou de commerce (Amazon). Par la maîtrise de la donnée, ces acteurs bénéficient des attributs foucaldiens d'un savoir panoptique et d'un pouvoir sur le comportement de chacun au sein d'un espace de socialisation totalement tracé, auquel les individus sont devenus dépendants (Foucault, 1975). L'analyse des données permet tout à la fois la maîtrise du général (activité économique et des

populations) et du particulier (accès à la vie privée de chacun). Cumulant le tout et les parties dans une approche tout aussi holistique que casuistique, la puissance centralisatrice de ces multinationales privées est traditionnellement mise en lien avec le *soft power* américain que les autres puissances continentales tentent tardivement d'endiguer avec des mesures de protection (règlement général de protection des données - RGPD - au sein de l'Union européenne) ou de cloisonnement (création de barrières techniques isolant les internet russes et chinois). Révélatrice des équilibres géopolitiques, internet devrait être le témoin, dans les années à venir, du développement des BATX[17] et de la maîtrise la 5G qui accompagneront et faciliteront l'affirmation de la puissance politique et économique chinoise. La puissance de ces multinationales s'illustre particulièrement à l'égard du pouvoir traditionnel des États dans les enquêtes judiciaires conduites par les forces de sécurité intérieure. Généralement installées aux États-Unis, l'accès à leur données implique le processus lourd et complexe d'une demande d'entraide pénale internationale (DEPI). Toutefois, s'abstrayant du cloisonnement juridique des États, l'enquêteur peut tout aussi bien adresser directement sa demande auprès de l'opérateur privé dans le cadre d'une *legal request*. L'opérateur de l'internet examinera alors cette demande au regard de ses conditions générales d'utilisation (CGU) et acceptera de répondre aux enquêteurs si celles-ci sont enfreintes (*e.g.*, en cas de pédopornographie ou d'apologie du terrorisme). En l'espèce, le droit contractuel des opérateurs de l'internet s'avère d'une plus grande efficacité que les traités d'entraide judiciaire (*Mutual Legal Assistance Treaty* - MLAT).

[17] Acronyme désignant les quatre plus grandes entreprises technologiques chinoises : Baidu, Alibaba, Tencent et Xiaomi.

Au-delà de la régulation des géants de l'internet, la toile fait l'objet de nombreuses initiatives d'acteurs privés cherchant à renforcer leur sécurité dans un cyberespace qui est source de risques comme de profits pour les entreprises. La sécurité des systèmes d'information (SSI) est ainsi devenue un marché autonome et fortement structuré, sous une forme internalisé aux entreprises ou sous celle de prestations de services. Par exemple, la création de CERT (*Computer Emergency Response Team*) illustre la volonté de centraliser les données et d'analyser les cyber menaces afin d'y apporter des parades appropriées. En France, l'agence nationale de sécurité des systèmes d'information (ANSSI) est un organisme public venant unifier ces initiatives éparses en apportant une vision d'ensemble. Ces dix dernières années la *cyber threat intelligence* (CTI) s'est développée comme méthode de ces organisations. Cette discipline structure le recueil et l'analyse des informations sur les cyber menaces. L'intention est de comprendre la nature des atteintes, le profil des cibles et des attaquants. L'objectif est d'anticiper, de détecter ou de parer aux attaques informatiques. Ces méthodes s'inspirent fortement des principes du renseignement et se fondent sur le recueil de données multi-sources (*e.g.*, sources humaines, ouvertes ou techniques), la détection des signaux faibles (*Indicators of Compromissio*n - IOC), un traitement et une analyse débouchant sur des mesures de remédiation diversifiées du niveau tactique au niveau stratégique (Kuerbis *et al.*, 2022).

Il convient également de ne pas négliger les initiatives citoyennes sur la toile. Particulièrement diversifiées, elles tendent à recréer un contrôle social en informant sur les menaces (sur les sites et réseaux sociaux), en organisant une vigilance (lanceurs d'alerte, signalement de contenus illicites), en constituant une aide à la détection (*e.g.*, site

haveibeenpwned en matière de compromission d'identifiants) débouchant parfois sur une logique de milice (*e.g.*, action violente de certains traqueurs de pédophiles) (Hadjimatheou, 2019 ; Frampton, 2020). Dans ce même ordre d'idée, la viralité d'internet a favorisé le développement des fausses informations (*fake news*) que des initiatives de particuliers comme de professionnels, et notamment des entreprises de presse tentant de restaurer leur rôle, tentent de limiter par une démarche d'éclaircissement fondée sur une analyse critique (*debunking, hoaxbusting*) (Petratos, 2021).

Face à ces initiatives éparses et peu coordonnées, les administrations françaises se sont également organisées afin de répondre aux cyber menaces[18] par la création d'agences d'analyse et de remédiation, tels que l'ANSSI[19], destinée à la protection des organismes d'importance vitale (OIV), ou le GIP ACYMA[20], destiné aux particuliers et aux entreprises. Le système pénal s'est, quant à lui, articulé autour de compétences décentralisées (C-NTECH, ESI, NTECH[21], ICC[22]), d'unités d'enquête ou d'appui dédiées (EC3[23], C3N[24], OCLCTIC[25], BEFTI[26]) ou de juridictions spécialisées (*e.g.*, section J3 au tribunal judiciaire de Paris). Transposant son organisation territoriale à la problématique numérique, la gendarmerie nationale a, par ailleurs, créé en 2021 un commandement dans le cyberespace (ComCyberGend) et orienté la gestion de ses ressources humaines vers cette thématique (*e.g.*, création d'un recrutement destiné aux officiers scientifiques, intégration de compagnies de « cyber-gendarmes »). Ces services ne sont toutefois qu'une simple évocation de l'ensemble des administrations françaises impliquées dans la lutte contre les cyber menaces dans le cadre de la lutte contre la fraude (*e.g.*, CSCE[27]), du renseignement (*e.g.*, DGSI[28], DGSE[29], cyber douanes) ou de la défense nationale (COMCYBER[30]).

En vingt ans, les institutions publiques ont ainsi constamment évolué avec le droit pour lutter contre la cybercriminalité, tentant de répondre, souvent de façon réactive aux menaces avec des moyens techniques et des prérogatives juridiques adaptés. Sur la base de pouvoirs généraux ou de textes spécifiques, la procédure pénale s'est ainsi adaptée

[18] Pour une présentation et un organigramme des chaînes cyber (protection, défense, renseignement et judiciaire), disponible le site de l'IHEMI le 31 juillet 2022 : https://www.ihemi.fr/articles/organisation-france-europe-cybersecurite-cyberdefense-V2

[19] Agence nationale de sécurité des systèmes d'information (ANSSI), créée en 2009 et relevant d'un organisme rattaché au Premier ministre, le secrétariat général à la défense et à la sécurité nationale (SGDSN).

[20] Groupement d'intérêt public « Action de lutte contre la cybermalveillance » (ACYMA).

[21] La gendarmerie nationale dispose de correspondants N-TECH (C-NTECH) dans les unités territoriales, d'enquêteurs sur internet (ESI) dans les unités de recherche et des spécialistes nouvelles technologies (N-TECH) dans les unités d'appui, formant une communauté de 8.000 professionnel dénommée CYBERGEND.

[22] Enquêteurs en cybercriminalité (ICC) de la police nationale.

[23] European Cybercrime Center (EC3) de l'office européen de police (EUROPOL).

[24] Centre de lutte contre les criminalités numériques (C3N) de la gendarmerie nationale.

[25] Office central de lutte contre la criminalité liée au technologies de l'information et de la communication (OCLCTIC) rattaché à la police nationale.

[26] Brigade d'enquête sur les fraudes aux technologies de l'information et de la communication (BEFTI) de la préfecture de police de Paris.

[27] Centre de surveillance du commerce électronique (CSCE) relevant du service national des enquêtes (SNE) de la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

[28] Direction générale de la sécurité intérieure (DGSI), service de renseignement du ministère de l'intérieur chargé de la sécurité nationale et des intérêt fondamentaux de la Nation sur le territoire national.

[29] Direction générale de la sécurité extérieure (DGSE), service de renseignement du ministère des armées chargé de la recherche et de l'exploitation des renseignement intéressant la sécurité de la France, ainsi que de la détection et de l'entrave hors du territoire national, des activités d'espionnage dirigées contre les intérêts français.

[30] Commandement de la cyberdéfense (COMCYBER), rattaché au ministère des armées et réunissant, sous une direction opérationnelle unique et interarmes, les forces de cyberdéfense.

aux enjeux de la détection d'infractions et de la collecte de preuves : saisie et exploitation des supports numériques[31], accès aux données détenues par un tiers[32], enquêtes sous pseudonyme[33], interceptions de correspondance[34], perquisitions et saisie de données en ligne[35], captation de données à distance[36]. L'ensemble de ces pouvoirs trouvent leur équivalent dans le code de la sécurité intérieure[37] où est ajoutée, par ailleurs, la notion d'algorithme, ou « boîte noire », obligeant les fournisseurs d'accès à mettre à disposition des données de connexion à fin de traitement par les services de renseignement[38]. En revanche, le droit français refuse la mise en œuvre de procédés de lutte informatique offensive (LIO)[39] dans le cadre des missions d'enquête judiciaire.

S'adaptant au niveau tactique, les forces de l'ordre évoluent peu cependant dans leur stratégie, les dispositifs de lutte contre la délinquance continuant à recourir à un traitement individualisé et parcellisé du contentieux fondé sur la plainte de la victime. La mise en œuvre de plate-forme de recueil de signalement fait exception à cela. Sans souci de cohérence, celles-ci se sont démultipliées au sein des forces de l'ordre ces dernières années pour le signalement de contenus illicites (PHAROS)[40], le signalement d'escroqueries en ligne à la carte bancaire (PERCEVAL)[41], la plainte en ligne pour escroqueries (THESEE)[42] ou tout simplement la prise de contact en ligne avec les forces de l'ordre[43]. Mise en œuvre par la gendarmerie nationale, la plate-forme PERCEVAL[44] représente un changement de paradigme car elle ne fait plus de la plainte de la victime un préalable : le seul signalement de celle-ci est pris en compte, enrichi avec d'autres sources, rapproché en vue de générer des éléments permettant soit l'ouverture d'une enquête judiciaire, soit la recherche de solutions préventives avec les partenaires (Barlatier, 2020a). Cette approche apparaît comme un signe prometteur d'une nouvelle articulation entre la

[31] Art. 14, 66, 77-1 et 156 CPP et 230-1 suiv CPP pour la mise au clair de données chiffrées.
[32] Art. 14 CPP en sources ouvertes, art. 60-1, 77-1-1 et 99-3 CPP pour les données en sources fermées.
[33] Art. 230-46 CPP.
[34] Combinaison des art. 100 et 706-95 CPP pour l'interception du flux avec les art. 56 suiv, 76, 92 suiv, 706-95-1 CPP et la convention de Budapest pour l'exploitation des données en mémoire.
[35] Art. 56 suiv, 76 et 92 pour les perquisitions de jour, dont art. 57-1 pour les perquisitions à distance, art. 706-28, 706-35, 706-73, 706-89 et 706-91 CPP pour les perquisitions de nuit, convention de Budapest pour les données situées à l'étranger, art. 56 suiv, 76, 92, 94, et 96 CPP pour les saisies.
[36] Art. 706-102-1 CPP.
[37] Art. L851-1 CSI pour le recueil des données de connexion ; art. 851-2 CSI pour l'interception en temps réel des données de connexion, le géolocalisation en temps réel et les interceptions de correspondances par voie hertzienne ; art. L851-1-1 CSI pour les interceptions de sécurité ; art. L851-6 CSI pour l'identification d'un utilisateur par son appareil et le recueil de ses données de connexion ; art. L853-1 CSI pour la sonorisation et la captation d'images ; art. L853-2-1 CSI pour le recueil et la captation de données informatiques ; art. L853-3 CSI pour l'autorisation de pénétrer dans un véhicule ou un lieu privé pour la mise en oeuvre de ces techniques ; loi du 30 octobre 2017 prévoyant les visites domiciliaires, les assignations à résidence, ainsi que les mesures individuelles de contrôle administratif et de surveillance (MICAS - art L228-1 à L228-7 CSI), telles que l'interdiction d'entrer dans un périmètre géographique, l'obligation de se présenter périodiquement à un service de police ou à une unité de gendarmerie, celle de déclarer son lieu et ses changements de domicile, et le placement sous surveillance électronique.
[38] Art. 851-3 CSI.
[39] Introduction dans un système de traitement automatisé en vue d'en extraire, d'en altérer ou d'en neutraliser les données.

[40] La plate-forme PHAROS est accessible sous le lien suivant : https://www.internet-signalement.gouv.fr/PharosS1/ (consulté le 4 décembre 2022).
[41] La plate-forme PERCEVAL est accessible sous le lien suivant : https://www.service-public.fr/particuliers/vosdroits/R46526 (consulté le 4 décembre 2022).
[42] La plate-forme THESEE est accessible sous le lien suivant : https://www.moncommissariat.interieur.gouv.fr/fr/demarches/la-plainte-en-ligne-pour-les-arnaques-sur-internet-thesee (consulté le 4 décembre 2022).
[43] Issue de la récente fusion du site de la brigade numérique de la gendarmerie nationale et moncommissariat.fr de la police nationale, l'application ma sécurité est téléchargeable sous le lien suivant : https://play.google.com/store/apps/details?id=com.masecuriteapp&hl=fr&pli=1
[44] Dédiée aux escroqueries à la carte bancaire, la plate-forme PERCEVAL recueille en ligne les signalements des victimes sur la base d'une identification forte (*via* France Connect). Les informations ainsi collectées sont recoupées et enrichies avec les banques et e-commerçants afin de disposer de la masse critique d'informations nécessaires au développement de solutions de remédiation.

tradition judiciaire fondée sur la casuistique et la recherche de solutions nouvelles permettant une action à plus grande échelle.

Entre répression et régulation, les stratégies, souvent empiriques, choisies pour lutter contre la cybercriminalité se sont avérées insuffisantes et n'ont pas permis d'enrayer l'apparition d'une nouvelle dimension dans l'univers de la délinquance (Barlatier, 2019). De nouvelles méthodes en termes de compréhension et d'entrave pourraient ainsi être éprouvées. Elles invitent à présenter les apports du renseignement criminel.

3.2 Comprendre

Le renseignement criminel est une préoccupation ancienne et une méthode nouvelle. Il apparaît en France sous sa forme embryonnaire avec l'idée de « Haute police », où la préoccupation était de neutraliser les opposants politiques en les identifiant au sein de la population. Avec l'émergence de l'enquête en France, Vidocq importe cette préoccupation dans le champ criminel. Ancien condamné ayant construit sa réputation sur l'évasion, il acquiert une connaissance de la population criminelle au sein des bagnes, et met son savoir au service de la préfecture de police de Paris dans le cadre d'une action aussi efficace que contestée (Kalifa, 2013). Le renseignement criminel se fonde ainsi sur la logique de connaissance *a priori* des criminels. Cette vision sera contrebalancée quelques années plus tard par la promesse positiviste de solutionner le crime avec la science, inversant ainsi un schéma qui ne part plus des auteurs pour leur attribuer les faits qu'ils commettent, mais part des faits pour identifier les auteurs. La logique de l'enquête héritée de Vidocq restera néanmoins présente dans la culture et les méthodes des services de police judiciaire luttant contre la grande criminalité.

L'idée d'un savoir précédant l'action connait un renouveau avec l'émergence de l'*intelligence-led policing* (ILP), ou police guidée par le renseignement. Ce mouvement apparaît non pas dans le cadre d'une police scientifique portée par les sciences exactes, mais plutôt d'une approche scientifique de la police portée par les sciences humaines (Barlatier, 2020c). Partant du fameux « *Nothing Works* » de Robert Martinson (Martinson, 1974), après des premiers constats inquiétants sur l'efficience réelle des modes d'action des forces de l'ordre[45], les chercheurs ont abouti au constat criminologique que les pratiques policières devaient être évaluées et sortir des seules approches empiriques ou managériales qu'elles avaient connu jusqu'à présent. Les criminologues ont ainsi, tour à tour, proposé la création d'une police fondée sur la proximité avec les populations (*Community Policing* - COP ; Skogan, Hartnett, 1977), puis d'une police de résolution de problème (*Problem-Oriented Policing* - POP ; Goldstein, 1990). L'ensemble de ces politiques policières proposent le passage d'une police bitnérienne, pyramidale, bureaucratique, militarisée, réactive et concentrée sur ses propres modalités de fonctionnement (Bitner, 1970) à une police plus proactive et recentrée sur sa mission. Si elles ont montré une certaine efficience qui leur valent depuis d'être, tout à tour, reprises sous diverses politique gouvernementales (la fameuse alternance en France entre police d'intervention et police de proximité), le COP et le POP se limitent à proposer une compréhension et des entraves se réduisant à un traitement local de la délinquance. A la fin des années 1990, avec l'ILP, le criminologue britannique

[45] Par exemple, la célèbre expérience de Kansas City pour l'efficacité des patrouilles des police (Harris, 1977) ou l'étude de la Rand Corporation relative à la performance des enquêtes judiciaires (Chaiken *et al*., 1977).

Jerry Ratcliffe propose d'améliorer la pertinence de l'action policière en agissant à plus grande échelle sur les phénomènes criminels à partir de leur compréhension préalable (Ratcliffe, 2016).

Intégrée dans la criminologie francophone sous le vocable de « renseignement criminel », l'ILP repose sur les postulats de quatre grande théories criminologique (Maillard, 2017) :

- celle des « *prolific offenders* » (Wolfgang, Figlio, Sellin, 1972), qui indique que la majorité des infractions sont commises par une minorité de délinquants chroniques (*prolific offenders*) ayant érigé la criminalité en un mode de vie. La connaissance de ces individus permet de concentrer l'action des forces de l'ordre sur la population délinquante utile ;
- celle des « activités routinières » (Cohen, Felson, 1979), avançant l'importance de la notion d'opportunité criminelle dans la commission du crime, fruit d'une activité de routine où se rencontrent des individus (l'auteur, la victime) et des occasions (dans un cadre espace-temps). La compréhension de ces circonstances permet d'identifier les modèles fondés sur les répétitions criminelles (Bradford, 2017) ;
- celle du « choix rationnel » (Felson, Clarke, 1998), où le délinquant s'adapte à son environnement immédiat en fonction d'un calcul en termes de risques et de bénéfices. La compréhension de la délinquance implique donc de se mettre à la place du criminel et de connaître les paramètres de son choix ;
- celle des « *patterns* » (Brantingham, Brantingham, 1994), à partir de laquelle il est possible d'analyser les répétitions et les anomalies dans la récurrence des faits afin de pouvoir établir les caractéristiques uniques d'un phénomène criminel. Par exemple, dans une approche géographique, le mouvement du *hot spotting* se fonde sur l'analyse des concentrations criminelles.

L'ILP propose trois focales d'analyse (Maillard, 2017) :

- le niveau stratégique, qui est une aide à la compréhension des phénomènes, de la géographie et des groupes criminels ;
- le niveau opérationnel (ou opératif), qui est une aide à la décision pour les autorités politiques, hiérarchiques, administratives ou judiciaires ;
- le niveau tactique, qui est une aide à l'enquêteur ou au patrouilleur pour l'accomplissement de sa mission.

Au sein de la gendarmerie nationale, la méthode du renseignement criminel a été formalisée à partir du cycle du renseignement (collecte-traitement-analyse-production) et de la logique de raffinage qui y est attachée (*Data-Information-Knowledge-Intelligence*, mieux connu sous la dénomination « DIKI »). Face au processus linéaire de l'enquête judiciaire fondé sur l'exploration des pistes, le renseignement propose ainsi un processus circulaire selon une boucle itérative et incrémentale qui repose sur quatre qualités :

- l'exhaustivité, car la phase habile de collecte des données ne se limite pas aux seuls éléments de l'activité des services d'enquête (qui transforment bien souvent leurs analyses en de simples bilans d'activité), mais exploite l'ensemble des sources disponibles (ouvertes ou fermées, d'origine humaine, financière, cyber, technologique, culturelles, *etc.*) ;

- la rigueur, car la phase souvent technique de traitement de l'information impose de classer, d'uniformiser, d'indexer et de visualiser des données de plus en plus volumineuses afin d'en tirer des informations utiles à la confrontation et à l'exploration des éléments collectés ;
- pertinente, car la phase intellectuelle d'analyse doit permettre d'élaborer un savoir fondé sur une pensée critique ou la logique, comme la capacité de conception et de confrontation des hypothèses permettent de comprendre ce qui se voit et d'envisager ce qui ne se voit pas (*i.e.*, *intelligence gap*) ;
- maîtrisée, car la phase persuasive de production du renseignement doit transformer ce savoir en action dans le cadre de constats, d'interprétations et de recommandations utiles au destinataire.

Cette méthode n'est pas spécifique au renseignement criminel. Elle est un processus de connaissance mis en œuvre, de façon plus générale, par les « travailleurs du savoir » (Bouchez, 2004). Dans le monde du numérique, elle est déjà mise en œuvre par les acteurs de la *cyber threat intelligence* (CTI) chargés de l'analyse des cyber menaces (Wagner et al., 2019). La CTI est destinée à élaborer une analyse de risque permettant de connaître les menaces et d'identifier les vulnérabilités. Elle envisage la compréhension technique et contextuelle :

- des outils utilisés, par l'inventaire et la retro-ingénierie des *malwares*, des logiciels et autres infrastructures techniques de délinquance ;
- des modes d'action, par la connaissance des pratiques sur l'ensemble du processus, de la recherche d'informations préalables à la reconnaissance, des techniques de pénétration, d'attaque, des modalités d'exploitation des bénéfices (paiement, blanchiment et remploi) ;
- des acteurs, orientées sur le recensement des groupes cybercriminels et de leur rôle, permettant une connaissance de leurs caractéristiques et de leurs capacités, un suivi historique et une anticipation de leur évolution, la compréhension et l'attribution de leurs actes.

Impliquant une coordination entre les acteurs publics et privés fondée sur la circulation de l'information, la CTI repose sur des méthodes et des modèles relativement standardisés, tels que les référentiels *Kill chain*[46] et Mitre[47], ou les classement YARA[48] et SIGMA[49]. L'objectif est le partage de signaux faibles (dont les IoC, *indicators of Compromise*, destinés à la détection des signes d'intrusion), des tactiques et des techniques d'attaque, et enfin des mesures de remédiation pouvant être adoptées. Les éléments ainsi collectés sont versés dans un *security information and event management* (SIEM) qui est destiné à établir les relations et les corrélations entre les événements enregistrés et les modèles connus.

Sommairement décrite, la CTI est compatible avec les finalités et les méthodes du renseignement criminel. Orientée sur les aspects les plus techniques, elle ne répond pas intégralement aux

[46] Pour une synthèse d'écrits sur le référentiel *Kill Chain* : https://www.sciencedirect.com/topics/computer-science/kill-chain (consulté le 4 décembre 2022).

[47] Pour accéder aux à la documentation Mitre : https://attack.mitre.org/techniques/enterprise/ (consulté le 4 décembre 2022).

[48] Pour accéder à la documentation Yara : https://yara.readthedocs.io/en/stable/index.html (consulté le 4 décembre 2022).

[49] Pour une synthèse de ces méthodes : https://www.threat-intelligence.eu/standards/ (consulté le 4 décembre 2022). Ce site contient également un certain nombre de références utiles en termes d'analyse.

attentes de compréhension de l'ensemble des phénomènes délinquants. Particulièrement utile en termes d'atteintes aux systèmes de traitement automatisé de données (ASTAD), la CTI est insuffisante pour aborder les atteintes aux biens (escroqueries et fraudes, notamment) et aux personnes (insultes, diffamation, harcèlement, pédopornographie, *etc.*) qui doivent faire l'objet d'une compréhension criminologique plus que technique. La CTI permet d'élaborer un renseignement d'intérêt cyber (RIC) qui ne doit pas être confondu avec le renseignement d'origine cyber (ROC ou *cyber intelligence* - CYBINT) qui aborde le numérique comme une source de renseignement (tel que le *Social Media Intelligence* - SOCMINT) et non comme un sujet d'analyse (Brun *et al.*, 2022).

A cet effet, si la CTI est une méthode adaptée et compatible avec le renseignement criminel, elle ne doit pas être sanctuarisée au risque de perdre de sa pertinence. L'analyste en renseignement criminel spécialisé dans les cybermenaces doit évoluer dans un écosystème plus large, entouré de ses collègues spécialistes en termes de trafics illicites, de traite des êtres humains, de violences aux personnes, de victimologie, d'infractions économiques et financières, de vols et de recel, de connaissance des groupes criminels ou de géographie criminelle. L'analyste cyber doit pouvoir bénéficier de l'écosystème de compréhension des autres domaines de la criminalité car, pas plus que l'utilisation de la voiture au début du XX^{ème} siècle n'était sécable de la délinquance de son époque, la cybercriminalité au début du XXI^{ème} siècle n'est pas une forme de délinquance à part entière. Elle reste, pour l'essentiel, un nouveau mode d'action des criminalités traditionnelles.

Destiné à réduire l'incertitude par une compréhension au plus près des réalités, le renseignement criminel est un savoir en vue d'une action réelle et concrète sur la délinquance. Il est ainsi en mesure de renouveler les solutions de lutte contre la cybercriminalité.

3.3 Agir

La compréhension préalable des phénomènes permet de faciliter la recherche de solution et la détermination des stratégies pour les mettre en œuvre. Le renseignement criminel s'inscrit dans un objectif performatif de remédiation (au sens étymologique de « porter remède »). Les solutions qu'il propose n'ont pas à être limitées à la recherche d'une réponse judiciaire sur l'infraction principale, mais envisage plus largement l'annihilation d'un mode opératoire ou d'un groupe criminel par tout moyen légal.

A cet effet, le champ de la réponse policière s'inscrit dans la dynamique « *What works? What doesn't? What's promising?* ». Diversifiant le champ des possibles, il repose tant sur une logique de *benchmark* et de retour d'expérience de solutions déjà éprouvées, que sur la capacité à concevoir de nouvelles solutions innovantes, et parfois audacieuses. En application de la matrice SWOT (*Strengths, Weaknesses, Opportunities, Threats*), les recommandations doivent être conçues à partir d'une analyse des paramètres internes (forces et des faiblesses) et externes (opportunités et des menaces). Dans leur mise en œuvre, elles doivent être précises, évaluables, réalistes, pertinentes et cohérentes dans le temps, conformément aux principes SMART (*Specific, Measurable, Attainable, Relevant, Time-based*).

Sur le socle de ces notions fondamentales, trois formes de remédiations sont généralement distinguées :

- l'entrave pénale, qui consiste à mettre en

évidence un interdit afin de faciliter la constatation des infractions, d'améliorer le recueil des preuves ou de faciliter l'identification des auteurs. Elle recherche le prononcé d'une décision judiciaire adaptée concernant l'infraction principale ou des infractions secondaires ou incidentes. Cela pourrait consister à obtenir l'incarcération d'un individu sur le simple constat du non-respect de ses obligations de contrôle judiciaire, par exemple ;

- l'entrave administrative, qui consiste à mettre à profit, de façon distincte ou combinée, les pouvoirs dont disposent les administrations en termes fiscal, de prestations sociales, de répression de fraudes, de droit douanier, de législation sur les étrangers, *et cetera*. La coordination avec les administrations de l'État et des collectivités locales revêt alors un aspect essentiel afin d'autoriser une réaction intégrée de l'autorité publique à la criminalité, fondée sur la détection de situations criminelles, la dissuasion, l'empêchement ou la neutralisation des auteurs. Cela peut consister à créer un environnement administratif hostile à l'égard d'un délinquant, ou à combler une vulnérabilité réglementaire qui profite à la fraude ;
- l'entrave partenariale, qui consiste à proposer des solutions préventives ou curatives avec la coopération d'acteurs privés. Souvent fondée sur une action portant sur les circonstances du crime, elle consiste, dans une logique de prévention situationnelle, à mieux informer les victimes, à mieux protéger les cibles, à réduire l'utilité du crime ou à accroître les risques de détection et d'identification pour les auteurs. Cela consiste, par exemple, à inciter un commerce à modifier ses processus de vente pour réduire les opportunités de vol.

Le renseignement criminel ouvre ainsi le champ des possibles en termes de modes d'action. Les forces de l'ordre ne sont plus tenues à des processus standardisés mis en œuvre dans le cadre d'une obligation de moyens. Le traitement judiciaire de la délinquance n'est plus l'unique réponse des forces de l'ordre. Cela permet d'échapper à l'involution des buts que représente une approche managériale du système pénal (Jean, 2008 ; Cliquennois *et al.*, 2015), où les flux de délinquance traités dépendent de la capacité des institutions à les assumer (prise de plainte, élucidation, poursuite, capacité d'audiencement, stock pénitentiaire, *etc.*). L'analyste en renseignement criminel doit être en mesure de proposer de nouveaux filons d'efficacité et de tenter d'enrayer les phénomènes le plus en amont possible. S'inscrivant dans une approche pragmatique et conséquentialiste, il doit pouvoir bénéficier de la diversité des outils offerts par la criminologie. Le policier devient le catalyseur des moyens de lutte contre la délinquance.

L'écosystème cyber est particulièrement propice à un tel décloisonnement des solutions. Les acteurs de sa régulation proposent déjà des mesures de remédiation recourant à une gestion du risque, avec des réponses graduées, loin de l'approche disjonctive entre le légal et l'illégal. Abordant les phénomènes de façon holistique et non casuistique, ces solutions recherchent le plus fort impact au moindre coût. Fondées sur l'analyse de données, elles mettent en oeuvre des stratégies inventives. D'une façon générale, les méthodes d'entrave sur le

Web reposent sur la cinématique détection - caractérisation - blocage - signalement. Tel est le cas des algorithmes de détection des transactions frauduleuses mis en œuvre par les e-commerçants et les banques à partir des *patterns* de fraude connus. Le signalement des fraudes en ligne par les internautes sur les forums et réseaux sociaux est également un moyen de rétablir un contrôle social dans cet espace d'anonymat par une information pertinente des victimes destinée à désamorcer les situations pré-criminelles.

Certains États sont en mesure de mettre en œuvre des stratégies bien plus élaborées. Ainsi, pourtant considéré comme garantissant l'anonymat de ses utilisateurs, le *darkweb* n'échappe-t-il pas à l'action des services de renseignement. La surveillance du téléchargement et de l'utilisation de TOR[50] permet, par exemple, de disposer de signaux faibles à l'égard d'internautes susceptibles d'avoir des activités clandestines. Ainsi, des stratégies offensives et audacieuses ont pu être développées à l'égard des *darkmarket*. En 2017, une opération combinée du *Federal Bureau of Investigation* (FBI) et de la police néerlandaise a ainsi permis de saisir les deux plus importantes *marketplace*[51] : laissant leurs homologues néerlandais prendre le contrôle du site *Hansa Market* par des techniques de lutte informatique offensive (LIO) auxquelles leurs services sont habilités, les fédéraux américains ont ensuite saisi le site *Alphabay*. Poussés par la nécessité de continuer leur activité marchande, les utilisateurs d'*Alphabay* se sont majoritairement réfugiés sur *Hansa Market*, autorisant ainsi leur identification par la police des Pays-Bas. Complétée par une opération de communication à destination des utilisateurs de ces plates-formes, ce dispositif opérationnel a recherché une entrave pénale à l'encontre des principaux vendeurs, une entrave technique à l'égard des sites et un effet psychologique à l'égard d'utilisateurs du *darkweb*, désormais conscients de ne plus pouvoir préserver leur anonymat en ce lieu où ils se sentaient libre d'agir en toute impunité. A l'issue de cette opération, l'*US attorney general* Jeff Session avertira les trafiquants « *You cannot hide* ». Pour déployer une opération de telle ampleur, les autorités américaines et néerlandaises ont dû préalablement réaliser un travail de renseignement sur les objectifs (quelles plates-formes cibler ? comment en prendre le contrôle ? quels trafiquants neutraliser ?), avant de planifier une stratégie coordonnée qui sera mise en œuvre avec succès en recourant à modes d'action techniques et juridiques correctement planifiés.

En août 2019, en coordination avec le FBI, la gendarmerie nationale neutralise le *Botnet*[52] Retadup hébergé sur un serveur en Île-de-France. Réalisée sur renseignement, cette opération a permis la désinfection de 850.000 ordinateurs piratés. Cette entrave technique a permis d'atteindre une infrastructure de délinquance active depuis 2016 et qui était en mesure de contrôler et commander les machines à distance en vue de la commission de rançongiciels, de vols de données ou d'attaques DDOS.

En juillet 2020, la gendarmerie nationale annonce le démantèlement du réseau de *darkphones* Encrochat. Actif depuis 2015, ce réseau de communication

[50] Acronyme de *The Onion Router*, le réseau TOR est tout à la fois un réseau décentralisé et un navigateur, dont le fonctionnement garanti l'anonymat des utilisateurs. Il est l'un des *darknet* qui permet d'accéder au *darkweb*.

[51] Situées sur le *darkweb*, les *marketplaces* sont des sites commerciaux sur lesquels sont échangés des biens et services illégaux : drogue, armes, services illicites en ligne, numéro de carte de crédits volés, produits pharmaceutiques, fausse monnaie, *et cetera*. L'anonymat des échanges est compensé par des dispositifs destinés à garantir les transactions (*e.g.*, le système d'*escrow* instaurant un intermédiaire de paiement). Celles-ci sont opérées en crypto-actifs.

[52] Un *Botnet* est un réseau d'ordinateurs infectés, dont chacun peut être contrôlé à distance pour conduire des attaques de type DDOS, ou encore procéder à des envois de *spam*.

chiffré et sécurisé était essentiellement utilisé par des groupes criminels organisés de haut niveau, notamment en matière de trafic de stupéfiants. Détectant ce réseau en 2017, les gendarmes ouvrent une enquête devant la juridiction interrégionales spécialisée (JIRS) de Lille en 2018 et parviennent à comprendre le fonctionnement de ce réseau pour parvenir à intercepter les communications en temps réel à compter de 2019. Une équipe commune d'enquête franco-néerlandaise « Emma 95 / 26 Lemont » est créée dans le cadre d'Europol, en partenariat avec plusieurs forces de police à l'étranger. 120 millions de communications impliquant près de 60.000 utilisateurs sont ainsi exploitées en temps réel en vue d'opérations de saisies de stupéfiants (dont 100 tonnes de cocaïne), de saisies d'avoirs criminels (330 millions d'Euros), de la découverte de 19 laboratoires de drogues synthétiques et de lieux de détention et de torture mis en place par les groupes criminels. Plus de 200 projets d'assassinats sont ainsi déjoués et 5800 criminels arrêtés dont certains étant des cibles de haut niveau recherchées de longue date par les États. Ces résultats édifiant démontrent l'intérêt du travail en renseignement et de la détermination de filons d'élucidation permettant disposer de leviers d'efficacité contre la criminalité de masse transitant par les réseaux. L'exploitation de ces sources a également permis de comprendre l'envers du décors de la criminalité organisée et d'identifier des cibles de haut niveau (HVT, ou *high value targets*) animant depuis l'étranger (Dubaï notamment) les trafics en France. En 2021, une opération similaire est conduite par les autorités belges, néerlandaises et françaises sur le réseau chiffré Sky ECC. D'autres États renouvelleront cette expérience de lutte contre un phénomène à grande échelle en permettant aux forces de l'ordre de transformer une infrastructure utilisée par les délinquants en un moyen de lutte contre les groupes criminels.

Le réseau de téléphone chiffré ANOM représente une stratégie de déception autrement plus ambitieuse de la part des autorités américaines. Dans le cadre de l'opération *Trojan Shield*, le FBI et l'*Australian Federal police* (AFP) ont mis en place, de 2018 à 2021, un réseau de cryptophones qui a été utilisé par de nombreux groupes criminels. Déclenchée le 8 juin 2021, l'opération a permis l'interpellation simultanée de 800 individus dans 16 pays et la saisie de 40 tonnes de drogues.

Ces quelques exemples illustrent l'efficacité de stratégies d'entrave guidées par le renseignement. Elles renversent le paradigme judiciaire classique quant aux modalités de détection des affaires et de détermination des solutions de remédiation.

4. Conclusion

Cet article tente de situer la cybercriminalité en soulignant les spécificités de son écosystème technique et criminologique. Il indique que ce phénomène a pris le pas sur les autres formes de délinquance et constitue une priorité pour les force de l'ordre.

Qu'elle considère internet comme objet ou comme vecteur, cette délinquance de masse tend, en effet, à réduire à l'impuissance les processus classiques de réaction pénale consistant à constater les infractions pour ensuite les élucider par la révélation de leurs causes, en vue de poursuites et de réponses judiciaires.

Le renseignement criminel est capable de modifier cette posture réactive des forces de l'ordre. L'entrave pénale est alors mise en œuvre, non comme la volonté de réguler, par des actes de détail, un contentieux massif et difficile à élucider, mais comme une solution orientée et gagnante, cherchant

à atteindre avec précision le cœur des réseaux.

L'action judiciaire s'intègre alors comme composante d'un processus de savoir et se trouve combinée et coordonnée à un ensemble d'autres solutions. Sans renier l'enquête judiciaire, cette approche la remet dans une position d'efficacité dans le cadre de dispositifs à la fois imaginatifs et légaux.

Savoir guidant l'action, le renseignement devient alors le moyen d'aborder avec plus d'efficience la cybercriminalité dans cet environnement incertain et peu régulé qu'est le cyber espace. Conscient des risques d'un *Far-West*, terre de promesse comme de non-droit, où la cavalerie arrive toujours en retard, le renseignement criminel tente de réguler les effets de la création d'un *Far-Web* par une action résolue et proactive où il marque de son empreinte les immensités d'un territoire virtuel.

Bibliographie

1. Ablon L., Libicki M., Golay, A. A., *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Rand Corporation, 2014
2. Barlatier J., « Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime », *Risks*, vol. 8, n. 3, 2020b.
3. Barlatier J., « De L'enquête au Renseignement, Changement de Paradigme Pour la Victime » Paris: AJ Penal, 2020a, pp. 17-20.
4. Barlatier J., « De l'enquête scientifique à l'approche scientifique de l'enquête », *Médecine légale du vivant*, vol. 14, n. 1, 2020c, pp. 1-11.
5. Barlatier J., « L'enquête judiciaire est-elle une réponse appropriée à la cybercriminalité? », *Revue de la Gendarmerie Nationale*, 4ème Trimestre, 2019, pp. 159-62.
6. Barlatier J., *Management de l'enquête et ingénierie judiciaire, recherche relative à l'évaluation des processus d'investigation criminelle*, Thèse de Doctorat en Criminologie. Lausanne: UNIL/École des Sciences Criminelles, 2017.
7. Bitner E., *The Functions of the Police in Modern Society: Review of Background Factors, Current Practices and Possible Role Model*, Oelgeshlager, Gunn & Hain. Cambridge, 1970.
8. Bouchaud F., *Analyse forensique des écosystèmes intelligents communicants de l'internet des objets*, Thèse de doctorat en Informatique et applications, sous la direction de Gilles Grimaud et de Thomas Vantroys, soutenue en 2021 à l'Université de Lille.
9. Bouchez J.P., Les nouveaux travailleurs du savoir, Éditions d'organisation, Paris, 2004.
10. Bradford W.R., *Routine Activity Theory and Cybercrime, A Theoretical Appraisal and Literature Review. Technocrime and Criminological Theory*, Routledge, London/New York, 2017.
11. Brantingham P.L., Brantingham, P.J., « La concentration spatiale relative de la criminalité et son analyse : vers un renouvellement de la criminologie environnementale », *Criminologie*, vol. 27, n. 1, 1994, pp. 81-97.
12. Broadhurst R., Graborvsky P., Alazab M., Bouhours B., « An Analysis of the Nature of Groups engaged in Cyber Crime », *International Journal of Cyber Criminology*, vol. 8, n. 1, 2014, pp. 1-20.
13. Brun F., Cohen Y., Craciuneac C., Grépin F., Mouchès G., Wisson C., *L'apport du cyber dans les techniques d'investigation. Rapport de l'école de guerre économique*. Disponible en ligne le 31 juillet 2022 : https://www.ege.fr/infoguerre/lapport-du-cyber-dans-les-techniques-dinvestigation
14. Chaiken J.M., Greenwood P., Petersilia J., *The criminal Investigation Process. A Summary Report*, The Rand Paper Series. The Rand Corporation, Santa Monica, 1976.
15. Cliquennois G., Bellebna H., Léonard, T., « Management et système pénal: Présentation du dossier », *Droit et société*, vol. 90, n. 2, 2015, pp. 243-252.
16. Cohen L.E., Felson M., « Social change and crime rate trends: A routine activity approach » (1979), in Andresen M., Kinney

B.., *Classics in environmental criminology*, Routledge, London, 2010, pp. 203-232.
17. Crozier M., Friedberg E., *L'acteur et le système*, Seuil, Paris, 1977.
18. Douzet F., « La géopolitique pour comprendre le cyberespace", *Herodote*, vol. 1, n. 152-153, 2014, pp. 3-21.
19. Dregoir M., Klein E., *L'effet Iceberg et la Cybercriminalité*, Étude Service Central de Renseignement Criminel de la Gendarmerie Nationale, Centre de recherche de l'école des officiers de la gendarmerie nationale, Melun, 2017.
20. Dulaurans M., Fedherbes J-C., *Cyberharcelement et communautes en ligne: les resiliences organisationnelles en jeu! Un monde de crises au prisme des communications organisationnelles*, Universite Catholique de Louvain [UCL], Mons, Belgique, 2022, hal-03655311
21. Europol, *Internet Organized Crime Threat Assessment (IOCTA)*, disponible à l'adresse suivante : https://www.europol.europa.eu/iocta/2015/resources/iocta-2015.pdf
22. Felson M., Clarke R.V., *Opportunity Makes the Thief. Police Research Series, Paper 98*, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, London, 1998.
23. Foucault M., *Surveiller et punir. Naissance de la prison*, Gallimard, Paris, 1975.
24. Frampton L., *The Hunters and the Hunted: Exploring Practitioner and Public Attitudes Towards Paedophile Hunting Groups and the Implications for Risk Management*, Thèse Université de Portsmouth, 2021. Disponible à l'adresse suivante: https://pure.port.ac.uk/ws/portalfiles/portal/27089150/The_Hunters_and_The_Hunted._Exploring_Practitioner_and_Public_Attitudes_Towards_Paedophile_Hunting_Groups_and_the_Implications_for_Risk_Management.pdf (consulté le 4 décembre 2022).
25. Ghernaouti-Hélie S., *La cybercriminalité, le visible et l'invisible*, Presses polytechniques et universitaires romandes, Lausanne, 2009.
26. Goldstein H., *Problem-Oriented Policing*, Temple University Press, Philadelphie, 1990.
27. Hadjimatheou K., « Citizen-led digital policing and democratic norms: The case of self-styled paedophile hunters », *Criminology & Criminal Justice*, vol. 21, n. 4, 2021, pp. 547-565.
28. Harris L.H. (1977), *Response Time Analysis*, Missouri Police Department, Kansas City MO, 1977.
29. Jean J.P., *Le système pénal*, La Découverte, Paris, 2008.
30. Kalifa D., *Histoire des détectives privés*, Nouveau Monde edition, Paris, 2013.
31. Kemp S., « Fraud reporting in Catalonia in the Internet era: Determinants and motives », *European Journal of Criminology*, 2020, pp. 1-22.
32. Koops B-J., « The Internet and it's opportunities for cybercrime », *Tilburg Law School Legal Studies Research Paper Series*, vol. 1. n. 09, 2011, pp. 735-754.
33. Kuerbis B., Badeie F., Grindal K., Mueller M., « Understanding transnational cyber attribution: Moving from "whodunit" to who did it », in Cavelty M., Wenger A., *Cyber Security ans Politics, Socio-Technological Transformations and Political Fragmentation*, Routledge, Londres/New York, 2022.
34. Lalam N., « L'argent de la drogue en France », *Après-demain*, vol. 4, n. 44, 2017, pp. 46-48.
35. Lalam N., « Le trafic de drogue : un activité économique ancrée et adaptative », *Studia Diplomatica*, vol. 55, n. 5/6, Géopolitique et nouvelles criminalités internationales : actes du colloque des 13 et 14 décembre 2002 (Palais d'Egmont, Bruxelles) 2002, pp. 51-63.
36. Leukfeldt E. R., « Organised Cybercrime and Social Opportunity Structures: A Proposal for Future Research Directions », *The European Review of Organised Crime*, vol. 2, n. 2, 2015, pp. 91-103.
37. Leukfeldt E. R., Holt T., J., *The human factor of cybercrime*, Routledge, Londres, 2021.
38. Linde A, Aebi, M., « La criminologie comparee a l'heure de la societe numerique : Les theories traditionnelles

peuvent-elles expliquer les tendances de la cyber-delinquance ? », *Revue Internationale de Criminologie et de Police Technique et Scientifique*, vol. 4, n. 20, 2020.
39. Locard E., *Manuel de technique policière*, Payot, Paris, 1934.
40. Loveday B., « The Shape of Things to Come. Reflections on the potential implications of the 2016 Oce of National Statistics Crime Survey for the Police Service of England and Wales », *Policing: A Journal of Policy and Practice*, vol. 12, pp. 398–409.
41. Maillard de C., *Le renseignement criminel dans les forces de police françaises, une étude de l'absent et de l'existant au prisme du modèle de police guidée par le renseignement*, Thèse de doctorat en criminologie, sous la direction de Olivier Ribaux, soutenue en 2017 à l'école des sciences criminelles de l'université de Lausanne.
42. Margagliotti G., Borisova B., Ajil A., Rossy Q., *Mon canton, ma sécurité: sentiment de sécurité physique et numérique et opinions sur la police neuchâteloise*, Ecole des Sciences Criminelles, Lausanne, 2019.
43. Martinson R., (1974), « What works? Questions and answers about prison reform », *Public Interest*, vol. 35, 1974, pp. 22-54.
44. Petratos P. N., « Misinformation, disinformation, and fake news: Cyber risks to business », *Business Horizons*, vol. 64, n. 6, 2021, pp. 763-774.
45. Ratcliffe J., Intelligence-led Policing, Willan, Cullompton, 2016.
46. Rudesill D., S., Caverlee J., Sui D., *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*, Woodrow Wilson International Center for Scholars, STIP 03, October 2015, Ohio State Public Law Working Paper No. 314.
47. Skogan W. G., Hartnett S. M., *Community policing*, Chicago style, Chicago, 1977.
48. Théry G., *Les autoroutes de l'information*, Rapport au premier ministre, La documentation française, Paris, 1994.
49. Wagner T. D., Mahbub K., Palomar E., Abdallah A. E., « Cyber threat intelligence sharing: Survey and research directions », *Computers & Security*, vol. 87, 2019, 101589.
50. Wall D., *Cybercrime*, Polity press, Cambridge, 2007.
51. Wolfgand M. E., Figlio R., Sellin T., *Delinquency in a Birth Cohort*, University of Chicago Press, Chicago, 1972.
52. Yu S., *Human trafficking and the internet. Combating Human Trafficking: A multidisciplinary approach*, CRC Press, Boca Raton, 2015.

Textes juridiques

1. Code de procédure pénale (CPP).
2. Code de la sécurité intérieure (CSI).
3. Convention du Conseil de l'Europe relative à la cybercriminalité signé à Budapest le 23 novembre 2001. Série des traités européen n° 185.
4. Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, adopté le 17 novembre 2021. Disponible en ligne le 31 juillet 2022 : https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4c
5. Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite « Godfrain », NOR : JUSX8700198L, JORF du 6 janvier 1988.

doi: 10.14664/rcvs/245

Cybercriminalità e pluralizzazione del policing: alcune riflessioni sulla cyber threat intelligence

Cybercriminalité et pluralisation du policing : la cyber threat intelligence en question

Cybercrime and pluralization of policing: questioning the cyber threat intelligence

Camille Guisset et Giorgia Macilotti***

Riassunto
Il presente contributo si pone l'obiettivo di analizzare il ruolo svolto dal settore privato nel contrasto alla cybercriminalità, con particolare riferimento all'emergere di nuove strategie fondate su modalità d'azione proattive finalizzate alla raccolta di informazioni. L'attenzione sarà focalizzata in particolare sulla *cyber threat intelligence* (CTI), un'espressione utilizzata per descrivere un processo *e* un risultato basati sulla raccolta, l'elaborazione e l'interpretazione di differenti tipi di dati con l'obiettivo di fornire conoscenze che consentano di valutare la natura e le caratteristiche delle «minacce» di natura informatica. Particolarmente sviluppata dagli attori privati della cybersicurezza, la CTI è uno strumento di supporto decisionale che solleva diversi interrogativi in merito alla sua definizione, alla metodologia utilizzata e alla portata dei risultati ottenuti.

Résumé
Cet article vise à interroger le rôle joué par le secteur privé dans la lutte contre la cybercriminalité, en se focalisant notamment sur l'émergence de nouvelles stratégies fondées sur des modes d'action proactifs visant à la collecte de renseignements. Une attention particulière sera accordée à la *cyber threat intelligence* (CTI), une expression utilisée pour décrire un processus *et* un produit résultant de la collecte, l'analyse et l'interprétation de différents types de données dans l'objectif de fournir des connaissances permettant d'évaluer la nature et les caractéristiques des « cybermenaces ». Particulièrement développée par les acteurs privés de la cybersécurité, la CTI est un outil d'aide à la décision qui soulève plusieurs questions quant à sa définition, à la méthodologie utilisée et à la portée des résultats obtenus.

Abstract
This article aims to examine the role played by the private sector in the policing of cybercrime, focusing particularly on the emergence of new strategies based on proactive methods designed for collecting intelligence.
Particular attention will be paid to cyber threat intelligence (CTI), an expression used to describe a process *and* a product resulting from the collection, the analysis and the interpretation of different types of data in order to provide knowledge for assessing the nature and characteristics of cyber threats. Particularly developed by private cybersecurity actors, the CTI is a decision support tool that raises several questions about its definition, its methodology and the relevance of the results obtained.

Key words : cybercriminalité, cybersécurité, *policing*, *cyber threat intelligence*, acteurs privés

* Diplômée du master 2 Relations Internationales et Politiques de Sécurité et de Défense (Université de Toulouse Capitole), analyste en *cyber threat intelligence* et consultante en gestion de crise.
** Enseignante-chercheuse en sociologie, membre de l'Institut de Cybersécurité de l'Occitanie, chercheuse associée à l'Institut du Droit de l'Espace, des Territoires, de la Culture et de la Communication (Université de Toulouse Capitole).

1. Introduction[1]

Internet, cyberespace, réseaux, objets connectés, intelligence artificielle, *blockchain* sont plus que jamais des termes incontournables pour penser quelques-unes des principales transformations sociales en cours. Puisant leurs origines dans une époque post-industrielle caractérisée par le passage à une économie de services immatériels et par des profonds changements dans les rapports et les rôles sociaux (Bell, 1973), Internet et les technologies numériques figurent parmi les principaux vecteurs des mutations sociales auxquelles nos sociétés sont confrontées depuis la fin du siècle dernier. Les potentiels fournis par la numérisation et l'échange rapide des données couplés à la restructuration globale du capitalisme, à la mondialisation et à la « logique de réseau » ont contribué au renouvellement des modèles sociaux, culturels et politico-économiques au centre desquels se trouvent l'échange et le traitement de l'information (Castells, 2001).

Toutefois, ces technologies porteuses de progrès génèrent aussi de nouvelles vulnérabilités qui peuvent être exploitées à des fins criminelles. Des attaques par rançongiciels[2] aux atteintes sexuelles envers les mineurs en passant par l'usurpation de l'identité numérique, les formes de délinquance tirant profit des opportunités offertes par le numérique ne cessent de se diversifier et se multiplier (Décary-Hétu, Bérubé, 2018 ; Yar, Steinmetz, 2019 ; Fortin, 2020). Malgré les limites méthodologiques et interprétatives des statistiques sur la cybercriminalité (Côté *et al.*, 2016 ; Macilotti, 2018a ; Dupont, 2021), les données élaborées par les acteurs publics de la sécurité identifient plusieurs tendances utiles pour comprendre l'évolution actuelle des criminalités numériques, en lien notamment avec les effets de la crise sanitaire (ralentissement des activités économiques, diffusion du télétravail, pénurie de certains biens de première nécessité, etc.). Selon l'*Internet Crime Complaint Center* du FBI (IC3, 2022), par exemple, les plaintes pour des faits de cybercriminalité ont presque triplé aux États-Unis entre 2017 et 2021 (respectivement 301 580 et 847 376 plaintes enregistrées). En France, en 2020, le nombre de signalements liés à des rançongiciels traités par l'Agence Nationale de la Sécurité des Systèmes d'Information a été multiplié par quatre par rapport à l'année 2019 (respectivement 191 et 54 faits constatés ; ANSSI, 2021), avec une progression observée également en 2021 (203 signalements traités ; ANSSI, 2022). L'augmentation des cyberattaques ciblant des infrastructures critiques et basées, entre autres[3], sur l'utilisation de rançongiciels a été soulignée également par la police italienne des communications[4], avec 5 434 épisodes traités en 2021 (*Polizia Postale e delle Comunicazioni*, 2022) contre 507 en 2020 et 239 en 2019 (*Polizia Postale e delle Comunicazioni*, 2021).

[1] Bien que l'article soit le fruit d'une réflexion commune des auteures, il faut attribuer plus spécifiquement les sections 1, 2, 4 et 5 à Giorgia Macilotti et les sections 3.1, 3.2 et 3.3 à Camille Guisset.

[2] Selon l'agence nationale française en charge de la cybersécurité (ANSSI), une attaque par rançongiciel (en anglais *ransomware)* « consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement », https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/rancongiciel/

[3] Parmi les attaques contre les infrastructures critiques constatées par la *Polizia Postale e delle Comunicazioni* (2021 et 2022), on retrouve celles basées sur l'utilisation de rançongiciels, mais aussi celles liées à d'autres modes opératoires comme les attaques par déni de service, les accès frauduleux à un système informatique, les campagnes de phishing ou de type APT (*Advanced Persistent Threats*).

[4] Une réorganisation des services de cybersécurité et de lutte contre la cybercriminalité est actuellement en cours en Italie. Pour plus d'informations, voir l'article de Maurizio Tonellotto présenté dans ce même numéro de la revue.

Qu'il s'agisse de l'augmentation exponentielle des infractions *constatées*[5] par les services de police, de la professionnalisation des groupes criminels, de l'émergence de formes de cybercriminalité constituant des « menaces » graves pour les infrastructures essentielles des États et la sécurité nationale, il ne fait aucun doute que la délinquance numérique représente aujourd'hui « l'un des défis les plus complexes auxquels se heurtent les organisations policières » (Dupont, 2021, p. 55) et, de manière plus générale, les systèmes de contrôle social. Si depuis la fin des années 1990 les pouvoirs publics européens et nord-américains ont adopté plusieurs réformes visant à améliorer la prise en charge des phénomènes de cybercriminalité (introduction de nouvelles infractions, création d'unités de police spécialisées dans l'investigation numérique, mise en place de nouvelles stratégies d'enquête, etc.) (Jewkes, Yar, 2008 ; Bryant, Bryant, 2014 ; Macilotti, 2018b ; Yar, Steinmetz, 2019 ; Dupont, 2021), nombre de travaux soulignent à quel point la réponse publique en la matière s'avère encore particulièrement complexe. La sophistication croissante des conduites criminelles bénéficiant des évolutions rapides du monde numérique, les problèmes relatifs à l'augmentation exponentielle du volume des données à traiter, les difficultés des organisations et des « cultures » policières à s'adapter aux défis posés par l'environnement numérique, les problèmes de coopération internationale en matière judiciaire, sont autant d'aspects illustrant les problématiques auxquelles sont confrontés les professionnels des institutions pénales (Wall, 2007 ; Jewkes, 2012 ; Wall, Williams, 2014 ; Goodison *et al.*, 2015 ; Vincze, 2016 ; Holt *et al.*, 2015 ; Macilotti, 2018b ; Dupont, 2021 ; De Paoli *et al.*, 2021).

Il en ressort ainsi que l'évolution des criminalités numériques et les difficultés liées à la prévention et répression de ces phénomènes rendent urgente une réflexion approfondie non seulement sur la place et l'action des forces de police (voir, par exemple, Dupont, 2021), mais aussi sur l'émergence de modes de régulation faisant intervenir un ensemble plus diversifié d'intervenants (publics, privés, hybrides, voire citoyens). C'est ce que rappelait déjà en 2008 Michèle Alliot Marie, ancienne ministre française de l'Intérieur, à l'occasion d'une allocution portant sur l'amélioration des réponses aux criminalités numériques : « la lutte contre la cybercriminalité fait partie d'une chaîne, comme toute action en matière de sécurité. La police et la gendarmerie en sont des acteurs essentiels, mais ils ne sont pas les seuls »[6].

La prévention et la répression de la délinquance numérique renvoient en effet à un large éventail d'intervenants et de mécanismes de régulation, parmi lesquels un rôle non négligeable est joué par les acteurs privés de la sécurité (Wall, 2007 ; Dupont, 2016 ; Yar, Steinmetz, 2019). À partir de l'analyse de la littérature grise et des études les plus récentes sur le sujet, cet article propose alors de s'intéresser plus spécifiquement aux formes de contrôle social émanant de ce secteur, en se focalisant notamment sur les modes d'action « proactifs » visant à la collecte d'informations et à la production de renseignements. Pour ce faire, nous aborderons dans un premier temps le mouvement de pluralisation du *policing*, une notion

[5] Il n'est jamais inutile de rappeler que les statistiques produites par les services publics, que ce soit au niveau du ministère de la Justice ou de l'Intérieur, ne doivent pas être considérées comme des outils permettant de fournir une image exhaustive de l'état général de la délinquance. Elles sont avant tout les chiffres de l'activité policière ou judiciaire : une photographie à un moment donné de leurs actions en la matière (voir, notamment, Robert, Zauberman, 2011).

[6] http://www.interieur.gouv.fr/fr/Archives/Archives-de-Michele-Alliot-Marie-2007-2009/Interventions/14.02.2008-Lutte-contre-la-cybercriminalite

qui s'avère particulièrement utile pour illustrer les changements à l'œuvre dans le champ des réactions aux phénomènes de cybercriminalité (2). L'attention sera ensuite focalisée sur une méthode d'analyse de l'information, dénommée *cyber threat intelligence* (CTI), qui vise à fournir des connaissances permettant de mieux évaluer la nature et les caractéristiques des faits de cybercriminalité (3). Bien qu'elle ne soit pas limitée au secteur privé, la CTI figure parmi les principales solutions de sécurité proposées par les entreprises de cybersécurité et de services numériques. Cet outil d'aide à la décision soulève toutefois plusieurs interrogations quant à sa définition, à ses approches méthodologiques et à la portée des résultats obtenus (4).

2. La cybercriminalité et les manifestations d'un *policing* pluralisé

2.1 À propos de la pluralisation du *policing*

Le fait que différents types d'acteurs participent à la régulation des comportements déviants et délinquants ne constitue pas une nouveauté. Comme le soulignait déjà Robert Castel à la fin des années 1980, circonscrire « les régulations normativantes des comportements à l'action de l'appareil d'État » montre toutes ses limites, d'autant plus que « les formes les plus modernes de contrôle [fonctionnent] sur un mode capillaire en économisant le plus souvent la coercition directe » (1988, p. 74). L'émergence et la consolidation d'un secteur marchandisé de la sécurité (Ocqueteau, Warfman, 2011), la mobilisation de « pacificateurs indigènes » dans les quartiers populaires paupérisés (Boucher, 2015), l'émergence de services de sécurité mi-publics mi-privés dans les transports publics et dans le secteur de l'habitat social (Malochet, 2022), constituent quelques exemples du mouvement de « multilatéralisation » (Bayley, Shearing, 2001) ou de « pluralisation » du *policing* (Jones, Newburn, 1998 ; Crawford, 2008).

Globalement prise, la notion de *policing* « se réfère aux *activités*[7] qui sont déployées pour assurer la régulation sociale et à l'application des lois pénales » (Brodeur, 1995, p. 127), elle se rapporte « à toutes les activités de surveillance et de sécurisation visant à garantir la protection des personnes, des biens, et le respect des lois » (Malochet, 2022, p. 2). Le terme « pluralisation », quant à lui, a été utilisé par les spécialistes des organisations policières pour rendre compte de certaines évolutions majeures du champ du *policing*, à savoir le rôle progressivement plus important des acteurs non-policiers, et notamment de la sécurité privée (Shearing, Stenning, 1983), ainsi que la variété des organismes publics, privés et bénévoles mobilisés dans la régulation des phénomènes déviants et délinquants (Wakefield, Fleming, 2009). Ainsi définie, la pluralisation du *policing* désigne un processus caractérisé « par un partage accru de la fonction policière (…), une diversification des parties prenantes, ainsi qu'une restructuration des rapports entre le niveau central et le niveau local, la sphère publique et le secteur privé » (Malochet, 2017, p. 2). Ce « nouveau *policing* » (McLaughlin, 2007) mobilise un ensemble très diversifié d'intervenants qui présentent une grande variété de statuts, d'identités et d'« habitus » professionnels (Macilotti, Boucher, 2022).

Ce processus est particulièrement évident quand on interroge les réponses à la cybercriminalité, une notion désignant de manière générale[8] « toutes les infractions pénales tentées ou commises à

[7] Italique de l'auteur.

[8] La notion de cybercriminalité fait l'objet de plusieurs débats dans la littérature (voir notamment Bergeron *et al.*, 2020). Dans un souci de synthèse, nous employons ce terme selon la définition « pédagogique » proposée par le Groupe de travail interministériel français sur la lutte contre la cybercriminalité (Robert, 2014).

l'encontre ou au moyen d'un système d'information et de communication » (Robert, 2014, p. 12). C'est ce que rappellent notamment David Wall (1998, 2007), Yvonne Jewkes (2012), Majid Yar (2019) et Benoît Dupont (2016) lorsqu'ils montrent que la prise en charge des criminalités numériques n'est plus l'apanage exclusif des organisations policières, si tant est qu'elle l'ait jamais été. À l'instar des problèmes concernant « l'espace physique », la prévention et la répression des faits de cybercriminalité impliquent un large éventail d'acteurs qui, à différents niveaux et selon différentes modalités, interviennent dans la tentative de régulation du cyberespace.

Nous pouvons rappeler, par exemple, les initiatives citoyennes comme les *netizen* groupes ou les *cyber angels* dont l'objectif est d'améliorer la sensibilisation et la prévention en matière de criminalités numériques à travers l'implication directe des internautes[9] (voir, par exemple, Wall, 1998). Il s'agit de communautés ou plateformes en ligne, plus ou moins structurées, qui mettent à disposition différents types de contenus (guides, vidéos, *serious games*, …) portant sur les principales formes de cybercriminalité et les bons réflexes à adopter, tout en proposant des outils pour signaler des comportements illicites et pour échanger alertes, conseils et bonnes pratiques entre les usagers. La participation citoyenne à la lutte contre la cybercriminalité peut glisser parfois vers des actions revêtant un caractère punitif, comme dans le cas du vigilantisme numérique (Yar, Steinmetz, 2019). Cette pratique consiste « non seulement [à] alerter les autorités ou l'opinion publique, mais également [à] "se faire justice soi-même" en engageant des formes actives de surveillance, de répression ou de dissuasion ciblées » (Loveluck, 2016, p. 128). Le vigilantisme en ligne peut prendre différentes formes allant des groupes d'internautes qui s'organisent pour aider les forces de police à résoudre une enquête (Huey *et al.*, 2012) jusqu'aux communautés numériques qui se spécialisent dans l'identification de certains types de délinquants, comme les auteurs d'escroqueries en ligne ou d'abus sexuels à l'égard des mineurs (Yar, Steinmetz, 2019).

D'autres réponses aux criminalités numériques ont vu le jour grâce à la mobilisation d'organisations sans but lucratif en partenariat avec les acteurs du Net et les pouvoirs publics. Au Royaume-Uni, par exemple, un organisme nommé *Internet Watch Foundation* (IWT)[10] a été créé en 1996 afin d'améliorer la veille sur Internet et le retrait des contenus illicites. Il s'agit d'une organisation caritative établie par l'industrie du numérique en partenariat avec le gouvernement britannique dont l'objectif est de surveiller les échanges et les communications en ligne, tout en facilitant le signalement des faits de cybercriminalité par le biais d'une *hotline* spécifique. En France, l'Association des Prestataires de l'Internet (AFPI) a créé en 1998 la plateforme Point de Contact qui, outre à fournir des informations en matière de prévention et bonne hygiène numérique, propose un service en ligne permettant à tout internaute de notifier un contenu potentiellement illicite rencontré lors de sa navigation[11]. Des plateformes similaires ont été mises en place dans d'autres pays et peuvent être coordonnées par des organismes comme l'Internet Hotline Providers in Europe[12] (INHOPE), une organisation qui réunit une cinquantaine de *hotlines* et vise à fournir un soutien pour simplifier les procédures de notification des contenus illicites en ligne (Macilotti, 2020).

[9] https://www.cyberangels.org/

[10] https://www.iwf.org.uk/

[11] http://www.pointdecontact.net/

[12] https://www.inhope.org/EN

Au-delà des initiatives relatives à ces plateformes de signalement, les entreprises du numérique et le secteur des activités privées de sécurité jouent un rôle important dans d'autres domaines de la lutte contre la cybercriminalité. Ces acteurs peuvent collaborer directement avec les forces de police en fournissant, par exemple, des logiciels permettant d'améliorer l'analyse des données informatiques, le traitement des dossiers d'enquête ou la détection des contenus illégaux (Macilotti, 2018b). Cependant, leur contribution se concrétise en particulier à travers le développement d'une offre de biens et de services dédiés à la sécurité numérique et à la protection des données. Cela se traduit non seulement par la création de départements en charge de la sécurité des systèmes d'information au sein des entreprises, mais surtout par l'émergence de sociétés de services spécialisées en cybersécurité (Bradshaw, 2017 ; Yar, Steinmetz, 2019 ; Button, 2020), ainsi que par l'implication des industriels historiques de la défense dans la mise à disposition de solutions de sécurité pour un panel plus large de clients (D'Elia, 2015).

La régulation des faits de cybercriminalité a été également impulsée par l'action de plusieurs organisations internationales. Le Conseil de l'Europe, par exemple, a adopté le premier traité multilatéral sur le sujet : la Convention sur la Cybercriminalité (et ses protocoles) signée à Budapest le 23 novembre 2001[13]. L'ONU, quant à elle, non seulement a voté plusieurs résolutions en matière de cybersécurité, mais elle a établi des groupes d'experts gouvernementaux (GGE) chargés d'examiner les risques qui se posent ou pourraient se poser dans le cyberspace et les éventuelles mesures de coopération pour y faire face[14]. S'agissant de l'Union Européenne, un certain nombre de mesures ont été adoptées afin d'améliorer la lutte contre la cybercriminalité et la promotion d'un Internet de confiance. Cela passe également par la création de structures *ad hoc*, comme par exemple l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[15], pour renforcer la réponse communautaire en matière de cybersécurité et la coopération entre les États membres de l'UE.

Bien qu'elle se décline différemment en fonction des pays, des contextes et des périodes considérés, cette pluralisation des réponses à la cybercriminalité s'explique en raison de plusieurs facteurs.

Outre les difficultés précédemment évoquées relatives à la réponse policière, une autre raison tient à l'histoire et au développement d'Internet[16]. Depuis sa création, son fonctionnement dépend de l'intervention d'une grande variété d'acteurs et, par conséquent, sa régulation est tributaire d'une pluralité d'initiatives. Bien que des mesures législatives aient été introduites par les pouvoirs publics, elles ne constituent en effet qu'une partie des règles qui encadrent le fonctionnement du « réseau des réseaux » et les usages numériques. Les formes d'autorégulation proposées par certaines

[13] ETS 185, Convention sur la Cybercriminalité, 23 novembre 2001, disponible à l'adresse suivante : https://rm.coe.int/168008156d

[14] https://www.un.org/disarmament/fr/informatique-et-telematique/

[15] https://www.enisa.europa.eu/media/enisa-en-francais

[16] La naissance et le développement d'Internet sont le résultat de l'intervention de plusieurs acteurs : le champ de la *défense étatsunienne* qui, à la fin des années 1950, soutient le création du premier réseau d'ordinateurs interconnectés à distance (ARPANET) dans le but d'assurer les communications en cas d'attaque nucléaire ; la *communauté scientifique* américaine qui collabore avec le monde militaire pour le développement de ce premier réseau ; le milieu de la *contre-culture* des années 1960-1970 dans lequel évoluent les concepteurs d'Internet et les communautés d'informaticiens ; la tradition du *service public européen* qui a largement influencé les concepteurs du World Wide Web ; les *acteurs privés* du numérique qui ont participé au développement de la structure actuelle d'Internet grâce notamment aux solutions introduites pour la recherche et le référencement des contenus et à la création des plateformes de réseautage (Curran, 2012 ; Lallement, 2015 ; Boullier, 2016).

communautés afin de préserver les valeurs fondatrices d'Internet (libre circulation de l'information, transparence, refus de toute forme de censure et d'« interférence » étatique, etc.), les standards, les spécifications et les référentiels introduits par des organismes techniques comme l'ICANN[17], l'ISO[18] et l'IEFT[19], les codes de conduite imposés par les principales plateformes numériques, en constituent d'autres exemples (Freyssinet, 2012 ; Yar, Steinmetz, 2019).

Pour comprendre cette dynamique, il faut également l'inscrire dans le mouvement plus général de pluralisation du *policing*. À cet égard, plusieurs facteurs sont conjointement mis en avant par la littérature : les changements profonds liés à la diffusion de la « culture du contrôle » (Garland, 2001) et du « risque » (Beck, 2001), l'inflation des préoccupations sécuritaires, la remise en question de l'efficacité de l'État dans la traitement de la délinquance, la crise de légitimité des organisations policières (Malochet, 2017 ; O'Neill, Fyfe, 2017), l'émergence de nouvelles échelles d'action (au niveau local, européen, international, transnational), le contexte de crise des finances publiques, l'échec des politiques interventionnistes de l'État-providence (Lascoumes, Le Galès, 2012), les mouvements de décentralisation et de privatisation caractérisant l'action de l'État dans un vaste ensemble de domaines (Dieu, 2016).

2.2 La cybercriminalité et le secteur des activités privées de sécurité

Dans ce panorama de réponses à la cybercriminalité, un rôle non négligeable est joué par le secteur des activités privées de sécurité, notamment pour ce qui concerne l'offre de *cybersécurité*.

Si la notion de cybercriminalité renvoie aux infractions pénales commises à *l'encontre* ou au *moyen* d'un système d'information (Robert, 2014), celle de cybersécurité désigne, de manière générale[20], l'ensemble des technologies, des processus et des mesures visant à protéger les données numériques et à préserver les infrastructures servant à stocker et à transmettre ces données (voir, par exemple, ANSSI[21] ; Centre Canadien pour la Cybersécurité, 2022). En suivant cette perspective, la sécurité numérique peut être alors pensée comme l'une des activités participant à la régulation de la cybercriminalité.

Bien que le champ de la cybersécurité mobilise un large éventail d'intervenants à la fois publics et privés (Nye, 2014 ; Dupont, 2016 ; Bradshaw, 2017 ; Yar, Steinmetz, 2019), l'offre de biens et services proposés par les entreprises spécialisées dans la sécurité numérique s'avère actuellement très importante, notamment en raison du chiffre d'affaires qu'elle génère (Yar, Steinmetz, 2019 ; Button, 2020). Assurer l'intégrité, la confidentialité et le bon fonctionnement des systèmes d'information et des données, contrôler l'accès aux systèmes informatiques, protéger le contenu des données contre la manipulation, le vol et la divulgation non autorisée, accompagner les organisations dans les processus de transformation numérique, sont autant d'exemples illustrant les besoins adressés par l'offre commerciale des sociétés de cybersécurité. Cela passe par le développement d'une large gamme de solutions, telles que la conception et la fourniture de logiciels de différente nature (contrôle des accès, antivirus,

[17] *Internet Corporation for Assigned Names and Numbers*.
[18] Organisation internationale de normalisation.
[19] *Internet Engineering Task Force*.

[20] À l'instar de la notion de cybercriminalité, la conceptualisation du terme cybersécurité soulève encore plusieurs débats dans la littérature (voir, par exemple, Dupont, Whelan, 2021).
[21] Glossaire de l'ANSSI disponible à l'adresse suivante : https://www.ssi.gouv.fr/entreprise/glossaire/c/

protection des données, chiffrement des contenus et des transactions sensibles, etc.), l'élaboration de stratégies de cybersécurité et d'architectures sécurisées, la mise en conformité avec la réglementation et les référentiels de sécurité, la gestion des crise, la réponse à incident, sans oublier les activités de sensibilisation sur les criminalités numériques à destination des organisations et de leurs employés (Grabosky, Smith, 2001; Nugent, Raisinghani, 2002 ; Yar, Steinmetz, 2019).

Parmi les multiples services proposés, l'analyse des formes de cybercriminalité *considérées* comme des *menaces* à la cybersécurité constitue un domaine de plus en plus investi par ces acteurs privés, avec un chiffre d'affaires au niveau mondial qui devrait passer de 5,3 milliards de dollars en 2018 à 12,9 milliards en 2023 (Oosthoek, Doerr, 2021). L'activité porte en particulier sur l'analyse des caractéristiques et des évolutions des « cybermenaces », c'est-à-dire des conduites visant « à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient» (Centre Canadien pour la Cybersécurité, 2022, p. 2).

Puisant ses origines dans le domaine militaire et le champ du renseignement, la notion de cybermenace mérite toutefois quelques précisions car sa définition ne s'impose pas d'elle-même[22]. Plusieurs approches théoriques allant de l'interactionnisme symbolique (Becker, 1966) à la théorie sur la sécuritisation (Buzan *et al.*, 1997) en passant par la sociologie de l'action publique (Lascoumes, Le Galès, 2012 ; Neveau, 2015) montrent à quel point la définition d'une situation comme étant problématique ou menaçante ne va pas de soi, mais procède d'un travail collectif basé sur des activités concurrentielles de qualification et de mise en récit (Borraz, 2008 ; Milet, 2022).

Ainsi, la notion de cybermenace sera ici utilisée selon la signification générale qui lui est attribuée par la doctrine de sécurité française. D'après cette perspective, nous rappelle Jean-Paul Brodeur (2006), « il faut distinguer les risques qui ne sont pas le fruit d'une intention humaine – les risques naturels et matériels – et les risques, auxquels on réserve le terme de "menace", qui sont le produit d'une intention humaine malveillante » (p. 491). Selon cette approche, la notion de cybermenace renvoie donc aux risques numériques résultant d'une intention humaine malveillante et englobe notamment les actes d'espionnage (étatique ou industriel), de déstabilisation, de sabotage, ainsi que les formes de cybercriminalité susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des systèmes d'information[23]. Plusieurs travaux ont en effet souligné à quel point le panorama des menaces associées aux usages numériques a évolué au cours des quinze dernières années, le cyberespace étant tantôt utilisé à des fins d'influence et de confrontations géopolitiques, tantôt à des fins lucratives ou même de revendications sociales et politiques (pour une synthèse, Taillat *et al.*, 2018 ; Yar, Steinmetz, 2019).

C'est précisément dans ce contexte que s'inscrit le développement de nouvelles stratégies visant à améliorer la détection et le traitement des criminalités numériques à travers la mise en œuvre de modes d'action proactifs orientés vers la collecte d'informations (Wagner *et al.*, 2019 ; Basheer, Alkhab, 2021). Le référence est en particulier à la

[22] Pour une analyse plus approfondie, voir l'ouvrage de Marc Milet (2022) ; pour un approfondissement sur la notion de menace dans le contexte de la cybercriminalité et de la cybersécurité, voir l'article de Benoit Dupont et Chad Whelan (2021).

[23] Il s'agit notamment de la perspective adoptée par l'agence nationale française en charge de la cybersécurité (ANSSI) : https://www.ssi.gouv.fr/entreprise/principales-menaces/

cyber threat intelligence (CTI), une expression utilisée pour décrire à la fois un processus *et* un produit résultant de la collecte, de l'analyse et de l'interprétation de différents types de données dans l'objectif de fournir des connaissances permettant d'évaluer la nature et les caractéristiques des cybermenaces.

3. Répondre aux défis posés par la cybercriminalité : quel rôle pour la *cyber threat intelligence* ?[24]

3.1 Qu'est-ce que la *cyber threat intelligence* ?

Depuis une dizaine d'années, la *cyber threat intelligence* fait partie non seulement des stratégies d'action adoptées par les acteurs de la sécurité publique[25], mais aussi des solutions de sécurité proposées par le secteur privé. La CTI, aussi appelée « renseignement d'intérêt cyber »[26], tente d'appréhender les contours des différentes cybermenaces en les étudiant de manière globale afin de permettre une compréhension holistique du contexte dans lequel se déroule une cyberattaque donnée. Ainsi, elle peut être pensée comme une « discipline » permettant de collecter, capitaliser, contextualiser, exploiter et diffuser le renseignement relatif aux cybermenaces.

De manière générale, la *cyber threat intelligence* peut être définie comme un outil d'aide à la décision basé sur des techniques empruntées au champ du renseignement et dont l'objectif est de fournir une évaluation de la nature et des caractéristiques des menaces numériques (émergentes ou existantes). Il s'agit d'un « système d'information qui fournit des connaissances factuelles sur les cybermenaces » (Basheer, Alkhatib, 2021, p. 1) à partir d'un ensemble d'activités « de recueil, d'étude et de partage d'informations liées à des attaques informatiques » (ANSSI, en ligne)[27]. Les connaissances ainsi produites permettent de mieux comprendre les caractéristiques des cyberattaques et des modes opératoires adoptés par les auteurs, tout en fournissant des informations utiles pour la définition des mesures de sécurité les plus appropriées pour prévenir les cyberattaques et pour faire face à leurs conséquences (Friedman, Bouchard, 2015 ; Wagner *et al.*, 2019 ; Basheer, Alkhatib, 2021).

Bien que sa méthode s'inspire à des approches analytiques ayant déjà montré leur efficacité, la *cyber threat intelligence* se trouve finalement être une discipline complexe, faisant appel à des champs de compétences variées et nécessitant de faire l'objet d'une stratégie prédéfinie afin de servir son principal objectif : « disposer d'une évaluation précise et permanente de la menace cyber » (Germain, Massart, 2017, p. 57). Cette évaluation doit elle-même servir un but précis, étant celui de fournir des analyses de risques basées sur la menace étudiée et permettant de prendre des décisions face à celle-ci (Moinet, 2019). La dimension de la *finalité* est en effet au cœur de la majorité des approches développées sur le sujet. La CTI n'est jamais une fin en soi, elle ne vise pas le savoir pour le savoir : c'est

[24] Outre que par les résultats des études sur le sujet, cette partie est nourrie également par l'expérience professionnelle d'une des auteures en tant qu'analyste en *cyber threat intelligence*.

[25] En France, par exemple, un rôle fondamental en matière de CTI est joué par l'ANSSI, l'agence nationale en charge de la cybersécurité. Cet organisme publie régulièrement des rapports sur l'actualité des cybermenaces, des bulletins présentant les nouvelles vulnérabilités détectées, ainsi que des travaux de synthèse. Voir par exemple : https://www.ssi.gouv.fr/entreprise/principales-menaces/analyse-de-la-menace/

[26] Il importe toutefois de préciser que la définition du mot renseignement diffère quelque peu par rapport à celle du mot *intelligence*. Ce dernier « s'emploie dans des domaines variés comme l'économie, le commerce, l'enquête policière, etc., puisqu'il s'entend dans un sens plus étendu d'information et de système d'information ». La définition du terme renseignement est plus restreinte et renvoie généralement à la dimension « gouvernementale » ou « politique », à l'activité des services de l'État spécialisés dans la surveillance et la collecte d'informations (Chopin, Oudet, 2016, pp. 39-40).

[27] https://www.ssi.gouv.fr/entreprise/principales-menaces/analyse-de-la-menace/

une méthode d'analyse produisant une information utile à quelqu'un qui l'a demandée dans une perspective précise. Il s'agit d'un outil d'aide à la décision qui met en avant « des connaissances qualifiées et adaptées à de multiples destinataires souhaitant protéger des systèmes numériques : le niveau stratégique oriente les décideurs, le niveau opérationnel (TTPs) aide à la priorisation des projets de sécurisation alors que le niveau technique (IOCs) alimente les outils de détection et de recherche de compromission » (ANSSI, en ligne)[28].

3.2 La démarche d'analyse

Cet objectif de connaissance fine des cybermenaces se décline tout d'abord en fonction de la temporalité d'une cyberattaque :

- en amont d'une cyberattaque afin d'*anticiper* la menace cyber. La CTI est mobilisée dans l'objectif de développer des connaissances sur les outils technologiques et le type de menaces en « temps de paix » ;
- au cours d'une cyberattaque afin de *détecter* la conduite illicite et y *répondre*. La CTI est alors utilisée pour mieux identifier et catégoriser la menace ainsi que sa criticité en « temps de guerre » ;
- en aval d'une cyberattaque afin de *remédier* à l'attaque subie. La CTI est sollicitée dans l'objectif de définir les modalités pour rétablir les fonctionnalités des systèmes d'information et assurer le retour au « temps de paix ».

Ainsi, pour pouvoir être pleinement utilisée à chacune de ces temporalités, la *cyber threat intelligence* doit être pensée « en temps de paix », c'est-à-dire quand les efforts ne sont pas dirigés vers la réponse immédiate à une cyberattaque donnée. La construction de renseignement doit même être envisagée comme une stratégie sur le long-terme, passant par la création de savoir-faire et réflexes des analystes CTI (Moinet, 2019).

Cette construction, initialement réfléchie par de nombreux acteurs de la communauté cyber comme une tâche principalement technique, est aujourd'hui de plus en plus appréhendée de manière globale (Taillat *et al.*, 2018) et tend à progressivement impliquer de nouvelles disciplines. Effectivement, l'obtention d'*intelligence* pérenne et viable nécessite :

1) d'être pensée sur le long-terme par des personnes issues de formations managériales et capables de mettre en place une stratégie de collecte, exploitation et diffusion du renseignement pertinente ;
2) de faire appel à des personnes issues du monde de l'ingénierie informatique capables d'identifier et analyser les données techniques relevées sur la menace ;
3) de remettre en contexte les données techniques par des personnes issues de formations fonctionnelles telles que les études de sécurité ou les relations internationales afin d'analyser les données liées à la menace numérique en fonction du cadre dans lequel celle-ci évolue (contexte politique et géopolitique, économique et démographique, historique, social et culturel).

La conjonction de chacun de ces pans de compétences permet alors d'obtenir une évaluation fine de la menace numérique, celle-ci se basant sur un cadre d'étude complet, sollicitant l'ensemble du contexte dans lequel un évènement cyber se produit.

[28] https://www.ssi.gouv.fr/entreprise/principales-menaces/analyse-de-la-menace/

La mise en place de cette stratégie d'analyse n'est généralement pas arbitraire, mais elle s'appuie sur les éléments constitutifs d'une cyberattaque afin de cartographier l'ensemble de ce contexte. Dans cette perspective, la communauté internationale de *cyber threat intelligence* fait généralement appel à trois sources d'informations majeures : 1) celles relatives aux groupes d'attaquants, 2) celles portant sur les modes opératoires et 3) celles concernant les outils et les infrastructures d'attaques (voir, par exemple, Friedman, Bouchard, 2015).

Les *groupes d'attaquants* sont généralement classés en différentes catégories en fonction des intentions qui les animent, de leurs capacités techniques ainsi que des impacts potentiels générés par leurs attaques. La CTI cherche à caractériser le degré de sophistication et ainsi le risque que représente le groupe en lui-même. S'agissant des *modes opératoires*, l'attention est focalisée sur les stratégies adoptées par les acteurs et sur l'existence de modèles d'action récurrents, chaque groupe d'attaquants développant un schéma opératoire précis, rarement modifié au regard des habitudes que ces derniers établissent. Parmi les techniques les plus utilisées, nous pouvons rappeler la mise en place de mécanismes de persistance ou d'évasion sur le système victime ou encore l'exploitation de vulnérabilités techniques ou humaines plus ou moins rodées. L'analyse de la manière dont les acteurs organisent, exécutent et gèrent les cyberattaques est résumée par l'expression « Tactiques, Techniques et Procédures » (TTPs)[29], un terme développé par la communauté de CTI pour indiquer les « modèles d'activités et les méthodes associés à un acteur ou à un groupe d'acteurs spécifiques de la menace »[30] (Friedman, Bouchard, 2015, p. 62). L'examen de ces informations permet aux analystes de contextualiser la cyberattaque et d'appréhender le niveau de réflexion apporté à son séquencement. Enfin, l'attention est focalisée sur les *outils* et les *infrastructures d'attaques*, chaque groupe d'acteurs reposant sur un arsenal numérique plus ou moins sophistiqué et intelligemment utilisé pour mener chaque étape de leurs attaques. Généralement, ces groupes s'appuient sur des logiciels malveillants programmés pour exécuter des actions prédéfinies à chaque phase de l'attaque. Ils s'appuient également sur des infrastructures numériques, physiques ou non, afin de communiquer avec l'environnement ciblé. La CTI vient ici identifier le fonctionnement technique de ces outils et infrastructures ainsi que leur niveau de complexité.

À partir de l'analyse de ces éléments, qui par ailleurs ne relèvent pas toujours nécessairement de la sphère numérique, la CTI contribue à approfondir les connaissances sur les formes de cybercriminalité touchant les organisations tant publiques que privées. Pour ce faire, elle fait appel à une méthodologie bien connue par les services publics de sécurité et également reprise par le secteur privé : le cycle du renseignement. En effet, la *cyber threat intelligence* est plus que la simple collecte d'informations : elle couvre un panel d'activités liées entre elles.

Classiquement adopté par les institutions publiques pour mener leurs activités d'*intelligence* sur toute menace à la Nation, le cycle du renseignement consiste à réaliser en continu, et selon des besoins bien définis, des étapes permettant *in fine* de transformer une donnée en information stratégique

[29] Les TTPs sont modélisées au sein de la Matrice Mitre ATT&CK, qui correspond à une classification de l'ensemble des techniques et tactiques d'attaques utilisées par des opérateurs malveillants et dont l'enchevêtrement permet de générer des modes opératoires d'attaques associés à des groupes d'attaquants précis. Pour plus d'informations, voir https://attack.mitre.org

[30] Notre traduction : « Patterns of activities and methods associated with specific threat actors or groups of threat actors ».

(Chopin, Oudet, 2016 ; Moinet, 2019). Nous parlons alors de renseignement actionnable, c'est-à-dire d'une information dont l'analyse permet de prendre des décisions quant à la prévention ou réaction à un évènement. En effet, « le renseignement repose (...) sur l'idée que les germes de l'action future se trouvent dans la connaissance du présent et du passé » (Roubelat, 2019, p. 7).

Appliqué à la CTI, le cycle du renseignement répond au même objectif en l'adaptant à la menace évoluant au sein du cyberespace (Pech, 2019). Il s'agit donc d'étayer la connaissance disponible sur les cybermenaces afin de mieux anticiper, détecter, répondre et remédier aux actions de celles-ci. Pour se faire, les analystes CTI reposent sur les étapes classiques du cycle du renseignement, à savoir l'orientation, le recueil, le traitement, l'analyse et la dissémination[31].

L'*orientation* se matérialise par une expression de besoin d'informations, techniques ou de contexte, sur une menace donnée. Cette orientation peut évoluer à tout moment et nécessiter une adaptation des recherches effectuées (Moinet, 2019). L'étape du *recueil*, quant à elle, se base sur des activités de veille, menées au moyen de recherches ainsi que de recueil d'informations pertinentes et fiables. Cette opération est généralement effectuée par de la veille active (réalisée par l'analyste lui-même) et passive (s'appuyant sur des flux d'informations intégrés automatiquement au sein de plateformes de CTI) sur la cybermenace. Ces informations peuvent provenir de sources publiques, disponibles pour l'ensemble des utilisateurs de l'Internet en clair, comme de sources privées reposant sur la mise en place de partenariats privilégiés avec des éditeurs de cybersécurité (Pech, 2019). Dans la phase du *traitement*, il s'agit tout d'abord de capitaliser l'information recueillie au sein des plateformes de CTI d'agrégation et de management des données (Tounsi, 2019), puis de la contextualiser, notamment par la mise en perspective de celle-ci avec une multitude de facteurs techniques, opérationnels et stratégiques entourant la cybermenace. L'étape de l'*analyse* renvoie au « double processus de déstructuration (analyse) et de création (synthèse) » (Moinet, 2019, p. 17). En effet, le renseignement obtenu au moyen de l'exploitation de l'information nécessite une étude critique, partiale et stratégique, permettant *in fine* de le rendre actionnable et donc exploitable lors de la prise de décision finale, en prévention ou en réaction à une menace pesant sur les systèmes d'information. Cette étape, essentielle, permet d'évaluer les risques qu'une conduite donnée représente ainsi que ses potentiels impacts. La dernière phase, celle de la *dissémination* du renseignement, est pensée et adaptée au destinataire de celui-ci, le renseignement diffusé pouvant porter tant sur les outils techniques que sur les méthodes utilisées ou même encore sur les cibles et les impacts des faits étudiés.

Si ces étapes sont présentées ici de manière linéaire, il est à noter qu'il « s'agit bien d'un cycle puisque les renseignements ainsi obtenus permettent de réorienter les besoins et d'en découvrir de nouveaux » (Moinet, 2019, p. 14) et que tout renseignement diffusé est pensé selon l'auditoire final, la CTI se nivelant en différents versants tout aussi importants dans l'anticipation, la détection et la réaction aux menaces numériques.

[31] D'autres termes peuvent être utilisés pour indiquer les étapes du cycle du renseignement. Par exemple, le Pentagone emploie l'expression « diffusion et intégration » au lieu de « dissémination » et ajoute l'étape de l'« évaluation et feedback »; le FBI ajoute après la « dissémination » l'étape de la « demande » (voir Chopin, Oudet, 2016).

3.3 Les niveaux d'analyse

L'analyse des menaces et des incidents informatiques permet de fournir des connaissances qualifiées et adaptées à de multiples destinataires souhaitant protéger leurs systèmes d'information. Dans cette perspective, la communauté internationale de la *cyber threat intelligence* identifie trois niveaux d'analyse en fonction du public et des résultats ciblés (Abu *et al.*, 2018 ; Basheer, Alkhatib, 2021 ; Oosthoek, Doerr, 2021).

La CTI dite *stratégique* vise à orienter les décideurs. Ce premier niveau repose sur un renseignement dit de « haut niveau » et a pour but « d'aider les stratèges à comprendre les risques actuels et à identifier d'autres risques dont ils ne sont pas encore conscients » (Tounsi, 2019, p. 13). Ainsi, la CTI stratégique s'adresse principalement au personnel exécutif afin de lui fournir un panorama global sur la menace et l'orienter dans la prise de décisions opérationnelles, la gestion des ressources et des stratégies organisationnelles. Pour ce faire, elle fournit des informations concernant les groupes d'attaquants, leurs motivations, les secteurs d'activités et les zones géographiques ciblés ainsi que les impacts des opérations réalisées.

La CTI dite *opérationnelle* aide à la priorisation des projets de sécurisation. Ce second niveau, d'ores et déjà plus technique, s'attache à identifier « la manière dont les acteurs de la menace mènent leurs attaques » (Tounsi, 2019, p. 13). Elle s'appuie ainsi sur la compréhension des modes opératoires (TTPs), des logiciels malveillants et de la temporalité dans la réalisation technique de l'attaque. La CTI opérationnelle s'adresse aux dirigeants des équipes de protection afin d'orienter au mieux les stratégies de sécurité et de remédiation.

Enfin, la CTI dite *tactique* vient en appui à la détection des cyberattaques et permet de contextualiser les évènements de sécurité au moyen d'indicateurs techniques (IoCs - Indicateurs de Compromission) associés à des attaquants ou à des logiciels malveillants connus. Ce niveau de CTI intéresse généralement les analystes de détection de la menace et de réponse à incident. Prisée par la communauté cyber, la CTI tactique « est immédiatement exploitable et est plus facilement quantifiable par rapport aux autres sous-catégories de CTI » (Tounsi, 2019, p. 4).

Ces différents niveaux de CTI traduisent ainsi un besoin en renseignement de diverse nature, tantôt stratégique, méthodologique ou technique.

4. Enjeux et défis de la *cyber threat intelligence*

La *cyber threat intelligence* constitue un champ d'expertise particulièrement prometteur en raison des opportunités qu'elle offre pour le développement de solutions permettant d'améliorer la protection des systèmes d'information et la lutte contre la cybercriminalité (Wagner *et al.*, 2019 ; Basheer, Alkhatib, 2021 ; Paliotta, 2022). Au fil des années, des « communautés de pratiques » (Wenger, 1998) se sont aussi constituées autour du partage d'alertes, d'informations, de données techniques et de modèles d'analyse. Bien que selon des modalités et des temporalités différentes en fonction des contextes et des secteurs considerés, le « renseignement d'intérêt cyber » s'inscrit dans un réseau de collaborations et de configurations hybrides où interviennent des organismes publics de sécurité, des chercheurs indépendants, des analystes du secteur marchandisé de la sécurité et des entreprises de cybersécurité (Wagner *et al.*, 2019). Toutefois, un examen de la littérature et des travaux produits par la communauté elle-même permet de souligner plusieurs aspects problématiques

concernant tant les approches développées, que la portée des résultats obtenus (voir aussi Abu *et al.*, 2018 ; Basheer, Alkhatib, 2021 ; Oosthoek, Doerr, 2021).

Un premier élément concerne la notion de *cyber threat intelligence* dont la définition peut varier parfois de façon significative. Ce terme peut être en effet utilisé tantôt pour désigner le *processus* permettant d'obtenir des connaissances sur les cybermenaces, tantôt pour indiquer le *résultat* d'un tel processus d'analyse ; ou bien, il peut être mobilisé pour décrire les deux. Selon l'agence nationale française en charge de la cybersécurité, par exemple, l'« analyse de la menace, ou Cyber Threat Intelligence (CTI), implique *l'ensemble des activités*[32] de recueil, d'étude et de partage d'informations liées à des attaques informatiques » (ANSSI, en ligne)[33]. Kurt Baker, au contraire, utilise cette notion pour indiquer « les *données*[34] collectées, traitées et analysées afin de comprendre les motivations, les cibles et les stratégies de l'auteur de la menace » (2022, en ligne)[35]. Robert Lee, quant à lui, définit la CTI comme « le *processus* et le *produit*[36] résultant de la transformation des données brutes en informations répondant à une exigence spécifique, [c'est-à-dire] concernant des adversaires ayant l'intention, l'occasion et la capacité de nuire » (2016, en ligne)[37].

La CTI est donc une expression qui présente au moins deux acceptions : une acception intellectuelle (une connaissance, un savoir), une autre processuelle (l'ensemble des activités réalisées). Cela n'est pas sans rappeler les travaux sur la notion de renseignement, bien que dans ce cas il y ait également une acception institutionnelle liée à l'organisation produisant ce type de connaissances (les services de renseignement) (Chopin, Oudet, 2016).

Les approches peuvent également varier en fonction de la manière d'opérationnaliser la notion de CTI. D'après la société Gartner, par exemple, la *threat intelligence* renvoie aux « connaissances fondées sur des données probantes, y compris le contexte, les mécanismes, les indicateurs, les implications et les conseils actionnables, au sujet d'une menace existante ou émergente (…) qui peuvent être utilisées pour éclairer les décisions concernant la réponse du sujet à cette menace ou à ce danger » (McMillan, 2013, en ligne)[38]. Si cette définition met l'accent sur le type de données utilisées pour produire les connaissances, l'approche proposée par l'une des guide les plus citées en la matière insiste plutôt sur les motivations et les stratégies mises en œuvre par les acteurs malveillants : « la cyber threat intelligence est la connaissance des adversaires et de leurs motivations, intentions et méthodes qui est recueillie, analysée et diffusée afin d'aider le personnel de sécurité et les employés à tous les niveaux à protéger les actifs essentiels de l'entreprise »[39] (Friedman, Bouchard, 2015, p. 6).

[32] Notre italique.
[33] https://www.ssi.gouv.fr/entreprise/principales-menaces/analyse-de-la-menace/
[34] Notre italique.
[35] Notre traduction : « Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors », https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
[36] Notre italique.
[37] Notre traduction : « The process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm », https://www.robertmlee.org/intelligence-defined-and-its-impact-on-cyber-threat-intelligence/
[38] Notre traduction : « Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard », https://www.gartner.com/en/documents/2487216
[39] Notre traduction : « Cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise ».

Le cadre méthodologique du « renseignement d'intérêt cyber » constitue un autre domaine qui mérite d'être interrogé. Dans cette perspective, un premier aspect à aborder concerne les données utilisées dans le cadre des activités de CTI. Celles-ci sont en effet alimentées par des sources de nature variée allant des processus de détection interne aux entreprises jusqu'aux services proposés par les éditeurs de cybersécurité, en passant par les informations diffusées par les organismes publics ou partagées librement au sein des communautés de CTI (pour une synthèse Wagner *et al.*, 2019).

Cette richesse d'informations entraîne toutefois une augmentation croissante du volume de données qui nécessitent d'être traitées, contextualisées et interprétées (Friedman, Bouchard, 2015 ; Abu *et al.*, 2018 ; Oosthoek, Doerr, 2021). Cela demande une mobilisation de ressources et de compétences qui ne sont pas toujours à la portée des équipes techniques. C'est ce que révèle, par exemple, une enquête par questionnaire réalisée auprès d'un échantillon de près de 1000 professionnels du secteur de la cybersécurité : 56% des répondants déclarent que les données à traiter dans le cadre d'une stratégie de CTI sont trop volumineuses ou complexes pour pouvoir fournir des renseignements exploitables (Institut Ponemon, 2021).

Si le volume des données à analyser soulève plusieurs problèmes, l'absence et le retard de partage des contenus s'avèrent également problématiques. À cet égard, certains travaux montrent que les informations diffusées au sein de la communauté de CTI offrent des renseignements dont la valeur est parfois difficile à estimer, les données pouvant être incomplètes ou publiées des mois après la détection de la cyberattaque ou de la vulnérabilité informatique (Oosthoek, Doerr, 2021). Selon Samantha Bradshaw (2017), par exemple, l'émergence du secteur marchandisé de la cybersécurité contribue à expliquer ces aspects, la vente de certains types d'informations étant particulièrement rentable (ex. failles *zero-day*). De plus, nombre d'organisations hésitent à partager les données relatives aux faits dont elles ont été victimes en raison des dommages potentiels à leur réputation, la cyberattaque pouvant dévoiler une vulnérabilité technique ou de sécurité (Macilotti, 2019). Il ne faut pas non plus oublier que dans le cadre de la *cyber threat intelligence* sont mobilisées des données dont le partage n'est pas toujours autorisé ou est juridiquement encadré[40].

L'utilisation de données de faible qualité est un autre aspect mis en avant par les travaux sur le sujet. D'après l'étude réalisée par l'Institut Ponemon (2021), par exemple, 60% des personnes interviewées considèrent que les données dont ils disposent dans le cadre des analyses ne permettent pas d'obtenir des informations ayant valeur stratégique. Cela s'explique aussi en raison des pratiques de certains éditeurs consistant à présenter des éléments techniques, tels que les adresses IP, les noms domaine, les *hash* des fichiers, comme des renseignements. Or, la connaissance sur l'état de la menace n'est pas une information qui existe déjà à « l'état brut » : elle est toujours le résultat d'un processus délibéré de collecte, d'analyse, de contextualisation et d'interprétation d'un ensemble de données.

Un dernier aspect à souligner concerne les modèles développés par les acteurs et les plateformes de CTI pour définir et caractériser les menaces numériques. Si d'une part ces approches ont contribué à faire évoluer les méthodes d'analyse, de l'autre le manque

[40] Nous pensons, par exemple, au Règlement général sur la protection des données (RGPD, règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016) qui encadre le traitement des données personnelles sur le territoire de l'Union européenne.

de standardisation dû à l'utilisation de plusieurs modèles peut empêcher le partage des informations et l'efficacité des analyses réalisées (Abu *et al.*, 2018 ; Oosthoek, Doerr, 2021).

5. Pour conclure

Qu'il s'agisse des communautés d'internautes, des fournisseurs de services numériques, des organisations internationales, des acteurs de la sécurité privée ou du milieu associatif, la prise en charge des criminalités numériques mobilise un large éventail d'intervenants, tout en impliquant un changement d'échelle dans la mise à l'agenda et la structuration des réponses adoptées. Cette dynamique vient ainsi non seulement démentir l'hypothèse d'un déficit de régulation en matière de cybercriminalité (souvent évoqué à propos du « Far West numérique »), mais témoigne d'une nouvelle « architecture du *policing* globalisé » basée sur des assemblages hybrides de sécurité et des configurations collaboratives assez originales (Dupont, 2016, p. 96).

Un exemple à cet égard est offert par l'analyse de la littérature grise et scientifique sur la *cyber threat intelligence*. Inspirés par les approches développées par les services gouvernementaux de renseignement, les travaux sur « l'état de la menace cyber » ont contribué à l'émergence de communautés de pratiques composées d'éditeurs de solutions de cybersécurité, d'analystes du secteur marchandisé de la sécurité, de chercheurs indépendants ainsi que d'acteurs de la sécurité publique. Dans ce contexte, la CTI a contribué à une meilleure compréhension des criminalités numériques, en permettant notamment « de structurer des modélisations assez complètes des modes opératoires utilisés par les attaquants » (Salamon, 2020, p. 1615).

Toutefois, la revue des travaux sur le sujet montre à quel point le champ de la *cyber threat intelligence* est encore « dans son enfance » (Oosthoek, Doerr, 2021 p. 303). Tout d'abord, il n'existe pas de définition communément admise de la notion de CTI, les acteurs tendant à la définir en fonction de leur domaine d'expertise et de leur environnement de travail (voir aussi Abu *et al.*, 2018). De plus, plusieurs problèmes d'ordre méthodologique émergent lorsque l'on interroge les approches développées en la matière. C'est ainsi que certains auteurs affirment que « la CTI est un produit sans processus » (Oosthoek, Doerr, 2021 p. 302), en référence notamment aux problèmes liés à la nature des données utilisées, aux conceptualisations de qualité variable et à l'absence de standardisation.

Malgré ces difficultés, le « renseignement d'intérêt cyber » est un domaine émergent qui présente un potentiel significatif pour la protection des systèmes d'information et les réponses, tant publiques que privées, à la cybercriminalité. C'est notamment ce que souligne l'étude de l'Institut Ponemon (2021) précédemment citée : 79% des professionnels interviewés affirment que la CTI est « essentielle pour obtenir une posture de cybersécurité solide » (p. 1). Il s'agit d'une perspective partagée également par plusieurs organismes de sécurité numérique, tels que l'ENISA[41] au niveau européen ou l'ANSSI en France, qui sont par ailleurs particulièrement mobilisés dans la mise en œuvre de solutions[42] visant à mieux structurer les informations relatives aux cybermenaces et à répondre aux principaux problèmes méthodologiques existants.

[41] Depuis plus de 10 ans, l'ENISA est un acteur central dans l'évaluation des cybermenaces et des activités de CTI : https://www.enisa.europa.eu/topics/cyber-threats

[42] Nous rappelons, par exemple, le projet OpenCTI (Open Cyber Threat Intelligence) développé par l'ANSSI en partenariat avec le CERT-EU : https://www.ssi.gouv.fr/actualite/opencti-la-solution-libre-pour-traiter-et-partager-la-connaissance-de-la-cybermenace/

Références

1. Abu S., Selamat S. R., Ariffin A., Robiah Yusof R., « Cyber Threat Intelligence – Issue and Challenges », *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, n. 1, 2018, pp. 371-379.
2. Basheer R., Alkhatib B., « Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence », *Journal of Computer Networks and Communications*, ID 1302999, 2021, pp. 1-21.
3. Bayley D., Shearing C., *The New Structure of Policing*, National Institute of Justice, Washington, 2001.
4. Beck U., *La société du risque*, Aubier, Paris, 2001.
5. Becker H., *Social Problems: A Modern Approach*. New York: John Wyler, New York, 1966.
6. Bell D. (1976), *The coming of the post-industrial society: a venture in social forecasting*, Basic Books, New York, 1976.
7. Bergeron A., Pamar M., Paquette S., « Introduction et définitions de la cybercriminalité », in Fortin F., *Cybercrimes et enjeux technologiques*, Presses internationales Polytechnique, Montréal, 2020, pp. 1-20.
8. Borraz O., *Les politiques du risque*, Presses de Sciences Po, Paris, 2008
9. Boucher M., *Sociologie des turbulences. Penser les désordres des inégalités*, Paris, L'Harmattan, 2015.
10. Boullier D., *Sociologie du numérique*, Armand Colin, Paris, 2016.
11. Bradshaw S., « Combatting cyber threats: CSIRTS and fostering international cooperation on cyber security », in Global Commission on Internet Governance, *Cybersecrutiy in a volatile world*, Centre for International Governance Innovation, 2017, disponible à l'adresse : https://www.jstor.org/stable/resrep05239.13
12. Brodeur J.-P., « Le contrôle social : privatisation et technocratie », in *Déviance et Société*, vol. 19, n. 2, 1995, pp. 127-147.
13. Brodeur J.-P., « Le risque et la menace », *Canadian Journal of Criminology and Criminal Justice*, vol. 48, n. 3, 2006, pp. 491-498.
14. Brun P., Denécé É., *Renseignement et espionnage pendant l'Antiquité et le Moyen-Âge*, Ellipses, Paris, 2019.
15. Burrus G., Howell C. J., Bossler A., Holt T., « Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: a latent class analysis », *Policing: An International Journal*, vol. 43, n. 1, 2019, pp. 105-119.
16. Button M. « The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions », *Journal of Contemporary Criminal Justice*, vol. 36, n. 1, 2020, pp. 39-55.
17. Buzan B., Weaver O., De Wilde J., *Security : A New Framework for Analysis,* Lynne Rienner Publishers, London, 1997.
18. Castel R., « De l'intégration sociale a l'éclatement du social : l'émergence, l'apogée et le départ à la retraite du contrôle social », in *International Review of Community Development / Revue Internationale d'Action Communautaire*, n. 20, 1988, pp. 67-78.
19. Castells M, *La société en réseaux*, Fayard, Paris, 2001(1ère édition originale 1996).
20. Chopin O., Oudet B., *Renseignement et sécurité*, Armand Colin, Paris, 2016.
21. Côté A. M., Bérubé M., Dupont B., « Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité », *Réseaux*, vol. 3., n. 197-198, 2016 p. 203-224.
22. Crawford A., « The pattern of policing in the UK: policing beyond the police », Newburn T. *The handbook of policing*, Willan, Cullompton, 2008, pp. 147-182.
23. Curran J., « Reinterpreting Internet history », in Jewkes Y., Yar M. (ed.), *Handbook of Internet crime*, Willan, Cullompton, 2012, pp. 17-37.
24. D'Elia D., « La cybersécurité : de la représentation d'un bien public à la nécessité d'une offre souveraine », *Sécurité et stratégie*, vol. 19, n. 2, 2015, pp. 72-80.
25. De Paoli S., Johnstone J., Coull N., Ferguson I., Sinclair G., Tomkins P., Brown M., Martin R., « A Qualitative

Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists », *Policing: A Journal of Policy and Practice*, vol. 15, n. 2, 2021, pp. 1429-1445.
26. Décary-Hétu D., Bérubé M. (dir.), *Délinquance et innovation*, Presses de l'Université de Montréal, Montréal, 2018.
27. Dieu F., *Réponses à la délinquance*, L'Harmattan, Paris, 2016.
28. Dupont B., « La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale », in *Cultures & Conflits*, n. 102, 2016, p. 95-120.
29. Dupont B., « La police et la prévention de la cybercriminalité », in Amicelle A., Boivin R., Dupont B., Fortin F., Tanner S., *L'avenir du travail* policier, Les Presses de l'Université de Montréal – Édition Kindle, Montréal, 2021, pp. 50-93.
30. Dupont B., Whelan C., « Enhancing relationships between criminology and cybersecurity », *Journal of Criminology*, vol. 54, n. 1, 2021, pp. 1-17.
31. Fortin F. (dir.), *Cybercrimes et enjeux technologiques*, Presses internationales Polytechnique, Montréal, 2020.
32. Freyssinet E., *La cybercriminalité en mouvement*, Hermes, Paris, 2012.
33. Friedman J., Bouchard M., *Definitive guide to cyber threat intelligence*, CyberEdge, Annapolis, 2015.
34. Garland D., *The Culture of Control*, Oxford University Press, Oxford, 2001.
35. Germain G., Massart P., « Souveraineté Numérique », *Études*, vol. 10, n. 10, 2017, pp. 45-58
36. Gill P., Phythian M., *Intelligence in an Insecure World*, Polity Press, Malden, 2012.
37. Goodison S., Davis R., Jackson B., *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, RAND Corporation, Santa Monica, 2015.
38. Grabosky P., Smith R., « Telecommunication fraud in the digital age: The convergence of technologies », in Wall D. S. (dir.), *Crime and the Internet*, Routledge, London, 2001, pp. 29-43.
39. Holt T., Burruss G., Bossler A., *Policing Cybercrime and Cyberterror*, Carolina Academic Press, Durham, 2015.
40. Huey L., Nhan J., Broll R., « 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime », *Criminology & Criminal Justice*, vol. 13 n. 1, 2012, p. 81-97.
41. Jewkes Y., Yar M., « Policing cybercrime: emerging trends and future challenges », in Newburn T., *Handbook of policing*, Willan, Cullompton, 2008, pp. 580-605.
42. Jewkes, Y., « Public policing and internet crime », in Jewkes Y., Yar M. (dir.), *Handbook of Internet Crime*, Routledge, Oxon, 2012, pp. 525-545.
43. Jones T., Newburn, T., *Private security and public policing*, Clarendon Press, Oxford, 1998.
44. Lallement M., *L'Âge du faire. Hacking, travail, anarchie*, Seuil, Paris, 2015.
45. Lascoumes P., Le Galès P., *Sociologie de l'action publique*, Armand Colin, Paris, 2012.
46. Levi M., Doig A., Gundur R., Wall D., Williams M., *The Implications of Economic Cybercrime for Policing*, City of London Police, London, 2015.
47. Loveluck B., « Le vigilantisme numérique, entre dénonciation et sanction. Auto-justice en ligne et agencements de la visibilité », *Politix*, vol. 115, n. 3, 2016, pp. 127-153.
48. Macilotti G., « Studiare la cybercriminalità: alcune riflessioni metodologiche », *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. 12, n. 1, 2018a, pp. 51-80.
49. Macilotti G., *Pedopornografia e tecnologie dell'informazione. Devianza e controllo sociale nella realtà italiana e francese*, FrancoAngeli, Milano, 2018b.
50. Macilotti G., « Cybercriminalità », in Balloni A., Bisi R., Sette R. (dir.), *Criminologia applicata. Criminalità, controllo, sicurezza*, Wolters Kluwer-Cedam, Milano, 2019, pp. 311-350.
51. Macilotti G., « Online Child Pornography: Conceptual Issues and Law Enforcement Challenges », in Balloni A., Sette R. (dir.), *Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim*

Support, IGI Global, Hershey, PA, 2020, pp. 226-247.
52. Macilotti G., Boucher M., dossier *Les professionnels de la déviance et de la délinquance : quels enjeux d'hybridation ? Pratiques des acteurs, lieux d'intervention et logiques professionnelles*, *Sciences & Actions Sociales*, vol. 16, n. 1, 2022, pp. 1-14.
53. Malochet V., « Contours et positionnement d'une forme hybride de policing résidentiel », in *Champ pénal/Penal field* [En ligne], vol. 14, 2017, pp. 1-2.
54. Malochet V., « La pluralisation du policing en France. Logiques d'hybridation, effets de tropisme et enjeux d'articulation », *Sciences & Actions Sociales*, vol. 16, n. 1, 2022, pp. 53-67.
55. McLaughlin E., *The new policing*, Sage, London, 2007.
56. Milet M., *Sociologie politique de la menace et du risque*, Armand Colin – Édition Kindle, Paris, 2022.
57. Moinet N., « Le renseignement au prisme du couple agilité-paralysie », *Prospective et stratégie*, vol. 10, n. 1, 2019, pp. 13-27.
58. Neveu E., *Sociologie politique des problèmes publics*, Armand Colin, Paris, 2015.
59. Nugent J., Raisinghani M., « The information technology and telecommunications security imperative: Important issues and drivers », *Journal of Electronic Commerce Research*, vol. 3, n. 1, 2002, pp. 1-14.
60. Nye J., *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance, Paper Series No. 1., Waterloo, 2014.
61. O'Neill M., Fyfe N. R., « Plural policing in Europe: relationships and governance in contemporary security systems », *Policing and Society*, v. 27, n. 1, 2017, pp. 1-5.
62. Ocqueteau F., Warfman D. (2011), *La sécurité privée en France*, Paris, Puf, 2011.
63. Oosthoek K., Doerr C. (2021), « Cyber Threat Intelligence: A Product Without a Process? », *International Journal of Intelligence and CounterIntelligence*, vol. 34, n. 2, 2021, pp. 300-315.
64. Paliotta A. P., « Una riflessione preliminare sul processo di Istituzionalizzazione della Cyber Intelligence », *Quaderni di Cyber Intelligence*, vol. 1, 2022, pp. 10-20.
65. Pech Y., « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère », *Prospective et stratégie*, vol. 10, n. 1, 2019, pp. 73-102.
66. Ponemon Institute, *The State of Threat Feed Effectiveness in the United States and United Kingdom*, Ponemon Institute Research Report, 2021.
67. Robert M., *Rapport sur la cybercriminalité*, Groupe de travail interministériel sur la lutte contre la cybercriminalité, 2014.
68. Robert P., Zauberman R., *Mesurer la délinquance*, Presses de Sciences-Po, Paris, 2011.
69. Roubelat F., « Anticipation et renseignement », *Prospective et stratégie*, vol. 10, n. 1, 2019, pp. 7-11.
70. Salamon Y., *Cybersécurité et cyberdéfense : enjeux stratégiques*, Ellipses – Édition Kindle, Paris, 2020.
71. Shearing C. D., Stennin P. C., « Private security: Implications for social control », *Social Problems*, vol. 30, n. 5, 1983, pp.493–506.
72. Taillat S., Cattaruzza A., Danet D., *La cyberdéfense. Politique de l'espace numérique*, Armand Colin, Paris, 2018.
73. Tounsi W., *Cybervigilance et confiance numérique: la cybersécurité à l'ère du Cloud et des objets connectés*, ISTE, Paris, 2019.
74. Vincze E. A., « Challenges in digital forensics », *Police Practice and Research*, vol. 17, n. 2, 2016, pp. 183-194.
75. Wagner D., Mahbub K., Palomar E., Abdallah A. E., « Cyber threat intelligence sharing: Survey and research directions », Computers & Security, vol. 87, 2019, 101589.
76. Wakefield A., Fleming J., *The SAGE Dictionary of Policing*, Sage, London, 2009.
77. Wall D. S (dir.), *Crime and the Internet*, Routledge, New York, 2001.
78. Wall D. S., « Catching Cybercriminals: Policing the Internet », *International Review of Law Compurters & Technology*, vol. 12, n. 2, 1998, pp. 201-218.
79. Wall D. S., « Policing cybercrimes: situating the public police in networks of security

within cyberspace », *Police Practice and Research: An International Journal*, vol. 8, n. 2, 2007, pp. 183-205.
80. Wenger E., *Communities of Practice: Learning, Meaning, and Identity*, Cambridge University Press, Cambridge, 1998.
81. Yar M., Steinmetz K. F., *Cybercrime and Society*, Sage – Kindle Edition, London, 2019.

Sitographie

1. ANSSI, *État de la menace rançongiciel à l'encontre des entreprises et des institution*s, 2021, disponible à l'adresse suivante : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf
2. ANSSI, *Panorama de la menace informatique 2021*, 2022, disponible à l'adresse suivante : https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf
3. Baker K., *What is cyber threat intelligence ?*, disponible à l'adresse suivante : https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
4. Centre Canadien pour la Cybersécurité, *Introduction à l'environnement de cybermenace*, Centre de la sécurité des télécommunications, Ottawa, 2022, disponible à l'adresse suivante : https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces
5. IC3, *Federal Bureau of Investigation Internet crime report 2021*, 2022, disponible à l'adresse suivante : https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
6. Lee R. M., *Intelligence Defined and its Impact on Cyber Threat Intelligence*, disponible à l'adresse suivante : https://www.robertmlee.org/intelligence-defined-and-its-impact-on-cyber-threat-intelligence/
7. Polizia Postale e delle Comunicazioni, *Resoconto attività - Polizia Postale e delle Comunicazioni Anno 2020*, 2021, disponible à l'adresse suivante : https://questure.poliziadistato.it/statics/29/5.01.2021--allegato-al-consuntivo-2020--attivita-polizia-postale.pdf?lang=it
8. Polizia Postale e delle Comunicazioni, *Resoconto attività - Polizia Postale e delle Comunicazioni Anno 2021*, 2022, disponible à l'adresse suivante : https://questure.poliziadistato.it/statics/46/resoconto-attivita-polposta-2021-e-calabria.pdf?lang=it

doi: 10.14664/rcvs/246

Età e criminalità: approcci empirici e teorici dell'esordio criminale in età adulta

Âge et crime : approches empiriques et théoriques de l'engagement criminel à l'âge adulte

Age and crime: Empirical and theoretical approaches of criminal adult onset

Eleni Kontopoulou *

Riassunto
Secondo la curva età-delinquenza, la prevalenza della criminalità presenta un aumento nel periodo di transizione dall'infanzia all'adolescenza, un picco verso la fine dell'adolescenza e un calo durante l'età adulta. In questo contesto, il più alto tasso di desistenza è osservato verso la fine dell'adolescenza e l'inizio dell'età adulta, indipendentemente dal momento dell'insorgenza del comportamento antisociale o criminale. Tuttavia, l'esperienza di ricerca ha evidenziato l'esistenza di delinquenti che sembrano compiere attività criminali per la prima volta durante l'età adulta. La presente analisi si focalizza sui dati empirici relativi alle dimensioni del fenomeno e ai fattori associati al suo verificarsi. Al contempo, si farà particolare riferimento agli approcci teorici in materia nel tentativo d'identificare il processo che ha come punto di partenza la minore età e che, durante il periodo di transizione all'età adulta, porta all'esordio e alla carriera criminale.

Résumé
Selon la courbe âge-délinquance, la prévalence de la criminalité présente une augmentation à la période de transition de l'enfance à l'adolescence, un pic vers la fin de l'adolescence et une baisse lors de l'âge adulte. Dans ce contexte, le taux le plus élevé de désistance du crime est observé vers la fin de l'adolescence et le début de l'âge adulte, quel que soit le moment d'apparition du comportement antisocial ou criminel. Néanmoins, les recherches ont mis en évidence les cas de délinquants qui commettent un crime (pour la première fois) à l'âge adulte. La présente analyse se focalise sur les travaux de recherche portant sur les dimensions du phénomène ainsi que sur les facteurs associés à son apparition. Une référence particulière sera faite aux approches théoriques sur le sujet pour tenter d'identifier le processus qui a comme point de départ la minorité d'âge et qui, pendant la période de transition à l'âge adulte, conduit au comportement criminel et à la carrière criminelle.

Abstract
According to the age-crime curve, prevalence in crime displays an increase over the period from the late childhood to adolescence, a peak towards the end of adolescence and a downward trend afterwards during adulthood. In this context, the highest rate of desistance is observed towards the end of adolescence and the beginning of adulthood regardless of the time of antisocial or criminal onset. However, research experience has highlighted the existence of offenders who appear to engage in crime for the first-time during adulthood. The present analysis focuses on the empirical experience regarding the dimensions of the phenomenon as well as the factors associated with its occurrence. At the same time, particular reference will be made to the theoretical approaches to the phenomenon in an attempt to identify the process whose starting point is placed in minority and, during the period of transition to adulthood, leads to criminal onset and a criminal career.

Key words: age, crime, adult criminal onset, criminal careers

* Eleni Kontopoulou: PhD Criminologist, Panteion University of Social and Political Sciences, Athens-Greece, ORCID https://orcid.org/0000-0003-0461-9073.

1. Introduction

The first reference to the relationship between age and crime is attributed to the Belgian mathematician and statistician Quetelet in 1831 who, studying statistical data on crimes against persons and property, found that crime peaked towards the end of adolescence up to mid-twenties (Piquero *et al.*, 2003, p. 360; Zarafonitou, 2004, p. 85). The background for further systematic study of this relationship was laid by the classic research by the Gluecks Unraveling Juvenile Delinquency (1950) and the cohort study of Wolfgang, Figlio and Sellin (1972) entitled Delinquency in a birth cohort which was a milestone and gave rise to the establishment of the first National Academy of Sciences Panel on Criminal Careers and the development of the so-called criminal career paradigm[1] (Piquero et al., 2007, p. 2). Within the positivist approach of this paradigm, criminal career was defined as the «longitudinal sequence of offenses committed by an offender who has a detectable rate of offending during some period» (Blumstein *et al.*, 1988, p. 2)[2] and a series of questions were posed for investigation regarding both the onset and continuity of offending behaviour and the desistance and termination of criminal activity[3]. The criminal career paradigm created the necessary background for the development of the so-called Developmental/Life Course Criminology[4] in which the risk factors[5], the protective factors[6] and the life events[7], that have an impact on the configuration of the various dimensions[8] during a criminal career at different age stages with an emphasis on the onset, continuation and desistance[9] from crime, are being examined.

On this basis, a range of dynamic/developmental theories[10] has been deployed concerning the phenomenon of criminal careers (Farrington, 2003; Thornberry, Krohn 2001; Moffitt, 1993; Sampson, Laub, 1993; Le Blanc, 1997). According to a well-established standpoint of Developmental Criminology as it has been elaborated according to the research experience so far regarding the study of the relationship between age and crime, it has been stated that the criminal onset is placed between the ages of 8 and 14, while the age at which desistance from crime is observed, is placed between 20 and 29

[1] The criminal career paradigm was particularly developed in the 1980s, focusing on the study of the individual dimensions of criminal careers. However, as Farrington states, it was characterised as a paradigm without a theoretical foundation around issues relating to the development of offending behaviour over time, the role of risk factors and life events (Farrington, 2003, p. 222).

[2] According to Farrington, the paradigm approach of criminal careers allows for a quantitative measurement of the phenomenon through statistical methods of analysis (Farrington, 1987, p. 59 as cited in Ulmer, Spenser, 1999, p. 97).

[3] In this light, the individual dimensions of a criminal career seem to be related to different causal risk factors as Ulmer and Spencer (1999, p. 97), typically mention. See also Blumstein, et al., 1988, p. 4.

[4] Farrington (2003, p. 221) states: «Developmental and Life Course Criminology is especially concerned with documenting and explaining within-individual changes in offending throughout life. It is a further elaboration of the criminal career paradigm that became very prominent in the 1980s by adding in the study of risk factors and life events (…) To some extent DLC theories were a reaction to what was perceived as a largely atheoretical criminal career paradigm».

[5] By risk factor is meant «a variable that predicts a high probability of offending» (Zara, Farrington, 2016, p. 53; Morizot, Kazemian, 2015).

[6] Protective factors are defined as those factors which «reduce the likelihood of problem behavior either directly or by mediating or moderating the effect of exposure to risk factors» (Arthur et al. 2002. p. 576; Morizot, Kazemian, 2015).

[7] On life events or life circumstances see Zarafonitou, 2004, p. 95 and Laub, Sampson, 2001. Regarding the effect of life circumstances (e.g. romantic relationships, marriage, employment, parenthood) on the development of criminal trajectories during the transition time period from adolescence to early adulthood see Horney et al., 2012.

[8] The several dimensions of criminal careers refer to elements such as: prevalence, offending frequency, specialization, escalation, co-offending, persistence/continuity, adult-onset etc. (Piquero et al., 2012, p.14; Piquero et al., 2007).

[9] For the definition of desistance, the methodological issues that arise when measuring it and the research and theoretical approaches see Laub, Sampson, 2001.

[10] As Piquero et al. (2007, p.2) mention, developmental and life course theories were developed in order to provide a theoretical foundation for the criminal career paradigm.

years of age[11]. Meanwhile, prevalence[12] appears to undergo a peak near the late adolescence, specifically during the 15-19 age period (Piquero *et al.*, 2007, p. 3). In general, according to international research experience, prevalence in criminal activity[13] shows an increase over the period from the late childhood to adolescence, a peak towards the end of adolescence and a downward trend afterwards during adulthood. The above empirical finding captures what is called the negative age-crime curve (Loeber, Farrington, 2012, p. 5; Piquero *et al.*, 2007, p. 7; Laub, Sampson, 2003). The negative age-crime curve has been observed to hold regardless of the historical period in which the criminal phenomenon is examined, the composition of the sample under scrutiny, the type of data source and the type of antisocial or criminal behaviour investigated (DeLisi, 2015, p. 51). On this basis, Hirschi and Gottfredson (1983) argued for a relationship that is fixed and uncorrelated with other demographic factors. However, proponents of the criminal career paradigm were the first to challenge this view (DeLisi, 2015, p. 52) while Farrington (1986), criticising the above fixed and unchanging relationship hypothesis, argued that the age-crime curve may vary at the individual level compared to the aggregate level. Indeed, research evidence has demonstrated that while at the aggregate level the age-crime curve remains the same regardless of the historical study period and data source, however, at the individual level the pattern of criminal activity appears to vary, with a number of factors co-shaping this variation (DeLisi, 2015, p. 59)[14].

In this respect, it should be noted that early antisocial or criminal onset is a predictor of a long criminal course and of the commission of many crimes. Moreover, it is generally accepted that there is a 'continuity' of antisocial and delinquent behaviour over time from childhood to adolescence and then into adulthood (Farrington, 2003, p. 223; Piquero et al., 2007, p. 3). However, it should be noted that the majority of juveniles who adopt antisocial behaviour[15] in adolescence do not display the same behaviour in adulthood (Robins, 1978) and the association between early antisocial or criminal onset and the engagement in antisocial behaviour in adulthood appears to arise on the basis of a rather retrospective processing of data than future prediction (Zara, Farrington, 2016, p. 53 & 58). The above finding is consistent with the fact that the highest rate of desistance is observed

[11]With the exception of so-called chronic offenders. Chronic offenders (life-course persistence offenders according to Moffitt's classification) are a small group of offenders, representing 5-8 % of the population, perpetrating a high percentage of crimes committed and is involved in an increased number of anti-social and violent acts. However, within the context of a respective research design, operational definitions may vary. Zarafonitou (2004, p. 89) mentions the term 'professional' criminals who «commit a consistently large number of offenses over a much longer period of time and therefore manifest a behaviour 'contrary to the overall negative age/crime relationship», (Our translation). See in this regard Zara, Farrington, 2016, p. 32,49 & 58-64; Moffitt, 1993; DeLisi et. al., 2014.

[12]As Rhodes (1989, p. 3) states prevalence «is a population statistic showing the percentage of people who commit at least one crime during a stipulated period».

[13] Prevalence should be distinguished from the term frequency which reflects an average annual (individual) crime rate denoted by the Greek letter λ (lambda) (Blumstein et al.,1988, p. 3). In this context, concern has been raised as to whether the curve depicting the relationship between age and crime at an aggregate level reflects the function of prevalence or frequency and, by extension, whether it is possible to draw firm conclusions at the individual level on the basis of data that are referred to an aggregate level. Piquero et al. (2007, p. 7-8) state: «Is the peak in the age/crime curve a function of active offenders committing more crime, or is it a function of more individuals actively offending during those peak years and fewer during the later years? (...) to what extent is the slowing of offending past the peak age a function of deceleration in continued criminal activity or stopping by some people?». For the above issue see also Gottfredson, Hirschi, 1986.

[14] It should be noted that the age-crime curve may also vary according to the type of criminal offence (e.g. the curve for crimes against property seems to peak at an earlier time compared to the curve for violent crimes), gender (the curve seems to peak earlier for males than for females) and the type of data (the curve for criminal offences reported on the basis of self-reported data seems to peak earlier than the curve formed on the basis of data from official records) (Loeber et al., 2012, p. 317).

[15]Delinquent behaviour is a manifestation of a broader syndrome of anti-social behaviour (Farrington, 2003, p. 224).

towards the end of adolescence and the beginning of adulthood regardless of the time of antisocial or criminal onset (Loeber, Farrington, 2012, p. 5).

As already mentioned, the age-crime curve places the onset of delinquent behaviour during the period of minority, however, research has highlighted the existence of offenders who appear to engage in delinquency for the first-time during adulthood (Piquero *et al.*, 2012, p. 25). Therefore, it becomes of particular interest to empirically investigate both the dimensions of the phenomenon and those factors that function protectively during minority as well as those that increase the likelihood for someone to engage in delinquent behavior during the transition from minority to adulthood (Thornberry *et al.*, 2012, p. 48). Research experience to date, however, around the existence of this particular pattern of criminal trajectory remains limited and, according to some researchers, this phenomenon is extremely rare (Moffitt *et al.*, 2001). The absence of research data and the perception of rarity of the phenomenon seems to have equally affected any attempts to theorise it as scientific interest around the development of an explanatory framework remains limited (Thornberry *et al.*, 2012). In this context, the present analysis will report on the available empirical evidence around the phenomenon focusing on both the issue of its dimensions and the factors associated with its occurrence. At the same time, particular reference will be made to the theoretical approaches to the phenomenon in an attempt to identify that evolutionary process which has as its starting point minority and, during the period of transition to adulthood, leads to the onset of delinquency and a criminal career.

2. Research experience on the dimensions and risk factors of adult criminal onset

Gomez-Smith and Piquero (2005, p. 515) mention that the established argument that the criminal onset is placed in the juvenile period is due to the high prevalence of adolescent offenders in crime as well as to the aggregate level of the age-crime curve, resulting in the prevailing view that the frequency in which the criminal onset is observed in adulthood is relatively rare or negligible[16]. However, in 1986 Blumstein and his colleagues argued that 4-5 out of 10 adult offenders have no history of involvement in delinquency during the juvenile years. In particular, it was found that 40-50% of adult offenders had no history of contact with police during minority (Piquero *et al.*, 2012, p. 25). Similar high rates appear to occur in the female population of adult offenders as demonstrated by Swedish longitudinal empirical studies (Eggleston, Laub, 2002, p. 614). For example, in a representative sample of the Swedish population (709 males and 680 females) which was surveyed from age 10 to age 30, it was found that 54. 2% of adult male offenders had engaged in criminal behaviour for the first-time during adulthood while the corresponding rate for females was as high as 79.3% (Magnusson, 1988 as cited in Eggleston, Laub, 2002, p. 617). In the same study it was found that 1 in 4 males in the sample became involved in the criminal justice system by receiving a criminal conviction for the first time after the age of 20. In fact, it is worth mentioning that for the females in the sample the peak age point for the criminal onset was placed at a later time compared to males, namely in the age period 21-23 years of age[17] (Stattin *et al.*, 1989, p. 373, 379).

[16] Related to this is Moffitt's consistent claim that offenders rarely start their criminal activity as adults. Cf. Moffit, 1993.
[17] For the males in the sample, the peak age was 15-17 years.

Wolfgang et al. (1987) in a follow-up research on the sample of the cohort study Delinquency in a Birth Cohort concluded that 24.2% of all individuals in the sample who had committed a criminal offence and had been arrested, were individuals who had begun their criminal activity in adulthood with no previous history of involvement in committing a criminal offence during minority. In the same vein, Eggleston and Laub (2002) concluded that the criminal onset in adulthood is not a rare phenomenon (Koppen, 2018, p. 93).

At this point it should be emphasised that longitudinal researches in which the existence of adult offenders, who do not have a history of criminal behaviour during their juvenile years, has been established, mainly use data from the investigation of the records of police arrests or criminal convictions (Eggleston, Laub, 2002, p. 603; Piquero *et al.*, 2012, p. 27; Kirk 2006). Under this foundation, it is argued that the phenomenon of criminal onset in adulthood is an outcome of the use of official data reflecting the reporting process by the criminal justice system (McGee, Farrington, 2010, p. 530). The above statement raises the reasonable question as to whether persons who are recorded as initiating their criminal activity in adulthood may have exhibited involvement in criminality during their minority for which, however, they never came into contact with the criminal justice system (Piquero *et al.*, 2012, p. 27). In the context of such a conclusion, the different per research design conceptualisation and operationalisation of 'adult onset' with reference to the age at which this onset[18] is placed, should be also taken into account.

Motivated by the above reasonable concern, McGee and Farrington (2010) raised the question of the reasons why an individual may engage in criminal behaviour while underage without being noticed by the institutions of the criminal justice system. In the framework of the Longitudinal Prospective Study Cambridge Study in Delinquent Development[19] the above research question was investigated. In this study, the time point for the criminal onset in adulthood was set at 21 years of age[20]. Of the total sample (404 males) 167 males had been involved in committing crimes up to the age of 50. Of the total of 167 individuals, only 23% (38 individuals) began criminal activity at the age of 21 or older based on criminal conviction history. As McGee and Farrington report the percentage identified within the survey is lower than the corresponding percentage which has been identified within other research and this could be due to the age criterion of 21 years and above as most of the surveys adopt a lower age threshold (18 years) for timing the criminal onset in adulthood. As they point out, «as men age, there is less likelihood of being detected by the criminal justice system for a first offense and first-time offenders decrease dramatically after age 20 and are very sparse from age 36 onwards» (McGee, Farrington, 2010, p. 537). In order to answer the question of whether these offenders started offending in adulthood or earlier without ever being detected by the criminal justice system,

[18] Most relevant research places adult onset at 18 years of age (McGee, Farrington, 2010, p. 533).

[19] For details of this research see Zara, Farrington, 2016 and Farrington et al., 2013. This is a longitudinal prospective study of a sample of 411 males living in a working-class area of South London with a starting point of 1961-1962. The majority of the males were born in 1953. At the age of 18 years the sample participation rate in the interviews was close to 95%, at the age of 32 years 94% and at the age of 48 years 93%. Of the total of 404 individuals (final sample), 167 were involved in committing a crime at some point in their lives. Taking criminal conviction as a measure, offending appears to peak at 17 years of age and of the total number of offenders, 70.7% were recidivists (118 people).

[20] In England, the categorisation is as follows: juvenile offenders aged 10-17 years, young adults aged 18-20 years and adults aged 21 years and older who are subject to more severe criminal treatment. Cf. McGee, Farrington, 2010, p. 534.

possible offending before the age of 21 was investigated on the grounds of self-reported data. According to the survey data, a rate of 30% of individuals (11 individuals) who had initiated engagement in offending activity from 21 years onwards reported high levels of offending involvement in minority (McGee, Farrington, 2010, p. 540). Along the same lines, the mean for self-reported offending in minority was examined between those who first became involved in offending (based on criminal conviction history) from age 21 onwards and those who were already involved in offending in minority (based on criminal conviction history). Although those who had already engaged in offending as juveniles had a higher mean, a group of 7 persons with criminal onset from the age of 21 onwards was identified which had a higher mean at the age of 14 and a corresponding group of 5 persons with a higher mean at the age of 18[21] (McGee, Farrington, 2010, p. 541). In this case, it was argued that these individuals should not be classified as offenders who first became involved in crime during adulthood as based on the frequency of their involvement in offending they should have already been flagged by the criminal justice system as early minority. After all, the higher the frequency of involvement in criminal offences, the greater the likelihood of being identified by the criminal justice system. McGee and Farrington concluded that the inclusion of such a group of people in the category of those who start offending from the age of 21 years onwards is an inaccurate result of the official recording of crime by the criminal justice system (criminal conviction history). In line with the above, it was found that both individuals who started their involvement in delinquency from the age of 21 years onwards and those who had already been involved in the criminal justice system during their minority reported that they had committed criminal acts such as assault, vandalism and drug use which have low rates of detection and flagging by the criminal justice system. However, those who had been involved in the criminal justice system during their minority years were equally likely to commit burglary and vehicle theft and therefore had an increased likelihood of arrest (McGee, Farrington, 2010, p. 545).

As part of a study of the factors associated with being involved in criminal acts in adulthood, Eggleston and Laub (2002) attempted to answer the question of whether there is a differentiation between adult offenders who become involved in offending from the age of 18 onwards and those who have already been involved during minority. They evaluated data from two cohorts from 1942 and 1949 respectively (Racine birth cohorts)[22] in which 889 males and females initially participated and the final sample consisted of 732 participants (51% males and 49% females)[23]. The sample's contact with the police was investigated through data collection for the period 1948-1976[24] and it was found that 61.2% (448) had no contact with the police. Specifically, 14.3% had a history of police contacts only during the period of minority and specifically during the age period 6-17 years, a percentage of 11.3% had a history of police contacts only during the period of adulthood (18 years and above) and a percentage of 13.1% had had contact with the police both during minority and adulthood.

[21] Two out of 5 individuals also had a higher mean at the age of 14.

[22] See also Shannon, 1994.

[23] The follow-up period of the sample covered a time range from the age of 6 to the age of 25 years (the 1949 cohort) and 32 years (the 1942 cohort).

[24] The contact with the police did not concern traffic violations and low-level offences which according to the law are only committed by minors (status offences) and did not necessarily lead to arrest.

Finally, it is worth mentioning that among all adult offenders, those who first came into contact with the police after the age of 18 constituted a percentage of 46.4% (Eggleston, Laub, 2002, p. 609-610). In the context of exploring a range of factors such as e.g. demographic characteristics, family variables, variables referring to the adolescent period and related to e.g. school, peer friends and drug use, but also variables referring to adulthood and related to e.g. friendships with other offenders and drug use, it was found that between individuals who started offending from the age of 18 onwards and those who were involved in offending both in minority and in adulthood there are many similarities in the influence of these variables on the occurrence of offending behaviour in adulthood (Eggleston, Laub, 2002, p. 611-612; Piquero *et al.*, 2012, p. 26). On this basis, Eggleston and Laub (2002, p. 612-613) conclude that «the predictors of adult offending are similar for all adult offenders independent of past delinquency». They even point out that this conclusion could support the view that the factors associated with the criminal onset in adulthood are similar to the factors associated with the continuation of criminal behaviour from minority to adulthood. In the same vein, Gomez-Smith and Piquero (2005) did not identify variables that differentiate offenders who initiate offending in adulthood versus adult offenders who were already committing criminal offences during the period of minority (Piquero et al., 2012, p. 27). Specifically, they studied a sample of African American men and women drawn from the Philadelphia Perinatal Birth Cohort Project[25] to examine participation as captured in the officially recorded offending starting point at the age of 18 and older and its associated factors. In the framework of this survey, those who had no recorded police contact as minors but had a history of at least 1 criminal conviction as adults were defined as offenders with a criminal onset in adulthood[26], those who had at least 1 police contact during minority but no history of criminal convictions in adulthood were defined as offenders who desisted while those who had a history of at least 1 police contact during minority and a criminal conviction in adulthood were defined as offenders who persisted (Gomez-Smith, Piquero, 2005, p. 521). According to the research data, 689 persons had never been involved in committing a criminal act, 78 persons were identified as offenders who initiated their criminal onset after the age of 18, 144 persons desisted crime and 76 persons were identified as persistent offenders. Thus, the percentage of offenders who had no history of involvement in the criminal justice system before the age of 18 was estimated to be 7.9%, with a higher percentage of men than women, contrary to the results of previous studies where the opposite was found (Kratzer, Hodgins, 1999 as cited in Smith-Gomez, Piquero, 2005, p. 517). At the same time, it was established that individuals whose mothers smoked during pregnancy were more likely to engage in criminal behaviour in adulthood. Finally, those persons who scored higher on a specific test of cognitive ability (California Achievement Test)[27] were less likely to engage in delinquent behaviour in adulthood. This finding supports the view that cognitive abilities may act as protective factors[28].

In the context of the longitudinal prospective research Cambridge Study in Delinquent

[25] 987 people were studied up to their mid-fourth decade of life.

[26] In the framework of the research design the starting point of adulthood is after age 18.

[27] The test was designed to measure, assess, and analyse school performance by focusing on verbal and numerical ability (Gomez-Smith, Piquero, 2005, p. 520).

[28] For the meaning of 'risk and protective factors' and related terms see above.

Development and in respect of risk factors for the criminal onset during or after adulthood, Zara and Farrington (2010, p. 258) point out the need to investigate both risk and protective factors during minority and how these factors may interact. They, therefore, attempted to examine the role of certain psychological characteristics in the criminal onset in adulthood on the assumption that these characteristics function protectively during minority but such protective character seems to disappear when the person passes into adulthood. Their research data showed that in the case of the criminal onset from the age of 21 and above[29], there are individual factors of a psychological nature which are identified during minority and act as a temporary protective factor during this period, but which take on the character of a risk factor when the person reaches adulthood. Individuals whose starting point for their criminal behaviour was the age of 21 resembled more to non-offenders in the period before the age of 21 and at the age of 32 these individuals resembled more to offenders who had been involved in committing offences since they were underage. The strongest predictors were recorded as a history of nervousness and neuroticism[30], which seem to be protective during minority but seem to lose their protective effect in adulthood. Such characteristics may protect the juvenile from associating with other offenders of the same age and from risky actions and activities. It is argued, however, that in such a situation the individual is not shielded against the challenges and demands of adult roles (Zara, Farrington, 2010, p. 270).

3. Theoretical approaches on adult criminal onset

The debate around the issue of developing an adequate explanatory framework regarding the criminal onset in adulthood reflects two different perspectives regarding the acceptance or non-acceptance of the existence of the phenomenon under consideration (McGee, Farrington, 2010, p. 530). In this context, static theories such as Gottfredson & Hirschi's (1990) classical theory of the level of self-control that is fixed early in childhood[31] and remains unchanged over time without being influenced by life events, state that the criminal onset in adulthood is a particularly rare phenomenon[32]. Gottfredson and Hirschi argue that individuals whose criminal onset is placed in adulthood demonstrate a high level of self-control in adolescence which works protectively and which will lead them very quickly to desistance from crime (Thornberry et al., 2012, p. 53). In the same vein, Moffitt (1993), within the dual taxonomy which she developed, incorporating into it[33] evidence pointing to both the concept of stability and the concept of change[34], argued that involvement in delinquency

[29] In this context, and in contrast to earlier publications relating to the sample of participants in the longitudinal prospective study Cambridge Study in Delinquent Development, the starting point of criminal behaviour for those initiating in adulthood is placed at 21 years and beyond, based on both criminal convictions and self-reported data. On the importance of combining data sources Zara and Farrington mention: «we have previously investigated the characteristics of late-onset offenders based only on convictions, but this might produce misleading results, and errors in allocating a person to a specific onset group can be reduced by combining self-reported delinquency and official data» (Zara, Farrington, 2010, p. 259; Zara, Farrington, 2009).

[30] Neuroticism is considered as being a personality trait that increases the likelihood for someone to develop phobic and stressful disorders (Chountoumadi, Pateraki, 2008, p. 379).

[31] The low level of self-control appears to be associated with inadequate parental child-rearing practices during the period of minority (Gottfredson, Hirschi, 1990).

[32] According to another view, this phenomenon does not exist as it is a methodological construction (Zara, Farrington, 2016, p.35; McGee, Farrington, 2010, p. 530).

[33] Regarding Moffitt's typological theory which falls within the field of Developmental Criminology see Moffitt, 1993, 2006 and Farrington, 2003.

[34] Ulmer and Spencer (1999, p. 102) state that: «Developmental and life course perspectives offer useful

during adulthood is extremely rare (Moffitt et al., 2001 as cited in Thornberry et al., 2012, p. 53). In contrast, according to Laub and Sampson's (2003) life-course model which focuses on the role of social bonds[35] in the context of an informal social control, the criminal onset in adulthood is a phenomenon that is considered to be expected and the explanatory framework around it is based on the weakening of the individual's social bonds during adulthood as reflected through life events[36]. In the framework of Developmental/Life-course Criminology it is of particular interest the theory of Thornberry and Krohn (2001) in regard to the explanation of the phenomenon of involvement in the criminal onset after the period of minority. In particular, they ascribe the late criminal onset to factors such as low IQ, low educational level and reduced social skills, referring to the importance of so-called human capital. These deficits are already observed during juvenile years, however, the individual's strong social bonds with family and school seem to play a protective role during this period. When the individual is in the transition phase of adulthood, however, he or she is no longer in the safe and supporting environment in which he or she has been living and is confronted with the challenges and demands of adopting adult roles. In such a pressured background, friendly interactions with other offenders and the use of alcohol and drugs act as reinforcers increasing the chances of offending behaviour (Thornberry *et al.*, 2012, p. 60; McGee, Farrington, 2010, p. 531; Farrington, 2003, p. 244). Another theoretical approach is the one which was developed within social psychological theories[37] with an emphasis on emotion, cognitive processes and the formation of personal identity based on the individual's social experience and interaction with the environment[38]. Thornberry et al. (2012) give the typical example of a young person from low socio-economic backgrounds who has expectations of a successful professional career which is ultimately not achieved due to lack of available legal means. Thus, failure to achieve the goal during adulthood generates feelings of frustration and anger which can lead to a change of thought and attitude, encouraging involvement in illegal activities. They state in this regard: «The psychological realm is important because these attitudes and emotions are important mediators-it is the individual's reaction to accumulated structural disadvantage that is the key» (Thornberry et al., 2012, p. 66). On this basis, and given the multifactorial nature of the criminal phenomenon, it is important to take into consideration many different factors, including cognitive factors, which, however, are not so often highlighted in the study of crime (Maruna, 2001).

4. Conclusion

Based on the above research evidence, the need for both further empirical investigation of the phenomenon and the development of an adequate theoretical framework to explain it is indicated. The

theoretical extensions of criminal career research. These perspectives take note of both the stability (persistence) and dynamic changes (onset and desistance) in offending during a person's life».

[35] The development of strong social bonds depends on the individual's attachment to socialising institutions such as family and school, without ignoring the importance of friendships and parental nurturing practices (Sampson, Laub, 1993; Farrington, 2003, p. 241).

[36] Sampson and Laub pay particular attention to the impact of life events during the transition period from minority to adulthood such as marital life, family formation, job acquisition etc. (McGee, Farrington, 2010, p. 531; Farrington, 2003, p. 241; Thornberry et al., 2012).

[37] See for example Mead's theory on symbolic interaction (Mead, 1925, 1934).

[38] The importance of cognitive factors and cognitive transformation has been stressed especially in the study of desistance from crime (Maruna, 2001; Giordano *et al*. 2002; Kazemian, 2015).

methodological limitations of the research designs so far, mainly regarding the type of research data (data from official records), limit to a certain extent the value of the available research outcomes. Therefore, the use of self-reported data is considered of paramount importance in order to illustrate the true dimensions of the phenomenon. Indeed, the comparison of self-reported data and official data in the context of studying the criminal onset during adulthood is a relatively recent area of research interest. In addition, based on the empirical studies available so far, there seems to be a lack of investigation of risk factors that are closer to the phenomenon under consideration, with research interest focusing on both risk and protective factors that are identified during minority. In this context, the formulation of an adequate explanatory framework of the phenomenon presents, as can be expected, several difficulties. However, it is clear that a true representation of the phenomenon based on a combination of data sources and the identification of both the associated risk and protective factors will provide a solid basis for the development of more effective prevention and response policies.

References

1. Arthur, M.W., Hawkins, D., Pollard, J.A., Catalano, R.F., Baglioni, A.J., «Measuring risk and protective factors for substance use, delinquency and other adolescent problem behaviors», Evaluation Review, 26(6), 2002, p. 575-601.
2. Blumstein, A., Cohen, J., Farrington, D.P., «Criminal career research: Its value for Criminology», Criminology, 26(1), 1988, p. 1-35.
3. Blumstein, A., Cohen, J., Roth, J., Visher, Ch., Criminal careers and "career criminals", Vols 1 and 2, National Academy Press, Washington, DC, 1986.
4. Chountoumadi, A., Pateraki, L., Dictionary of Psychology (Editing by Ch. Xenaki), TOPOS, Athens, 2008. (In Greek, Χουντουμάδη, Α., Πατεράκη, Λ., Λεξικό Ψυχολογίας (Επιμ. Χ. Ξενάκη),Τόπος, Αθήνα, 2008).
5. DeLisi, M., «Age-crime curve and criminal career patterns», in Morizot J. & Kazemian L. (Eds.), The Development of Criminal and Antisocial Behavior: Theories, Research and Practical Applications, Springer, 2015, p. 50-63.
6. DeLisi, M., Kosloski, A.E., Drury, A.J., Vaughn, M.G., Beaver, K.M., Trulson, Wright J.P., «Never desisters: A descriptive study of the life-course persistent offender», in DeLisi M. & Beaver K.M. (eds.), Criminological Theory: A life-course approach, Jones & Bartlett Learning, Burlington, 2014, p. 297-310.
7. Eggleston, E.P., Laub, J.H., «The onset of adult offending: A neglected dimension of the criminal career», Journal of Criminal Justice, 30 (6), 2002, p. 603-622.
8. Farrington, D.P., «Age and crime», Crime and Justice, 7, 1986, p.189-250.
9. Farrington, D.P., «Developmental and life-course criminology: Key theoretical and empirical issues-The 2002 Sutherland Award Address», Criminology, 41(2), 2003, p. 221-255.
10. Farrington, D.P., «Predicting individual crime rates», in Gottfredson D. & Tonry M. (eds), Prediction and Classification: Criminal Justice Decision-Making, University of Chicago Press, Chicago, 1987, p. 53-101.
11. Farrington, D.P., Piquero, A.R., Jennings W.G., Offending from childhood to late middle age: Recent results from the Cambridge Study in Delinquent Development, Springer, 2013.
12. Giordano, P.L., Cernkovich, S.A., Rudolph, J.L., «Gender, crime, and desistance: Towards a theory of cognitive transformation», American Journal of Sociology, 107(4), 2002, p. 990-1064.
13. Glueck, S., Glueck, E.T., Unraveling juvenile delinquency, Harvard University Press, Cambridge, 1950.

14. Gomez-Smith, Z., Piquero, A., «An examination of adult-onset offending», Journal of Criminal Justice, 33(6), 2005, p. 515-525.
15. Gottfredson, M.R., & Hirschi, T., A general theory of crime, Stanford University Press, Stanford, 1990.
16. Hirschi, T., Gottfredson, M., «Age and the explanation of crime», American Journal of Sociology, 89(3), 1983, p. 552-584.
17. Horney, J., Tolan, P., Weisburd, D., «Contextual influences», in Loeber R. & Farrington D.P. (eds), From Juvenile Delinquency to Adult Crime: Criminal Careers, Justice Policy, and Prevention, Oxford University Press, Oxford, 2012, p. 86-117.
18. Kazemian, L., «Desistance from crime and antisocial behavior», in Morizot J. & Kazemian L. (eds.), The Development of Criminal and Antisocial Behavior: Theories, Research and Practical Applications, Springer, 2015, p. 295-312.
19. Kirk, D.S., «Examining the divergence across self-report and official data sources on inferences about the adolescent life-course of crime», Journal of Quantitative Criminology, 22(2), 2006, p. 107-129.
20. Kratzer, L., Hodgins, S., «A typology of offenders: a test of Moffitt's theory among males and females from childhood to age 30», Criminal Behaviour and Mental Health, 9(1), 1999, p. 57-73.
21. Laub, J.H., Sampson, R.J., «Understanding desistance from crime», Crime and Justice, 28, 2001, p. 1-69.
22. Laub, J.H., Sampson, R.J., Shared beginnings, divergent lives: Delinquent boys to age 70, Harvard University Press, Cambridge, 2003.
23. Le Blanc, M., «A generic control theory of the criminal phenomenon: The structural and dynamic statements of an integrative multilayered control theory», in Thornberry T.P. (ed.), Developmental Theories of Crime and Delinquency. (Advances in Criminological Theory, Vo1.7.), Transaction, New Brunswick, 1997
24. Loeber, R., Farrington, D.P., «Introduction», in Loeber R. & Farrington D.P. (eds), From Juvenile Delinquency to Adult Crime: Criminal Careers, Justice Policy, and Prevention, Oxford University Press, Oxford, 2012, p. 3-13.
25. Loeber, R., Farrington, D.P., Howell, J., Hoeve, M., «Overview, conclusions and key recommendations», in Loeber R. & Farrington D.P. (eds), From Juvenile Delinquency to Adult Crime: Criminal Careers, Justice Policy, and Prevention, Oxford University Press, Oxford, 2012, p. 315-370.
26. Magnusson, D., Individual development from an interactional perspective: a longitudinal study, Lawrence Erlbaum Associates, Hillsdale,1988.
27. Maruna, S., Making good: How ex-convicts reform and rebuild their lives, American Psychological Association, Washington, 2001.
28. McGee, T.R., Farrington, D.P., «Are there any true adult-onset offenders?», British Journal of Criminology, 50(3), 2010, p. 530-549.
29. Moffitt, T.E., « Adolescence-limited and life-course-persistent antisocial behaviour: A developmental taxonomy», Psychological Review, 100(4), 1993, p. 674-701.
30. Moffitt, T.E., «A review of research on the taxonomy of life-course persistent versus adolescence-limited antisocial behavior», in Cullen F.T., Wright J.P. & Blevins K.R. (eds.), Taking stock: The status of criminological theory, Transaction, New Brunswick, 2006, p. 277-312.
31. Moffitt, T.E., Caspi, A., Rutter, M., Silva P.A., Sex differences in antisocial behavior: Conduct disorder, delinquency and violence in the Dunedin longitudinal study, Cambridge University Press, Cambridge, 2001.
32. Morizot, J., Kazemian L., «Introduction: Understanding criminal and antisocial behavior within a developmental and multidisciplinary perspective», in Morizot J. & Kazemian L. (eds.), The Development of Criminal and Antisocial Behavior: Theories, Research and Practical Applications, Springer, 2015, p. 1-18.

33. Piquero, A.R., Farrington, D.P., Blumstein A., Key issues in criminal career issues: New analyses of the Cambridge Study in Delinquent Development, Cambridge University Press, Cambridge, 2007.
34. Piquero, A.R., Farrington, D.P., Blumstein, A., «The criminal career paradigm», Crime and Justice, 30, 2003, p. 359-506.
35. Piquero, A.R., Hawkins, J.D., Kazemian, L., «Criminal Career Patterns», in Loeber R. & Farrington D.P. (eds.), From Juvenile Delinquency to Adult Crime: Criminal Careers, Justice Policy, and Prevention, Oxford University Press, Oxford, 2012, p. 14-46.
36. Rhodes, W., «The criminal career: Estimates of the duration and frequency of crime commission», Journal of Quantitative Criminology, 5(1), 1989, p. 3-32.
37. Robins, L.N., «Sturdy childhood predictors of adult antisocial behaviour: Replications from longitudinal studies», Psychological Medicine, 8(4), 1978, p. 611-622.
38. Sampson R.J., Laub J.H., Crime in the making: Pathways and turning points through life, Harvard University Press, Cambridge, Massachusetts, London, 1993.
39. Shannon, L.W., Juvenile delinquency and adult crime, 1948-1977 (Racine, Wisconsin): three birth cohorts (computer file). Conducted by the University of Iowa, Iowa Urban Community Research Center, 2nd ICPSR ed. Ann Arbor, MI: Inter University Consortium for Political and Social Research, Producer and Distributor, 1994.
40. Stattin, H., Magnusson, D., Reichel H., «Criminal activity at different ages: A study based on a Swedish longitudinal research population», British Journal of Criminology, 29(4),1989, p. 368-385.
41. Thornberry, T.P., Giordano, P., Uggen, Ch., Matsuda, M., Masten, A., Bulten, E., Donker, A.G., «Explanations of offending», in Loeber R. & Farrington D.P. (eds.), From Juvenile Delinquency to Adult Crime: Criminal Careers, Justice Policy, and Prevention, Oxford University Press, Oxford, 2012, p. 47-85.
42. Thornberry, T.P., Krohn, M.D., «The development of delinquency: An interactional perspective», in White S. (ed.), Handbook of Youth and Justice, Plenum, New York, 2001, p. 289-305.
43. Ulmer, J.T., Spencer, W., «The contributions of an interactionist approach to research and theory on criminal careers», Theoretical Criminology, 3(1), 1999, p.95-124.
44. Van Koppen, M.V. «Criminal career dimensions of juvenile and adult-onset offenders», Journal of Developmental and Life Course Criminology, 4(1), 2018, p. 92-119.
45. Wolfgang, M.E., Figlio, R.M., Sellin, T., Delinquency in a birth cohort. University of Chicago Press, Chicago, 1972.
46. Wolfgang, M.E., Thornberry, T.P., Figlio, R.M., From boy to man, from delinquency to crime, University of Chicago Press, Chicago,1987.
47. Zara, G., Farrington, D.P., «A longitudinal analysis of early risk factors for adult-onset offending: What predicts a delayed criminal career?», Criminal Behaviour and Mental Health, 20(4), 2010, p. 257-273.
48. Zara, G., Farrington, D.P., «Childhood and adolescent predictors of late onset criminal careers», Journal of Youth and Adolescence 38(3), 2009, p. 287–300.
49. Zara, G., Farrington, D.P., Criminal recidivism: Explanation, prediction and prevention, Routledge, London, N.Y., 2016.
50. Zarafonitou, Ch., Empirical Criminology, Nomiki Vivliothiki, Athens, 2004 (In Greek, Ζαραφωνίτου Χ., Εμπειρική Εγκληματολογία, Νομική Βιβλιοθήκη, Αθήνα, 2004).

doi: 10.14664/rcvs/247

Figli di persone detenute: un'analisi italiana ed europea

Enfants de parents détenus : une analyse italienne et européenne

Children of imprisoned parents: an Italian and European analysis

Sara Fontanot *

Riassunto
L'articolo esamina la situazione dei bambini figli di persone in conflitto con la legge da una prospettiva vittimologica e socio-criminologica, considerando questi minori come vittime secondarie del reato commesso dal genitore. È stata condotta un'analisi comparativa sulla condizione di questi bambini in Italia e in Europa, analizzando alcuni aspetti quali il quadro legale, la gestione della maternità, la possibile presenza di minori in carcere e fornendo alcuni esempi di organizzazioni e associazioni che lavorano per tutelare il benessere di questi minori. È stata dedicata particolare attenzione al ruolo della scuola come fattore protettivo nei confronti di bambini con esperienza di carcerazione genitoriale. Inoltre, è stato realizzato un questionario che ha analizzato il livello di consapevolezza degli insegnanti del sistema scolastico italiano per capire se questi professionisti fossero consapevoli della presenza di studenti con almeno un genitore in carcere nelle loro classi.

Résumé
À partir d'une perspective victimologique et socio-criminologique, l'article traite de la situation des enfants de parents emprisonnés en les considérant comme des victimes secondaires de leurs infractions. Une analyse a été menée sur les conditions de ces mineurs en Italie et en Europe, en examinant le cadre légal, la gestion de la maternité et la présence éventuelle d'enfants en prison, tout en fournissant quelques exemples d'organisations et d'associations travaillant pour sauvegarder le bien-être de ces enfants. Une attention particulière a été accordée au rôle de l'école en tant que facteur de protection des enfants dont les parents sont emprisonnés. De plus, un questionnaire a été élaboré pour examiner le niveau de sensibilisation des professeurs italiens afin de comprendre si ces professionnels étaient conscients de la présence d'élèves mineurs ayant au moins un parent détenu dans leurs classes.

Abstract
The article examines the situation of children of parents in conflict with the law from a victimological and socio-criminological perspective, considering them as secondary victims of their parents' offences. A comparative analysis was conducted on the conditions of these minors in Italy and Europe, investigating the legal framework, the maternity management, the possible presence of children residing in prison, and providing some examples of organisations and associations working to safeguard the well-being of these children. Particular attention was dedicated to the role of the school as protective factor for children experiencing parental imprisonment. Moreover, a questionnaire was developed which examined the awareness level of teachers in the Italian school system to understand whether these professionals were aware of the presence of underage students with at least one imprisoned parent in their classrooms.

Key words: children of imprisoned parents, victims, comparative analysis Italy-Europe, crime prevention, role of the school

* Laureata in Scienze Criminologiche per l'Investigazione e la Sicurezza, Università di Bologna.

1. Introduction

Known as «hidden victims of imprisonment» (Philbrick *et al.*, 2014, p. 17) or secondary victims of parents' crime (Salvetti, 2019), children with parents in conflict with the law can be affected by the short and long-term negative consequences of parental separation and imprisonment. They have to bear the burden of their parents' criminal offence, and this is not easy for a child, especially if they do not receive support from society. Indeed, these children are often not properly considered and heard during the different stages of parental sentencing or taken into account by policy makers, stakeholders and professionals in different fields. Moreover, this group is vulnerable and needs particular attention because children experiencing parental imprisonment can be more at risk of having antisocial and criminal behaviours in the future (Murray, Farrington, 2005; Filograsso, Nardone, 2016; Mazza, 2002; Musi, 2012; Bambinisenzasbarre, 2009; Paris, 2017). Taking into account the fact that there is a lack of data regarding these children on a local, national, and European level (Council of Europe, 2018a) and also considering the probable consequences that these minors could face, it is fundamental to pay attention to this victimised and vulnerable group of children.

This article is the extract of a master thesis that aims to address the issue of children with imprisoned parents from the victimological and socio-criminological point of view, trying to explain why these children can themselves be considered victims. The aim is to make readers aware of the existence of this victimised group of children, their rights and needs that are often not noticed or considered. To be more specific, the main subjects are children aged 0 to 17 (without gender relevance) with one or more parents in conflict with the law. The thesis focuses on the situation of these children in Italy and in Europe, trying to describe their condition through the analysis of the legal framework as well as of the support network in prison and outside. Indeed, the research offers insight into the organisations working to safeguard and support these children. Moreover, the role of schools is taken into consideration because teaching and learning institutions seem to be an effective environment to identify and support this vulnerable group.

In order to provide reliable data, the author mentioned some research, such as studies of Murray and Farrington, Philbrick *et al*'s. paper, some milestone sociological theories (e.g.: Bronfenbrenner's Ecological Systems Theory and the Labelling Theory), and other qualitative and quantitative analyses. Statistics and figures were obtained primarily from Children of Prisoners Europe's website or from EuroPris, which was a useful source especially for the comparisons amongst different European countries. The author gained information also through interviews with professionals, from resources provided by different associations, and analysing the results of the questionnaire.

The article is divided into sections. After a brief introduction regarding the methodology and literature, we are going to analyse the situation of these victims, the possible psycho-social difficulties as well as practical and economic consequences that they can face. Then we consider the possible risk of antisocial and criminal behaviours that these minors could face, also offering examples to prevent crime and instances of protective factors to support the child's well-being. Afterwards the situation of children in Italy is considered, analysing the legal framework and reporting the case study of Bambinisenzasbarre. The same topics are

investigated on a European level, offering a picture of the conditions of children with parents in conflict with the law in different countries. Moreover, the NGO Children of Prisoners Europe and its projects and initiatives are briefly described. Consequently, the role of schools in the support of children with imprisoned parents is taken into consideration. Some examples of associations and projects working with schools to raise awareness and to support children are described, such as Families Outside, For Fangers Pårørende and the School Zone project. In the end, there is an analysis of a questionnaire filled out by teachers of the Italian school system in order to understand their level of awareness of students with parents in prison and to gain data about this invisible and under studied social issue.

2. Methodology and literature

Different methodological approaches were used for this research. Part of the thesis focuses on the analysis of secondary literature retrieved from academic and scientific resources. Indeed, it has been noticed that literature about this social issue is growing and that means that the awareness level among academics and researchers of children with parents in conflict with the law is rising.

Moreover, qualitative and quantitative data obtained through interviews with professionals in the field and through a questionnaire for teachers within the Italian school system have been included.

There were four semi-structured interviews, following a similar and prepared investigative path, but also giving space for direct discussion with the professionals. The professionals interviewed included the Director of Operations of Children of Prisoners Europe (Paris, France), the Chief Executive of Families Outside (Edinburgh, Scotland), the Senior Advisor of For Fangers Pårørende (FFP) (Oslo, Norway) and the Schools and Prison Family Coordinator at HMP Parc (Bridgend, Wales). They were selected thanks to their expertise in the field of children with imprisoned parents and to the innovative activities they are involved with in their respective associations.

The questionnaire, written in Italian, consists of 15 both open and closed questions with the aim of examining the awareness level of teachers in the Italian school system in order to understand whether these professionals are aware of the presence of minor students with at least one imprisoned parent in their classrooms. The statistical sample is made up of teachers in different educational levels of the Italian school system (nursery school, kindergarten, primary school, middle school and high school). The data refer to experiences with minor students. The sample was reached through the distribution of the link for the online questionnaire via various social networks, instant messaging applications and by sending e-mails (220) to educational institutions of different levels. The school institutions contacted were selected in the regional capital and the number was decided on the basis of the response rate. The questionnaire link was accessible from 23rd August 2022 to 2nd November 2022, so it was possible to give their answers during this time.

To determine the questions for the questionnaire, the starting point was a brainstorming session to understand what information was useful. Once the topics and aspects of interest were identified, the questionnaire was created online. Some of the questions were needed to identify the social and demographic characteristics of the respondents and to obtain details about their professional career, while the others aim to gain knowledge about the topic.

It was hypothesised that a low number of teachers were aware of the issue and/or the presence of students with one or more parents in prison, with few local awareness-raising activities for professionals.

A total of 303 responses were collected. It is interesting to point out the discrepancy between the emails sent (which in any case is only a tool used to share the questionnaire) and the number of replies. Out of 220 emails sent, 303 were the total replies. These figures indicate that there was little participation on the part of educational institutions. Moreover, the author hoped to create a map depicting the distribution of awareness across Italian regions, to understand whether there was a link between awareness and the actual local presence of many children with imprisoned parents. Due to the lack of answers in some regions and consequently a heterogeneous response rate, it was impossible to create the desired map.

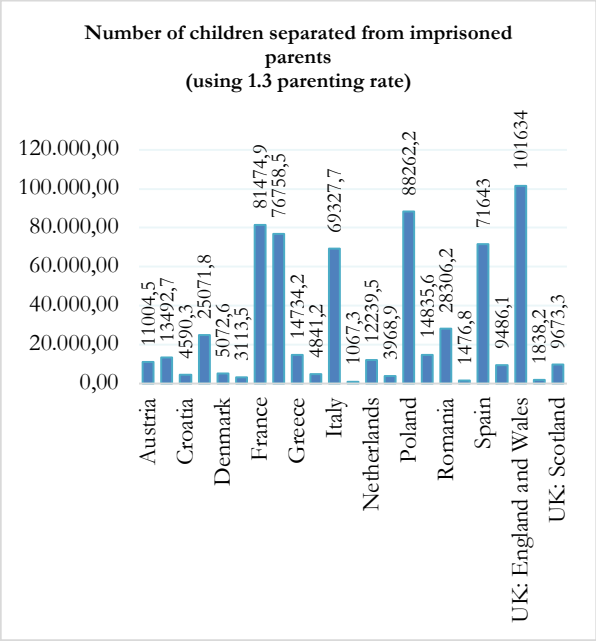
To summarise, the thesis and therefore this article consist of a mixed methodological approach including secondary literature, interviews, questionnaire, and fieldwork experiences.

3. Children with imprisoned parents: some numbers

On any given day, an estimated 2 million children are separated from a parent in prison in Europe (calculations made by Children of Prisoners Europe, from an extrapolation of a 1999 INSEE study), while about 800,000 children experience the same situation in EU 27 + UK (Children Of Prisoners Europe, n.d.-a). In Italy in 2019 there were around 100,000 children with at least one imprisoned parent (Salvetti, 2019). The number of these children is high in many countries, and it is rising following the increase of prison population across Europe (Philbrick *et al.*, 2014).

Despite the data reported above, it is important to remember that there is a dark figure of children with imprisoned parent(s) which means that it is difficult to understand how many children are in this situation because not all prison administrations of different countries have the duty to register or collect data about family situation and especially about the number and conditions of prisoners' offspring (EuroPris, n.d.-a; Glover, 2009) as well as the fact that the sense of shame and fear of being stigmatised stop family members from telling the truth about the imprisonment (Sack, Seidler, 1978; Mazza, 2002). Therefore, we are not adequately aware of how many children in each country are experiencing this situation. However, knowing the number of these children could help the implementation of policies and the offering of tailored activities and projects to safeguard them.

Figure 1 Number of children separated from imprisoned parents. Data retrieved from COPE website (Children Of Prisoners Europe, n.d.-b)



3.1 Children with imprisoned parents as victims: consequences of parental imprisonment

Having a parent in prison is considered as to be part of Adverse Childhood Experiences (ACEs), which are potentially traumatic events that occur in childhood, between 0 and 17 years of age (Centers for Disease Control and Prevention, 2022). The feeling of uncertainty and insecurity caused by the loss of a parent due to imprisonment can lead to post-traumatic stress and various difficulties and problems which may be internalised or externalised (Philbrick *et al.*, 2014). Acting-out behaviours (e.g.: hostile behaviour, use of drugs or alcohol, school truancy, aggressive acts, involvement in delinquent activities, etc.) are usually related to the father's absence, while acting-in behaviour (e.g.: daydreaming, unwillingness to engage in play, acting babyish, fear of school, school drop, etc.) to the mother's absence (Fritsch, Burkhead, 1981).

Continuing to analyse the consequences of parental detention on the child, Murray and Farrington (2005) stated that these children can face a range of psychosocial difficulties such as: depression; regression; hyperactivity; aggressive and/or changing behaviour; withdrawal; eating disorders; sleep problems; running away; poor school grades and delinquency. According to Murray and Farrington (2008), children with at least one parent in prison are twice as likely as their peers (Glover, 2009) to suffer from mental health problems, depression, and attention disorders.

With regard to the practical and financial consequences, in some cases children may have to leave their homes after parental imprisonment and move to live with relatives, friends or even in foster homes (Mazza, 2002). Prisoners' families are at risk of financial instability, poverty, debt, and potential housing disruption (Glover, 2009; Murray, Farrington, 2005). According to Western and Petit's study (2010), during the period of a parent's imprisonment, the family's earnings decrease by about 22% compared to the period before the imprisonment.

These children are also frequently overlooked in national policies as comprising a vulnerable group in their own right with particular needs (Philbrick *et al.*, 2014). One could argue that children are affected by secondary victimisation which is the condition of further suffering of the victim caused by an attitude of insufficient attention or negligence from agencies of social control (Sicurella, 2020). It is interesting to report Lauwereys's study (2020) in which seventeen Belgian criminal law judges were asked to reply to some open questions and to impose a sentence in a fictitious scenario. The results of the interviews highlight that little attention is given to children during the parental sentencing. Indeed, 5 out of 17 judges deemed the best interests of the child insignificant in the sentencing decision and many of them were not aware of the impact of parental incarceration on children. Following the concept of «judicialization of politics» (Hirschl, 2008), it is important to understand that judges have become policy makers themselves which means that a lack of attention on a judicial level could also cause a lack of awareness on a legislative level and therefore little safeguarding of children's rights and needs.

3.2 Higher risk to commit crime?

Some studies (Murray, Farrington, 2005; Filograsso, Nardone, 2016; Mazza, 2002; Musi, 2012; Bambinisenzasbarre, 2009; Paris, 2017) stated that children with imprisoned parent(s) have a higher probability to commit crimes than their peers without this background. Robins *et al.*'s research (1976) highlighted that parental arrest is correlated

with consecutive children's delinquency, while Sack (1977) discovered that 12 out of 24 children of imprisoned fathers included in his study manifested some form of problematic behaviour. According to Glover, children with imprisoned parents are about three times more at risk than their peers of committing antisocial or delinquent conducts (Glover, 2009). It is difficult to find a unique reason to understand why some children with imprisoned parents could be at higher risk of offending. The thesis mentioned some theories, such as the labelling theory and the intergenerational crime transmission theory. According to Rosenthal and Jacobson's Pygmalion Effect theory (Offredi, 2016), expectations of a person's behaviour can become self-fulfilling prophecies. Therefore, if children with imprisoned parents are labelled as delinquents and are expected to commit crimes in the future, there is a high probability that these children will engage in illegal conducts (Fine, 1977; Murray, Farrington, 2005). Moreover, theories of intergenerational transmission predict that children of convicted parents may have a greater risk of offending (Weijer *et al.*, 2014). Indeed, there is the risk that the child internalises and models the criminal behaviour of the parent (Filograsso, Nardone, 2016). Farrington (2002) suggested six mechanisms that might link parent to offspring criminality: intergenerational exposure to risk; assortative mating (male and female offenders tend to cohabit or marry); imitation and teaching of crime; mediation through environmental risks; genetic mechanisms, and official (police and/or court) bias. However, it is important to mention that many of these studies are based on a small sample and are mostly qualitative as well as outdated. Therefore, they are limited and not entirely reliable. Thus, it is important to analyse these data considering the fact that studies in this field are not totally valid and keeping in mind that focusing the attention on the children's (hypothesised) higher risk to commit antisocial behaviours can contribute to further stigmatisation. Having a parent in conflict with the law is not a deterministic factor.

The analysis of the interviews highlighted that the social condition after the parent's detention can particularly affect children's well-being and future. As the Senior Advisor of For Fangers Pårørende stated,

> *it's poverty, it's stigma, it's like maybe growing up with challenges that you wouldn't have if your parent wasn't in prison, it makes you more vulnerable* (Senior Advisor at For Fangers Pårørende, 16th March 2022).

The Chief Executive of Families Outside also reported the problem of social isolation and said that,

> *you have a situation break, they are disconnected from social support and that means the person who's gone to prison, but also the family might be isolated, the neighbourhood may target them, they might be ostracised, people losing friendships, that might have to move house* (Chief Executive at Families Outside, online interview, 11th March 2022).

The Director of Operations of Children of Prisoners Europe answered in a similar way, drawing attention to poverty, social exclusion, financial strain, bullying, and school drop-out, and highlighting that,

> *if the parent is in prison, the child is exposed to that, but I don't think there's a direct link* (Director of Operations at Children Of Prisoners Europe, 7th June 2022).
>
> *if a child is provided with support when their parent is in prison, they can go on to have a healthy and successful future* (Director of Operations at Children Of Prisoners Europe, 7th June 2022).

Indeed, studies have found out that some children with an incarcerated parent even fall in a low-risk group regarding behavioural difficulties and social competence if well supported (Johnson *et al.*, 2018; Kjellstrand *et al.*, 2018; Kremer *et al.*, 2020). It would be interesting to do more research in this field, highlighting the fact that some children can live a healthy, safe, happy, and far from the crime life despite parental imprisonment. Therefore, these children do not need pity or stigmatisation, but psychological, physical, economic, legal and political support.

3.3 Protective factors

One of the most important protective factors that can safeguard children and their well-being is maintaining the relationship with the imprisoned parent(s), using all the modalities of contact that the prison institution offers to prisoners and their family (La Vigne *et al.*, 2008; Philbrick *et al.*, 2014). According to Sack and Seidler (1978), children who maintain relationships with their imprisoned parents develop less destructive and anxious behaviour than those who cut off all communication with their parent.

Policy-making is also another factor that can protect these children. As stated by Bronfenbrenner (1979, p. 7) child development «can be enhanced by the adoption of public policies and practices that create additional settings and societal roles conducive to family life». For this reason, it is important to consider children during policy-making and the sentencing of their parent(s), trying to avoid «child-blind justice» (Children of Prisoners Europe, 2019a, p. 11). Another crucial aspect that could help the child's mental health is telling the truth about their parent's imprisonment. Secrets, by their nature, could create anxiety, shame, tension, guilt, and fear (Mazza, 2002).

Furthermore, another way to reduce negative effects of detention on children is to prefer non-custodial or community sentences (Children of Prisoners Europe, 2016). To provide a practical example, research conducted by Vanhaelemeesch, Vander Beken and Vandevelde (2014) showed that children are overall happier to have their parent(s) at home using the EM (Electronic Monitoring) rather than in prison. EM tends to reduce stigma and protect children; it helps maintaining the relationship with the convicted parent who can be therefore more present in child's life. However, it is important to take child's best interests into account and hear children's needs when deciding if provide the parent with the EM or not. Children, with their rights and needs, should always be the centre of judges' and professionals' attention.

What is the connection between protective factors and crime prevention? Why is it important to underline the safeguarding of children with imprisoned parents? As it was already observed, children with parents in conflict with the law can have a higher risk to become lawbreakers themselves than their peers who have not experienced a similar condition (Murray, Farrington, 2005; Filograsso, Nardone, 2016; Mazza, 2002; Musi, 2012; Bambinisenzasbarre, 2009; Paris, 2017). One can face this problem and support these children by offering them protective factors that keep them healthy, safe and far from criminality. However, it is important to stress the fact that before supporting these children for this reason, we should safeguard and offer them positive and coping opportunities as their fundamental right, always aiming at the child's best interest.

4. Children and parenthood in prison in Italy

When considering children with imprisoned parents, it is important to mention some Italian rules that consider children's best interests and try to safeguard them, and that means the «Circolare 10 dicembre 2009 - PEA 16/2007: Trattamento penitenziario e genitorialità - percorso e permanenza in carcere facilitati per il bambino che deve incontrare il genitore detenuto» and the Charter of Children with Imprisoned Parents by Bambinisenzasbarre.

Moreover, it is fundamental to take into account the consideration of motherhood and the possibility that some children can spend part of their life residing in prison with their parents. Indeed, the Italian legislation protects the relationship between mothers in conflict with the law and their children also trying to safeguard the principle of the best interests of the child. The Italian state is aware that prisons are not a suitable environment for the psychological, physical and social health of children (Monetini, 2012). However, as stated by law n° 62/2011 which modified law n° 354/1975, in Italy children can reside with their imprisoned mother in different institutions: inside the prison itself in some targeted nurseries (up to 6 years old); in the so-called ICAM or «Istituti a Custodia Attenuata per detenute Madri» which are penitentiary institutions ruled by the Prison Administration designed as a child-friendly environment in which mothers in conflict with the law can serve their sentence or wait for it with their children up to 6 or 10 years old; or in protected houses or «case famiglia protette» which are residential facilities located the urban network, in places accessible to social and health services, and housing a maximum of six families (Del Grosso, n.d.).

4.1 Case study (Italy): Bambinisenzasbarre

For 20 years, Bambinisenzasbarre has been working to offer psycho-pedagogical support to imprisoned parents and their children, as well as to raise awareness about the topic among public opinion and professionals. The association is focused on support for the imprisoned parents, their children and their relationship by engaging in operational activities helping people inside and outside prisons (Bambinisenzasbarre, n.d.-a).

It is difficult to summarise the many activities in which Bambinisenzasbarre is involved. This association had created the Charter of the Rights of Children of Imprisoned Parents that formally recognises the right of children to maintain direct contact with their imprisoned parent and support imprisoned parents in their parental role (Bambinisenzasbarre, n.d.-b). Bambinisenzasbarre also organises nationwide training sessions for prison officers and social workers with the aim of providing child-friendly guidelines in prison (Children of Prisoners Europe, n.d.-c). Thanks to a partnership with the Ministry of Justice, Bambinisenzasbarre has achieved and promotes a welcoming model for children entering prison. Part of this project is the creation of the so-called Yellow Space which is an integrated socio-educational space to take care and give attention to children in prison waiting to visit their parent (Bambinisenzasbarre, n.d.-c). Another noteworthy project is «The match with dad», a football match played by children and their imprisoned parents, held annually in different prisons across Italy since 2015 (Children of Prisoners Europe, n.d.-d). The aim is to raise awareness of children with imprisoned parents' rights and needs, to work on the concept of social inclusion and to eliminate stereotypes (Zyba, 2022). Another incredible pilot project is the «Yellow Telephone»

which is a helpline service provided to families in order to offer information and psychological counselling to support families during and after parental detention. It is also a consultancy service for professionals regarding the protection and maintenance of the child-parent relationship when the parent is in prison relationship (Bambinisenzasbarre, n.d.-d).

5. Dealing with parenthood during criminal justice proceedings in Europe

To depict the condition of these children on a European level, some aspects regarding the sentencing (e.g.: how judges manage the pre-trial and the trial of parents), the allocation and the visiting around different countries were investigated.

With regard to sentencing, in **Croatia**, for example, prosecutors or prison administrators may reject a family's application to visit a defendant at the pre-trial stage (Children of Prisoners Europe, 2021). Moreover, parents in pre-trial detention cannot access parenting skills enhancement programmes, therefore children are not equally treated and are considered on the basis of their parents' legal status (Ombudsman for Children, 2020). On the contrary, in **Slovenia**, if both parents are sentenced, they have the opportunity to alternate the serving of their sentences (Philbrick *et al.*, 2014).

Article 145(5) of **France**'s Code of Criminal Procedure states that whenever any defendant has exclusive parental authority over a child under the age of sixteen, the court must evaluate child's situation before pre-trial detention (Children of Prisoners Europe, 2019a).

According to the **Danish** legal practice, the sentence can be suspended in special cases. However, it is doubtful that this is a normal practice and that children's rights play a prominent role in such cases (Scharff Smith, Gampell, 2011).

In **Norway**, prison sentences are not served instantly, therefore people are allowed to prepare their personal affairs prior to detention, and that also includes the arrangement of appropriate childcare (Children of Prisoners Europe, 2018). Similar to Norway, **Sweden** offers the opportunity to mothers of young children to postpone the service of a sentence to arrange for childcare (Children of Prisoners Europe, 2019a).

Regarding the category of allocation, in **Belgium**, due to security imperatives or problems of overpopulation, convicted people are not always allocated in a facility close to their family (EuroPris, n.d.-a). In **the Netherlands**, prisoners are usually allocated to a facility in the region of their residence, but capacity issues can limit this (EuroPris, n.d.-a). Similarly, the **Swedish** Prison and Probation Service does not apply proximity to children as a principle (EuroPris, n.d.-a).

In **Catalonia**, the law states that inmates must serve their sentence in the facility closest to their family and social network (EuroPris, n.d.-a). The **Danish** Prison and Probation Service tries to place people in conflict with the law in prisons close to their family. This is also the case in **Norway** (Lynn, 2013; EuroPris, n.d.-a; Children of Prisoners Europe, 2019b).

In **France** and in **Ireland**, remand prisoners are allocated in the facility closest to the court in charge of their case, therefore regardless of the prisoner's place of residence (Crétenot, Liaras, 2013; EuroPris; n.d.-a).

Changing the subject from the allocation to the visiting, in **Catalonia**, pre-trial and sentenced prisoners have both the same rights and possibilities to receive family visits, therefore children are not

affected by their parent's legal status (EuroPris, n.d.-a).

In **Denmark**, the treatment of children during visits often depends on the prison staff culture and the individual prison officer on duty (Scharff, Gampell, 2011). According to a survey carried out by the Danish Prison Service in 2011, 41% of remand prisoners never received visits from family members (Children of Prisoners Europe, 2021). Similarly, in **Poland** the quantity and the quality of the family contact depend on individual prisons and the provision of facilities (Scharff, Gampell, 2011). In **Sweden**, visiting rights are granted contingently to the conditions of detention, the gravity of the crime and the rules of the penitentiary facility (Children of Prisoners Europe, 2021), therefore little attention is paid to children.

5.1 Children and parenthood in prison in Europe

In many countries, it is possible for imprisoned parents (usually mothers, but sometimes also fathers) to stay in prison or similar facilities with their children until the child reaches a certain age, even if there is no uniform approach across Europe concerning the age by which children can remain in prison with their parents (Scharff, Gampell, 2011). Differences may depend on prison culture, value regarding motherhood, family life and child-rearing (Philbrick *et al.*, 2014). However, it is internationally and generally recognised, also thanks to the European Prison Rules and the UN Bangkok Rules, that living conditions in prison should be safe, adequate for children's physical, psychological and emotional development, including access to health and education facilities, to open-door areas and specific services for children with disabilities (Halton, Townhead, 2020; Council of Europe, 2018a).

5.2 Case study (Europe): Children of Prisoners Europe

It is fundamental to mention a European organisation working on different levels for children experiencing parental imprisonment: Children of Prisoners Europe (henceforth COPE). COPE is a pan-European network, founded in 2000, working with and for children and young people with a parent in conflict with the law and/or in prison. It operates to develop and protect the rights and welfare of children, to support positive change, and to stimulate action to improve the living conditions of minors (Children of Prisoners Europe, n.d.-a). The Children of Prisoners Europe network is a group of organisations, NGOs and individuals, with 118 members and affiliates in 35 international countries. Each individual member brings and shares expertise and practical information from their professional and cultural context with the network, resulting in a body of knowledge related to the various situations of children with imprisoned parents across Europe (Children of Prisoners Europe, n.d.-e). COPE works with members to exchange best practices, learn, and explore new ways to improve support and policies which have an impact on imprisoned parent(s) and their children. As COPE Director of Operations stated during an interview:

> *we try to make sure that there is open communication between our head office and members, and that we promote communication between members, so they can learn from each other and share their good practices and experiences working to support children with imprisoned parents* (Director of Operations of Children of Prisoners Europe, 7th June 2022).

COPE's mission is «to safeguard the social, political and judicial inclusion of children with an imprisoned parent, while fostering the pursuit and exchange of

knowledge which enhances good practices, and contributes to a better understanding of the psychological, emotional and social development of these children» (Children of Prisoners Europe, n.d.-a).

6. Children with imprisoned parents and the role of the schools

Children with imprisoned parents are not always recognised as a group that may need support on a policy level (Morgan *et al.,* 2013), but there is an environment in which these children should be heard and supported: school. Indeed, the most obvious place where children are noticed is school (SCIE, 2008), as this is where they spend many hours of their lives. However, children with imprisoned parents often represent a forgotten population even in the education system (Morgan *et al*., 2013). Schools can be a game changer for children experiencing parental detention. School staff are often the child's first point of contact outside the family. This gives them the opportunity, if equipped with enough tools and awareness, to recognise the child's distress and to meet the child's needs (Children of Prisoners Europe, 2017). Moreover, schools can also help children boost their resilience (Lynn, 2017). It is not uncommon for a teacher, who could be aware or not, to work with a student with one or more incarcerated parents.

Unfortunately, teachers and school staff are not always aware of the issue of students with parents in prison. In order to reach a good level of consciousness, teaching staff could be provided with information, resources and lesson plans to approach and understand children with imprisoned parents, as well as to raise awareness among other students (Lynn, 2017).

The question becomes: how to raise awareness among school staff and especially teachers? As suggested by Morgan, Leeson and Carter Dillon (2013), it could be effective to use leaflets or posters to raise awareness among school staff and to make children and families realise that the school is paying attention to the issue (Sack, Seidler, 1978; Mazza, 2002). Another useful tool to inform teachers is offering training on the effects of parental imprisonment on children, how to recognise children's distress, and how to support this vulnerable group (Morgan *et al*., 2013).

6.1 Case study (role of the school): Families Outside

Families Outside is the only national charity in **Scotland** working exclusively on behalf of families affected by imprisonment. It is in contact with thousands of families every year, providing them with information and support on a range of topics (Families Outside, n.d.). Indeed, Families Outside works to safeguard and help families experiencing imprisonment by providing direct support to affected people, by training and raising awareness among professionals in the field, and by developing policy and practices. Moreover, this association is a positive example of good practice in raising awareness and supporting children in schools. Families Outside has pioneered training sessions for teachers. As the Chief Executive of Families Outside stated

> *the main way that we as an organisation work in schools is to provide training for the teachers to let them know what the impact of imprisonment is and how they can support children in that situation* (Chief Executive of Families Outside, 11th March 2022).

These sessions are incredibly innovative because some of them take place inside the prison to

experience what it is like going into prison to visit a parent. Many teachers admitted that, before having this experience, they were not aware of this issue and that the training has had an impact on them and on the way they consider this group of children. To the question «Why is speaking in school so important? », the Chief Executive replied

> *I think that school is so important because it's the one place where every child is supposed to be, as you know that the children are going to be there. So, it's a really good way of reaching children who experienced this and not everybody as a family member will be visiting the prison, so you can provide support and information at the prison* (…) *One of the best ways of preventing offending is keeping people in school as long as possible* (Chief Executive of Families Outside, 11th March 2022).

6.2 Case study (role of the school): For Fangers Pårørende

Another striking example of an association working for children with imprisoned parents is For Fangers Pårørende (henceforth FFP). FFP works to help prisoners in **Norway**'s prisons and their social network to cope with detention. To summarise the incredible amount of work carried out by this NGO, FFP is able to provide advice on economic, social and community issues, applications, complaints, as well as on the situation of children and the family. Moreover, the NGO organises social and cultural events for children, young people, and adults who have a family member in prison. It also offers a counselling service. Focusing on the school field, FFP was and is active also in this sector. Indeed, this NGO has a project called «Subject aid» through which teachers have the opportunity to obtain information materials on parental imprisonment and to talk about the topic in class. FFP leaves its information materials, such as leaflets, in schools, to raise and spread awareness among school staff. Through this project, FFP provides teachers with a package with films, a questionnaire, and information data that can be used in the classroom to teach lessons. The Senior Advisor of For Fangers Pårørende stated that

sometimes teachers and social workers at schools call us because they experience having a child in school that has parents or another family member in prison and they call us to get advice and sometimes they can come and have a talk with us mainly on their own and maybe sometimes also with the child and the parents (Senior Advisor of For Fangers Pårørende, 16th March 2022).

Moreover, during the interview, the Senior Advisor said that FFP organised a workshop in schools where they presented a roleplay and then asked the class what they would do if they were in that child's shoes. That is a way of also raising awareness among students and trying to destroy the taboo around imprisonment. When asked about the role of schools and teachers in the child's future, the Senior Advisor responded that it is important to give children a positive and safe environment, to make them comfortable to open up and to provide support.

6.3 Case study (role of the school): the School Zone

The School Zone is a service at the HMP Parc (**Wales, UK**) accessible to all fathers present in the jail, according to the child's best interest and only if there are no measures or restrictions in place. It offers support to fathers, their children and families through the active and multilateral partnership with children's schools. This holistic project is an element of HMP Parc's Invisible Walls model and promotes engagement with imprisoned fathers by demonstrating the importance of keeping fathers connected with their children's education. The

School Zone project is the first service of its kind to be run within a British and European prison facility. It consists of three main interventions: school reports and updates, children's showcase events and the You and Me Club.

Regarding the School reports and updates, reports are sent by the school to the School Zone coordinator who scans them and shares them with the father. The imprisoned parent responds to the school by thanking them and writing a short letter to their child, which is delivered through the school. In this way, schools share quarterly school reports with fathers, providing them with their child's progress, and fathers can respond to the school and their child.

Children's Showcase Events have been delivered at HMP Parc since 2014. This intervention mirrors a parent-teacher event that takes place in schools every school term, but it is organised inside the prison with imprisoned fathers. Teachers are invited to the prison visiting room to meet the father and show him the schoolwork, while the child and mother or carer are also present. Since 2014, 351 children and over 240 schools across South Wales have participated in these Children's Showcase (Children of Prisoners Europe, 2022).

The You and Me Club takes place in the visiting room once a month. The main aim of this initiative is to maintain close relationships between imprisoned fathers and their children through structured «learning together» interventions including storytelling, art, drawing, writing and board games. This is an incredible way for children to interact with their fathers through a one-to-one activity which is usually extremely appreciated by children.

6.4 Questionnaire to examine the awareness level of teachers of students with imprisoned parents.

As part of the thesis project, the student realised a questionnaire with the aim of examining the awareness level of teachers in the Italian school system to understand whether these professionals are aware of the presence of underage students with at least one imprisoned parent in their classrooms. The questionnaire is a useful tool, both on an academic level, to get a picture of information or misinformation on the issue, and on a personal level, for teachers, to discover this social emergency.

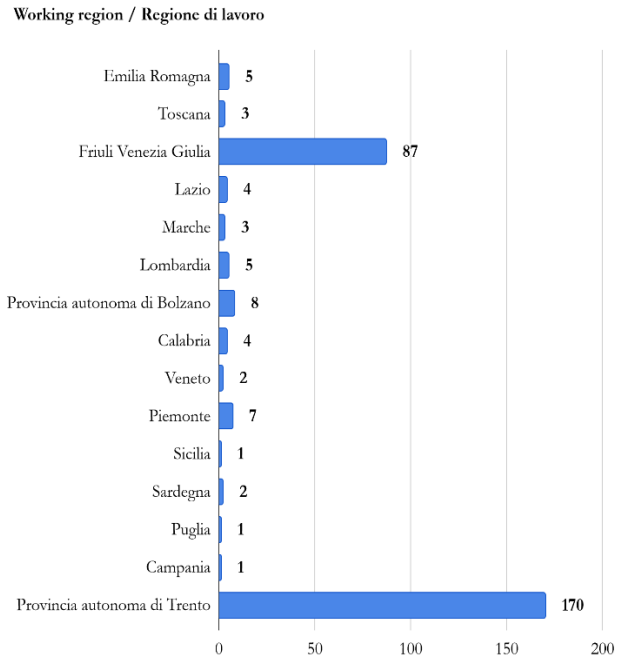
It was hypothesised that a low number of teachers were aware of the issue and/or the presence of students with one or more parents in prison, with few local awareness-raising activities for professionals.

Analysing the data collected (303 responses), most of the respondents are currently teaching in High schools (40.09%) and have been working for 0-10 years (27.7%) or 10-20 years (27.1%). However, 42.9% of the respondents stated that they have also worked in different educational institutions (e.g.: kindergarten and primary school). The majority of them work in the Provincia Autonoma di Trento (56.1%) and in Friuli Venezia Giulia (28.7%) which means that here the questionnaire was more widely distributed.

The question «Considering your entire teaching career, do/did you know under-age students with at least one parent in prison? » is the core of the questionnaire. 180 respondents answered that they had not met a student with at least one parent in prison, versus 123 who answered "yes". The thesis writer expected a larger gap between teachers who had not met and the ones who had met a child experiencing parental imprisonment. Most of the 123 teachers have only met one child experiencing parental incarceration in their professional career (41 respondents), while 31 teachers answered that they had encountered two children in the same situation.

According to the data, the main way in which teachers learned about the detention of a student's parent is through their colleagues (27), directly from the student (24), from social services (19), and during class councils (18). Some teachers (17) stated that the other parent told them about the partner's detention. It is interesting that 4 teachers (two in Friuli Venezia Giulia and two in Trento) mentioned the mass media as the way they discovered the imprisonment of a student's parent.

Figure 2 Working regions of the respondents



98.3% of the respondents stated that they had not been involved in any kind of awareness-raising training or course, while only 5 out of 303 respondents had participated in some educational activities. This information is important and contributes to the conclusion that the level of awareness depends mostly on personal experience, and it is not provided by organised courses. However, 80.5% of the teachers stated that they were ready and willing to participate in any activities regarding children with imprisoned parents in order to better understand this situation and the child's needs and rights. This information underlines that teachers' motivation is high, professionals seem interested in the topic, motivation is present "from below", but there are still no initiatives "from above".

Figure 3 Teachers' participation to awareness-raising courses

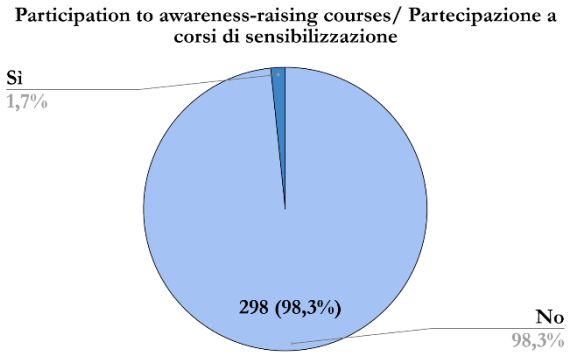
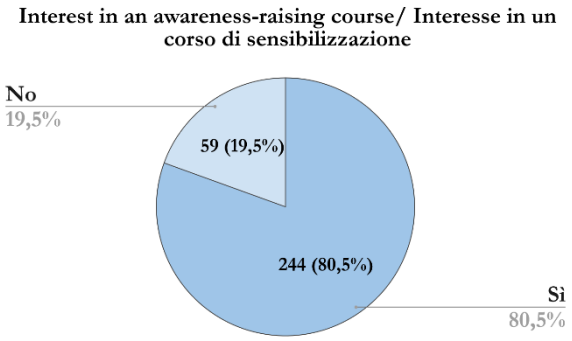


Figure 4 Interest of the respondents in participating in an awareness-raising course



244 out of 303 (80.5%) answered that the survey was useful, while 59 considered it irrelevant, mostly because they wanted to receive information from the survey.

Analysing the limits of this research, it is important to highlight the lack of scientificity and criteria in the implementation, dissemination, and analysis of the questionnaire, and consequently, the unreliability and

non-scientific nature of the results, which are more a source of qualitative than quantitative information.

Moreover, some critical issues have been identified regarding the way the questionnaire was developed and structured, such as the lack of a dedicated and proper section for entering the social and demographic characteristics of the respondents; the lack of an adequate pre-test before sharing the questionnaire; and critiques about some questions. Dealing with sharing issues, the questionnaire was sent to School Regional Offices which apparently cannot send emails to all regional schools. The questionnaire was also shared via social media and social networks, but this could create distortions. Moreover, it must be considered that the tool is a self-reported questionnaire, and this could imply that the person does not know how to fill in the document causing an incorrect answer. Furthermore, there is no analysis of verbal and non-verbal communication, important data for understanding the frame of the actual answers.

Furthermore, we do not have data for all 20 Italian regions and some areas have an incredibly high response rate (e.g.: teachers working in the Provincia Autonoma di Trento are 170 out of 303 replies) which implies that there was not a homogeneous rate of participation in the questionnaire, making the results not reliable, but only an indication.

Figure 5 Map representing working regions of respondents of the questionnaire

7. Conclusion

This article has examined the situation of children with imprisoned parents in Italy and Europe, with the aim of understanding why these minors can be defined as victims. Indeed, children experiencing parental imprisonment can suffer from psycho-social, economic and practical consequences as well as a higher risk of antisocial or criminal behaviour than their peers without this experience (Fritsch, Burkhead, 1981; Murray, Farrington, 2005; Glover, 2009; Philbrick *et al.*, 2014; Filograsso, Nardone, 2016; Mazza, 2002; Musi, 2012; Bambinisenzasbarre, 2009; Paris, 2017). Moreover, this vulnerable group is often unseen by part of society, as it can be observed from the lack of laws and rules safeguarding these minors. For these analysed reasons, it is possible to describe children with imprisoned parents as «forgotten children», «collateral victims», «hidden victims of imprisonment» or «orphans of justice» (Philbrick *et al.*, 2014, p. 17), also considering Gordon's statement: «It is clear that the family, both adults and

children, are sentenced too when a parent goes to prison» (2018, p. 1). However, it is important to highlight that the awareness of children with imprisoned parents is slowly increasing, especially thanks to many research activities and different associations and organisations working to support these children.

With regard to the condition of children with imprisoned parents in Italy, they are often considered on the legislative level as tools to reduce their parents' recidivism or help their social reintegration, with only a few exceptions that take into account their best interests. Children can stay with their parents in conflict with the law under specific conditions in prison nurseries, in the so-called ICAM and in protected houses. However, it is commonly recognised that the penitentiary environment is not safe for a child, therefore alternative sentences to detention should be provided to people with children.

The situation in other European countries is not that different from the Italian one. In many countries children can stay with their parents in penitentiary institutions, but there is no common and shared age limit. Despite that, it is internationally acknowledged the importance of providing a safe, suitable and well-equipped environment for the minors residing in prison.

The most innovative part of this article is the one dedicated to the analysis of the role of schools in supporting students with at least one imprisoned parent. Indeed, schools can offer support and protection for children as well as provide them a safe space where they can open up and be understood. However, school staff not always is aware of the presence of students experiencing parental detention (Morgan *et al.*, 2013; Children of Prisoners Europe, 2017). Leaflets, posters, and awareness-raising trainings could be a great way to make teachers aware of this situation.

A questionnaire was realised and shared among teachers of the Italian school system to understand their awareness level of children with parents in conflict with the law. Through the analysis of the results, it can be understood that most teachers do not have a high level of awareness of this social issue, and more than half of respondents report that they have never had a student experiencing parental imprisonment in their class (however, this information is not reliable, as analysed in the article). Data highlight the fact that few awareness-raising courses are offered on the Italian territory, therefore professionals recognise and acknowledge this social issue only if they had personal experiences with students having one or more parents in prison. Despite that, rates of motivation and curiosity regarding the topic of children with imprisoned parents and how to support them are relatively high, and that is a positive factor. With this in mind, schools should provide more courses and workshops about this issue to provide professionals with information and therefore to meet children's needs and rights. This research is innovative because there are no data about students experiencing parental imprisonment and about the level of awareness among teachers, therefore this could be a starting point for a deeper and more structured national study.

To conclude, it is hoped that this comparative research has been useful to obtain a clear picture of the situation of children with imprisoned parents and organisations working for and with them in Italy and in Europe. However, the aim is that there will be more studies regarding this social issue because children experiencing parental imprisonment are still often unseen.

Bibliography

1. Bronfenbrenner, U. (1979). *The Ecology of Human Development. Experiments by nature and design*. United States of America, Harvard University Press.
2. Farrington, D. P. (2002). Families and crime. In J. Q. Wilson & J. Petersilia (Eds.), *Crime: Public policies for crime control* (pp. 129-148). Institute for Contemporary Studies Press.
3. Filograsso, I. & Nardone, R. (2016). Rilegato come un libro. Raccontare e raccontarsi in carcere per ripensarsi padri senza sbarre. MeTis, anno VI, numero 1, 63-73.
4. Fine, B. (1977) Labelling theory: an investigation into the sociological critique of deviance. *Economy and Society*, 6(2), 166-193, doi: 10.1080/03085147700000003
5. Fritsch, T.A. & Burkhead, J.D. (1981). Behavioral reactions of children to parental absence due to imprisonment. *Family Relations*, 30(1), 83-88. doi: 10.2307/584240
6. Gordon, L. (2018). *Contemporary Research and Analysis on the Children of Prisoners: Invisible Children*. United Kingdom, Cambridge Scholars Publishing.
7. Halton, L. & Townhead, L. (2020). *Children of Incarcerated Parents: International Standards and Guidelines*. Quaker United Nations Office.
8. Johnson, E. I., Arditti, J. A., & McGregor, C. M. (2018). Risk, protection, and adjustment among youth with incarcerated and non-resident parents: A mixed-methods study. *Journal of Child and Family Studies*, *27*, 1914–1928. https://doi.org/10.1007/s10826-018-1045-0
9. Kjellstrand, J., Yu, G., Eddy, J. M., & Martinez, C. R. (2018). Children of incarcerated parents: Developmental trajectories of externalizing behavior across adolescence. *Criminal Justice and Behavior*, *45*(11), 1742–1761. https://doi.org/10.1177/0093854818785400
10. Kremer, K. P., Poon, C. Y. S., Jones, C. L., Hagler, M. A., Kupersmidt, J. B., Stelter, R. L., Stump, K. N., & Rhodes, J. E. (2020). Risk and resilience among children with incarcerated parents: Examining heterogeneity in delinquency and school outcomes. *Journal of Child and Family Studies*, *29*, 3239–3252. https://doi.org/10.1007/s10826-020-01822-1
11. Hirschl, R. (2008), *The Judicialization of Politics*, in G.A. Caldeira, R.D. Kelemen, K.E. Whittington (eds), The Oxford Handbook of Law and Politics, Oxford, Oxford University Press.
12. La Vigne, N.G., Davies, E. & Brazzell, D. (2008). *Broken Bonds. Understanding and Addressing the Needs of Children with Incarcerated Parents*. Washington DC, Urban Institute.
13. Lauwereys, H. (2020). Het belang van het kind in het Belgische straftoemetingsrecht: de visie van correctionele rechters. *TIJDSCHRIFT VOOR STRAFRECHT*, (2), 98-111.
14. Mazza, C. (2002). And then the world fell apart: the children of incarcerated fathers. *Families in Society,* 83 (5/6), 521-529.
15. Murray, J & Farrington, D.P. (2008). The effect of Parental Imprisonment on Children. *Crime and Justice: Review of Research*, 37, 133-206
16. Murray, J. & Farrington, D.P. (2005). Parental Imprisonment: Effect's on boys' antisocial behaviour and delinquency through the life-course. *Journal of Child Psychology and Psychiatry*, 46 (12), 1269- 1278
17. Musi, E. (2012). Rimanere padri "dentro". Il diritto alla famiglia. In V.Iori, A.Augelli, D.Bruzzone & E.Musi (A cura di), *Genitori comunque. I padri detenuti e i diritti dei bambini* (pp.53-80). Milano: Franco Angeli s.r.l.
18. Robins, L., West, P., & Herjanic, B (1976). Arrest and delinquency in two generations: A study of black urban families and their children. *Journal of Child Psychiatry and Psychology*, 16, 125-140
19. Sack, W.H. & Seidler, J. (1978). Should children visit their parents in prison? *Law and Human Behavior*, 2(3), 261-266
20. Sack, W.H. (1977). Children of imprisoned fathers. *Psychiatry*, 40, 163-174.
21. Salvetti, M. (2019). Padre e figlio: un legame oltre le sbarre (sezione VII). *Giurisprudenza penale*, 2-bis, 331-339.

22. Sicurella, S. (2020). *Vittimologia, teorie e definizioni*. [PowerPoint slides]. Scienze Criminologiche per l'Investigazione e la Sicurezza, Università di Bologna.
23. Social Care Institute for Excellence [SCIE] (2008). *Children's and families' services SCIE guide 22. Children of prisoners – maintaining family ties*. SCIE.
24. Vanhaelemeesch, D., Vander Beken, T., & Vandevelde, S. (2014). Punishment at home: Offenders' experiences with electronic monitoring. *European Journal of Criminology*, 11(3), 273–287. https://doi.org/10.1177/1477370813493846
25. Weijer, S., Bijleveld, C., & Blokland, A. (2014). The Intergenerational Transmission of Violent Offending. *Journal of Family Violence*. 29. 10.1007/s10896-013-9565-2
26. Western, B. & Petit, B. (2010). *Collateral costs: incarceration's effect on economic mobility*. Washington DC, The Pew Charitable Trusts.

Sitography

1. Bambinisenzasbarre (2009). *Spazio giallo*. http://www.ristretti.it/areestudio/affetti/bambini/spazio_giallo.pdf
2. Bambinisenzasbarre (n.d.-a). *Bambinisenzasbarre Onlus, for the rights of children with imprisoned parents*. https://www.bambinisenzasbarre.org/chi-siamo/, 22.09.2022
3. Bambinisenzasbarre (n.d.-b). *Carta dei diritti dei figli dei genitori detenuti*. https://www.bambinisenzasbarre.org/carta-dei-diritti-dei-figli-dei-genitori-detenuti/, 19.09.2022
4. Bambinisenzasbarre (n.d.-c). *About us*. https://www.bambinisenzasbarre.org/about-us/#activ, 23.09.2022
5. Bambinisenzasbarre (n.d.-d). *Telefono giallo: cellulare, email, app*. https://www.bambinisenzasbarre.org/telefono-giallo-app/, 23.09.2022
6. Centers for Disease Control and Prevention (2022). *Fast Facts: Preventing Adverse Childhood Experiences*. https://www.cdc.gov/violenceprevention/aces/fastfact.html, 01.09.2022
7. Children of Prisoners Europe (2016). Community sanctions and restorative justice. *European Journal of Parental Imprisonment*, 3. https://childrenofprisoners.eu/wp-content/uploads/2019/02/EJPI-English_01_2016_Summer_web.pdf
8. Children Of Prisoners Europe (2017). *Campaign 2017*. https://childrenofprisoners.eu/campaign-2017/, 15.10.2022
9. Children Of Prisoners Europe (2018). *Child Talk a Reflective Toolkit for Prison Administrators and Staff on Supporting the Child-Parent Relationship*. https://childrenofprisoners.eu/wp-content/uploads/2019/09/Prison-Toolkit_2019.pdf
10. Children Of Prisoners Europe (2019a). *Keeping children in mind. Moving from 'child-blind' to child-friendly justice during a parent's criminal sentencing*. https://childrenofprisoners.eu/wp-content/uploads/2022/04/Keeping-children-in-mind-toolkit.pdf
11. Children Of Prisoners Europe (2019b). *Implementation Guidance Document*. https://childrenofprisoners.eu/wp-content/uploads/2020/06/IGD_2019.pdf
12. Children Of Prisoners Europe (2021). *Impacts of pre-trial detention procedures on children with parents in conflict with the law*. https://childrenofprisoners.eu/wp-content/uploads/2022/01/Impacts-of-pre-trial-detention-procedures-on-children-with-parents-in-conflict-with-the-law_COPE.pdf
13. Children Of Prisoners Europe (2022). "*My parents have been arrested, what now? Public policies for the future". Conference Outcome Report*. https://childrenofprisoners.eu/wp-content/uploads/2022/10/2022-Cascais-Conference-Report.pdf
14. Children Of Prisoners Europe (n.d.-a). *Who we are*. https://childrenofprisoners.eu/who-we-are/, 04.12.2022
15. Children Of Prisoners Europe (n.d.-b). *Children separated from parents*.

https://childrenofprisoners.eu/facts_and_figures/children-separated-from-parents/, 02.09.2022
16. Children Of Prisoners Europe (n.d.-c). *Training programmes for the implementation of the Memorandum of Understanding*. https://childrenofprisoners.eu/database/training-programmes-for-the-implementation-of-the-memorandum-of-understanding/, 23.09.2022
17. Children Of Prisoners Europe (n.d.-d). *La partita con papà - The game with dad*. https://childrenofprisoners.eu/database/la-partita-con-papa-the-game-with-dad/, 23.09.2022
18. Children Of Prisoners Europe (n.d.-e). *The Network*. https://childrenofprisoners.eu/the-network/, 09.10.2022
19. Council of Europe (2018a, April 4). European Committee on Crime Problems (CDPC). *Explanatory Memorandum to Recommendation CM/Rec(2018)5 concerning children with imprisoned parents*. https://rm.coe.int/explanatory-memorandum-to-cm-recommendation-2018-5-eng/16807b3439
20. Crétenot, M. & Liaras, B. (2013). *Prison conditions in France*. Antigone Edizioni. http://www.prisonobservatory.org/upload/PrisonconditionsinFrance.pdf
21. Del Grosso, I. (n.d.). *Documento tavolo 3 donne detenute*. https://www.giustizia.it/resources/cms/documents/sgep_tavolo3_allegato2.pdf
22. EuroPris (n.d.-a). *Table of Recommendations and Practices*. https://www.europris.org/recommendations/?export=true
23. Families Outside (n.d.). *About us*. https://www.familiesoutside.org.uk/about-us/, 16.10.2022
24. Glover, J. (2009). *Every night you cry. The realities of having a parent in prison. Believe in children*. Barnardo's. https://www.bl.uk/britishlibrary/~/media/bl/global/social-welfare/pdfs/non-secure/e/v/e/every-night-you-cry-the-realities-of-having-a-parent-in-prison.pdf
25. Lynn, H. (2013). Police, Judges & Sentencing. Arrests, Trials & Children's Rights. *Justice for Children of Prisoners*. Children Of Prisoners Europe. https://childrenofprisoners.eu/wp-content/uploads/2019/02/JudgesSentencingNewsletter.pdf
26. Lynn, H. (2017). Applying Human Rights Education principles when discussing parental imprisonment in the classroom. In H. Lynn (Ed.), First port of call: The role of schools in supporting children with imprisoned parents, 4-6, Children Of Prisoners Europe. *European Journal of Parental Imprisonment, 6*. *https://childrenofprisoners.eu/wp-content/uploads/2019/02/EJPI_06_2017-ENGLISH_Web.pdf*

doi: 10.14664/rcvs/248

Crimini ambientali ed ecomafie: un argomento criminologico tuttora complesso

Crimes environnementaux et écomafias : un sujet criminologique encore complexe

Environmental crimes and ecomafias: a criminological topic still complex

*Eleonora Medina**

Riassunto
Questo articolo nasce con l'intenzione, per quanto possibile, di mostrare l'attuale situazione inerente alla materia ambientale in campo criminologico, partendo da ricerche di natura etimologica, letteraria, storica, giuridica, investigativa e vittimologica. La natura dello studio trattato è quindi multidisciplinare e ha l'obiettivo di mostrare come in criminologia i crimini ambientali siano ancora in fase di sviluppo, ma soprattutto come sia necessario ampliare il campo di azione e di ricerca attraverso argomentazioni, analisi ed interviste ad esperti del settore. Questo ampliamento servirebbe a dimostrare una natura più complessa e assai meno semplicistica del fenomeno, che risulta tutt'oggi limitata a determinati settori; un suo possibile riconoscimento potrebbe portare in un futuro allo sviluppo di una consapevolezza, di una presa di coscienza che, da un lato, favorirebbe la prevenzione e l'attenzione delle persone e, dall'altro, seppur con molte difficoltà ed ostacoli, potrebbe spingere gli organi competenti a prendere in considerazione il fenomeno nella sua forma più completa e quindi ad apportare delle modifiche normative.

Résumé
Cet article se propose d'interroger la façon dont les crimes environnementaux sont abordés en criminologie, en se basant sur des études étymologiques, littéraires, historiques, juridiques, d'investigation et victimologiques. Il s'agit donc d'une recherche multidisciplinaire visant à montrer que l'analyse des crimes environnementaux est encore en cours de développement en criminologie et, surtout, qu'il est nécessaire d'élargir le champ d'action et d'étude en incluant des arguments, des analyses et des entretiens avec des experts. Cet élargissement servirait à démontrer la nature plus complexe et beaucoup moins simpliste du phénomène, encore limité à certains domaines, et dont la reconnaissance éventuelle pourrait conduire dans le futur à une meilleure prise de conscience. Celle-ci, d'une part, favoriserait la prévention et l'attention des personnes, et, d'autre part, bien qu'avec de nombreuses difficultés et obstacles, pourrait inciter les pouvoirs publics à prendre en considération le phénomène et donc à apporter des modifications législatives.

Abstract
The purpose of the following article is to illustrate the state of the art with regard to research on environmental crimes in the field of criminology. The article is based on a multidisciplinary research approach which encompasses etymology, literature, history, law, criminal investigation as well as victimology. The aim of this research work is to highlight, through arguments, analyses and interviews with experts, how environmental crimes are still developing as an area of research in criminology and why it is necessary to widen its field of action and study. If this happens, the complexity of environmental crimes would be demonstrated and would not be limited to specific sectors as it is today. If this complexity is recognised, awareness about the topic could be raised in the future, leading to the promotion of preventive measures and attracting people's attention. Furthermore, although facing many difficulties and obstacles, competent bodies could take the topic into consideration and modify the legislation.

Key words: ambiente, diritto, vittime, mafia.

* Laureata in Scienze Criminologiche per l'investigazione e la Sicurezza – Università di Bologna.

1. Introduzione

In un primo momento, appare significativo ed indispensabile tentare di tracciare una via, una direzione a questo lavoro, introducendo, seppur brevemente, quale sia il suo scopo, quali risultati sono attesi e soprattutto le possibili difficoltà che si potranno trovare durante la sua trattazione. Questo articolo nasce con l'intenzione di sottolineare come il tema e la questione ambientale non siano sufficientemente sviluppati, ovvero di come si limiti la loro trattazione ad un aspetto prettamente naturalistico; questo vale in tutti i campi, da quello storico e letterario fino a quello criminologico e giuridico. L'obiettivo finale è di dimostrare attraverso una ricostruzione multidisciplinare, che abbraccia storia, letteratura, etimologia, scienze sociali e giurisprudenza, che sia possibile ampliare lo sguardo e la percezione della questione ambientale, soprattutto in campo criminologico, con un conseguente sviluppo anche vittimologico.

Si riporteranno inoltre interviste di figure di spicco che operano all'interno del settore ambientale di pubblica sicurezza[1] e non solo, con lo scopo di riportare aggiornamenti sia su alcuni dei fenomeni criminosi ambientali più noti, come il traffico illecito di rifiuti e le navi a perdere, sia su possibili modifiche normative a livello nazionale.

Dall'altra parte, ci si aspettano molte difficoltà in questa dimostrazione, sia perché da un lato l'ambiente è stato quasi sempre trattato ed inteso con un'accezione naturalistica, sia perché questa concezione è ormai intrinseca nella cultura e percezione generale, rendendo quindi arduo provare a svincolare quest'interpretazione vecchia e comune dalle menti dei più. Allo stesso modo, qualora si dovesse anche riuscire a dimostrare questo possibile ampliamento della questione ambientale, un cambiamento repentino e soprattutto effettivo appare assai difficile vista la sua mole e la quantità dei vari sottoargomenti: potrebbe essere un processo lungo e tortuoso, che incontrerebbe difficoltà in particolar modo dal punto di vista giuridico.

Nonostante tutti questi possibili ostacoli, si è fermamente convinti che un ampliamento sia necessario, doveroso e possibile, sia per una questione di onnicomprensività dei fenomeni ambientali, che di arricchimento della materia stessa, ancora giovane e acerba. Si confida inoltre che questo lavoro possa contribuire a sviluppare consapevolezza e a rendere più consci le persone in maniera tale da implementare l'attenzione a questi fenomeni così da poterli prevenire, sia sotto l'aspetto criminologico ed investigativo, che vittimologico.

1.1 La relazione uomo-ambiente: come si è sviluppato il rapporto nel corso del tempo, tra letteratura, storia e criminologia.

L'essere umano ha sempre interagito con l'ambiente e questo è un dato di fatto assodato. Tuttavia, quando si parla di ambiente in campo criminologico, come appurato anche dai codici giuridici di riferimento o dalle leggi, questo viene spesso identificato con un qualcosa di prettamente naturale: gli alberi, i fiumi, i parchi, il mare, l'oceano e via dicendo.

Eppure, l'ambiente non è solo questo, anzi. Se si prende come riferimento l'etimologia latina del termine ambiente, si riscontrerà come questo prenda in considerazione un numero molto grande di elementi al suo interno, non limitandosi quindi solo a quelli naturali.

La parola deriva infatti dal latino, da *Ambire*, in

[1] Più nello specifico Arma dei Carabinieri e Capitaneria di Porto.

particolare dalla sua forma al participio presente, *Ambiens, -entis*. Il verbo in questione è composto dal prefisso *Amb,* col significato di "intorno, all'intorno", ed *Ire*, cioè "andare". Se si uniscono i due significati e si fa riferimento al participio presente, il termine ambiente dovrebbe letteralmente significare ciò che sta intorno, ciò che circonda[2]. Questo amplierebbe quindi il campo di interesse della materia, non limitandolo, perciò, per quanto concerne la relazione con l'uomo, solo ad un aspetto prettamente naturalistico, come accade ora, ma come anche è accaduto in passato.
Se si osserva infatti la letteratura nazionale ed internazionale ed i contributi degli storici ambientali, si noterà come, nella quasi totalità dei casi, i riferimenti all'ambiente fossero di tipo naturalistico.

Questo è evidente già dall'antica Grecia, come nell'opera *Crizia* (circa IV secolo a.C) di Platone, nel quale il filosofo tratta anche il rapporto tra l'uomo ed il manto boschivo; ma anche nell'antica Roma, attraverso le opere di Plinio il Vecchio, con la sua *Naturalis Historia*, la cui prima pubblicazione è stata stimata tra il 77 ed il 78 d.C., ma soprattutto di Virgilio, che attraverso le *Bucoliche* ha descritto un ambiente naturale idilliaco e a cui aspirare.

Anche nel medioevo questa caratteristica era ben visibile, basti pensare ad esempio al *Cantico delle Creature* di San Francesco, in cui, in chiave ovviamente teologica, vi è un'esaltazione dell'ambiente naturale e delle sue caratteristiche: il sole, l'acqua, il fuoco, la terra ed il vento, per citarne alcuni.

Qualche anno più tardi, anche Boccaccio contribuirà in questo attraverso il *Decameron*, in cui l'ambiente rappresenta un elemento salvifico, in quanto protettore dei protagonisti dalla peste nera che imperversava nel Trecento.

In tempi più recenti non ci si è discostati molto da questa visione, anzi: già Verga nel suo romanzo *Storia di una capinera*, che non ha però come punto centrale il rapporto tra uomo e ambiente, descrive nella prima parte del libro la campagna in cui si trova la protagonista, a Monte Ilice, e come questa abbia su di lei un potere salvifico e di conforto, poiché il romanzo è ambientato durante l'epidemia di colera che colpì la città di Catania, e non solo, nel 1854; al contempo, Verga narra la sensazione di libertà, spensieratezza e benessere che la sua protagonista prova nello stare in mezzo alla natura.
Visione analoga, e precedente a quello dello scrittore siculo di circa un secolo, la si ritrova ne *I dolori del giovane Werther,* di Goethe. Sebbene anche questo non abbia come focus principale l'ambiente, il rapporto che vi è tra questo ed il giovane protagonista è indiscutibile: basti pensare al suo desiderio, una volta suicidatosi, di essere seppellito in mezzo a due tigli, o di come nel giorno 18 Agosto abbia manifestato i suoi sentimenti ed il suo stato d'animo a contatto con la natura circostante, ritrovandovi pace e serenità.
In mezzo a tutti questi esempi, pochi sono quelli che ampliano lo sguardo e hanno il coraggio di trattare l'ambiente come qualcosa di altro, oltre all'aspetto prettamente naturale, tra questi vi è Parini, nel 1700, e Calvino, nel 1900.
Parini, infatti, nella sua Ode, *La salubrità dell'aria*, si lamenta e critica le condizioni dell'aria della città di Milano, imputando le cause di questa condizione ad una mala gestione dell'amministrazione ed ai suoi abitanti, mentre loda e talvolta invidia gli abitanti della campagna che possono godere di un ambiente più sano.

[2] Questa definizione non ha valenza solo per gli esseri umani, ma si può considerare in riferimento a qualsiasi essere vivente, in quanto nella sua definizione etimologica non sono rintracciabili riferimenti specifici ed esclusivi all'uomo.

Calvino anche tratta di un contesto urbano nel suo racconto *La nuvola di smog*, in cui descrive il grigiore e l'inquinamento e le condizioni insalubri in cui abitato gli abitanti di una città immaginaria.
Entrambi gli autori mettono al centro la condizione dell'aria, che rientra appieno negli aspetti naturali, ma con la differenza che in questi due casi, gli scrittori portano all'attenzione un contesto differente, ovvero quello delle città.

1.2 L'ambiente e la storia: alcuni casi di contatto

Oltre ad un punto di vista prettamente letterario, ve n'è anche uno storico, ed è proprio questo che permetterà di comprendere il rapporto intrinseco e duraturo tra l'ambiente e l'uomo, seppur continuando a mantenere, nella quasi totalità dei casi, un'interpretazione di ambiente di stampo naturalistico.
Gli storici ambientali nel corso del tempo si sono dilettati nell'analisi più o meno approfondita dei differenti aspetti naturalistici e ambientali, il professor Jhon McNeill, ad esempio, è stato uno degli storici ad aver sviscerato maggiormente e sotto più aspetti la storia ambientale, soffermandosi però principalmente sul XX secolo (McNeill, 2020), mentre altri autori, come la professoressa Corona, la quale si è concentrata sulla situazione italiana, ed il professor Mosley, hanno rivolto la loro attenzione su meno sfaccettature, ma hanno cercato di coprire un tempo maggiore, partendo la prima all'incirca dal periodo unitario d'Italia (Corona, 2015), il secondo invece si è impegnato a ricoprire un periodo assai più lungo, analizzando anche casi del Quattrocento, e su scala globale (Mosley, 2013).
Tutti e tre, tuttavia, hanno trattato nello specifico dei casi e delle situazioni che risultano assolutamente attuali e alcune di particolare interesse anche per il mondo criminologico: tra questi vi è il disboscamento, le sue conseguenze e le condizioni del suolo, ed il trattamento delle acque, prettamente dolci. Tutti, lo ripetiamo, hanno mantenuto un approccio prettamente incentrato sulla natura, ma l'esposizione dei loro studi servirà come punto di partenza per fare riferimento a casi moderni che presentano delle similitudini col passato.
Il disboscamento è stato, ed è tutt'ora, purtroppo, un fenomeno assai diffuso: impiegato in tutto il mondo e fin dai periodi più antichi, per Corona vi erano tracce consistenti già nel periodo unitario (Corona, 2015), mentre per McNeill e per Mosley già dai tempi degli antichi romani (Mosley, 2013; McNeill, 2020): questo infatti non dovrebbe sorprenderci molto, poiché in passato dimore, utensili e mezzi erano prodotti principalmente da questo materiale, inoltre il disboscamento serviva, e serve tutt'ora, anche per fare spazio alle colture per la produzione di cibo ed ai pascoli.
In un primo momento questo fenomeno potrebbe non aver dato segno di chissà quali conseguenze, eppure con lo scorrere del tempo si è visto un progressivo impoverimento del suolo e soprattutto la sua erosione.
Il secondo aspetto è quello che, da un punto di vista criminologico ha più rilevanza, in quanto «[...] L'erosione espone il terreno a fenomeni franosi dovuti all'indisciplina delle acque piovane di scorrimento e può dunque essere la causa di un aumentato rischio idrogeologico su di un territorio in caso di fenomeni precipitativi intensi, quali alluvioni, o anche di situazioni di conclamato dissesto idrogeologico [...]»[3]. Ed è proprio il dissesto idrogeologico il cardine della situazione: l'Italia, oltre ad avere per "natura" una propensione a questa problematica, dovuta soprattutto per la sua

[3]Si veda: http://www.pratiarmati.it/caratteristiche-geotecniche/erosione-del-suolo/

conformazione territoriale (Corona, 2015), ha visto anche l'intervento dell'uomo come aggravante. Tra i fattori che peggiorano una situazione già così delicata, vi rientrano l'abusivismo edilizio e la conseguente cementificazione indiscriminata, che molto spesso sono gestiti da associazioni a delinquere, anche di stampo mafioso. Basti pensare ad uno degli ultimi rapporti di Legambiente: nel 2019 sono state 20 mila le nuove costruzioni abusive sul territorio nazionale e dal 2004 al 2020 solo una parte di queste, il 32,9%, è stata abbattuta[4].

Per quanto concerne invece le acque, tutti e tre gli autori hanno evidenziato il rapporto strettissimo tra queste e lo sviluppo delle città: l'acqua è l'elemento fondamentale per l'uomo, in quanto senza di essa è impossibile vivere, quindi l'essere umano ha sempre cercato di avere a disposizione fonti di acqua, soprattutto pulita, che spesso venivano ritrovate in sorgenti o in fiumi; sono proprio quest'ultimi una delle prime "vittime" della mano dell'uomo (Corona, 2015; Mosley, 2013; McNeill, 2020).

Era usanza in passato infatti che i rifiuti, quando non si sapeva dove locarli, venissero sversati nei fiumi, causando non solo un inquinamento del fiume stesso a partire da quel punto, ma generando poi problematiche anche lungo tutto il suo scorrere, provocando ad esempio epidemie. Anche per quanto riguarda il contesto italiano, molti sono i casi in cui si sono sversati rifiuti di varia natura nei fiumi[5], comportando un pericolo non solo per l'ambiente naturale, ma anche per i soggetti che entravano in contatto con quelle acque. In Italia basti pensare al fiume Oliva in Calabria in cui per anni sono stati sversati rifiuti di ogni genere, da quelli di tipo industriale, fino ai fanghi di depurazione[6].

Il mare anche è un elemento analizzato, ma solo da McNeill, e tra i vari esempi, si sofferma su quello nipponico che ha visto coinvolta la città di Minamata, in Giappone, ed il rispettivo golfo: a partire dal 1932, uno stabilimento chimico si mise a produrre un composto che aveva come elemento indispensabile per la produzione il mercurio. Fatto sta che i rifiuti dello stabilimento, impregnati di questo metallo, vennero riversati in mare. Gli effetti di questa azione si manifestarono inizialmente sugli animali: si riscontrò un'importante moria di pesci ed in seguito anche i gatti iniziarono a manifestare effetti di avvelenamento. Come ultima vittima, ovviamente, si arrivò anche all'uomo, la popolazione iniziò ad ammalarsi ed i bambini iniziarono a nascere con malformazioni e con danni cerebrali. Questa situazione venne risolta solo nel 1997 (McNeill, 2020).

Avvenimenti di una gravità tale riguardanti il mare, in Italia, per fortuna non ce ne sono mai stati, ma è innegabile che il Mar Mediterraneo sia stato utilizzato come "tappeto" per nascondere e far sparire rifiuti attraverso il fenomeno delle navi a perdere, navi su cui ancora non vi è una condanna definitiva.

Sempre McNeill riporta alcuni casi riguardanti il rapporto tra l'uomo e l'aria, o come preferisce lui, l'atmosfera, ed uno in particolare trova dei riscontri con un caso italiano.

Il distretto di Hanshin, una regione che comprende alcune delle città più importanti del Giappone, come Osaka e Kobe, dal 1890 al 1970 vide la

[4]Per approfondimenti, si veda: https://www.legambiente.it/comunicati-stampa/i-dati-del-rapporto-ecomafia-2020-nel-2019-in-aumento-i-reaticontro-lambiente/ e https://www.legambiente.it/?s=abbatti+l%27abuso

[5]Per approfondimenti, si veda: https://www.salernotoday.it/cronaca/sversamenti-rifiuti-denunce-carabinieri-noe-15-ottobre-2019.html e https://www.reggiotoday.it/cronaca/sversamenti-frantoi-controlli-e-denunce-nella-piana.html

[6]Per approfondimenti, si veda: http://www.comitatodegrazia.org/Blog/il-fiume-oliva-affogato-nei-rifiuti.html

propria area fortemente inquinata da industrie chimiche, metallurgiche, del cemento, il tutto sotto gli occhi degli organi preposti, i quali però riconoscevano in queste industrie un "interesse nazionale", non curanti quindi della popolazione locale che si ammalava sempre più e con maggior frequenza (McNeill, 2020).

Questo evento potrebbe richiamare il caso nostrano dell'ILVA di Taranto, le cui problematiche sono state "trattate" dalle autorità competenti ma la cui gravità e soprattutto pericolosità resta tuttora inalterata.

A questo punto si potrebbe riscontrare come anche gli storici, e solo in una piccolissima parte gli scrittori e i poeti, seppur involontariamente, abbiano trattato di crimini ambientali, pur mantenendo una visione quasi sempre legata all'ambiente naturalistico, non concedendo quell'ampliamento che abbiamo ritenuto necessario.

Si vedrà di seguito come purtroppo anche in campo criminologico vi sia una visione piuttosto statica del fenomeno.

1.3 L'ambiente in criminologia

Ufficialmente, la criminologia ambientale esisterebbe, ma rispetto agli altri argomenti della materia risulta assai più giovane e, soprattutto in Italia, gli studi in merito stanno inziando a svilupparsi solo nell'ultimo periodo. A livello internazionale, invece, la *green criminology* ha una diffusione maggiore e gli studi sono iniziati molto prima, tant'è che i suoi tre principali esponenti sono tutti di paesi anglofoni, e tra questi vi è anche colui che è ritenuto il "padre" della criminologia ambientale, il professor Michael Lynch, il quale ha iniziato i suoi studi intorno agli anni '80 del 1900 (Natali, 2015).

La materia quindi esiste, ma ha effettivamente una definizione unica ed univoca che accorda gli studiosi? Purtroppo, su questo la risposta dovrà essere negativa. Essendo un argomento oggettivamente giovane e di nicchia, i cui esponenti e studiosi sono relativamente pochi nell'insieme del mondo criminologico, non si è riusciti a trovare una definizione condivisa dalla comunità scientifica. Si prenderanno però in considerazione le tre definizioni che sono state riportate dai tre pilastri della materia, M. Lynch, nominato poc'anzi, R. White e P. Stretesky (Natali, 2015; Potter *et al.*, 2016).

Il primo riteneva che la criminologia ambientale dovesse «essere basata su una prospettiva politico-economica e che l'obiettivo non fosse soltanto quello di esporre le cause del danno ambientale, ma di proporre rimedi basati sull'azione politica o dei movimenti [...]» (Natali, 2015, p. 22). Questa definizione appare abbastanza ridotta, tuttavia, una visione più approfondita del pensiero di Lynch viene analizzata anche da G. R. Potter, A. Nurse, M. Hall e T. Wyatt, i quali riportano di come il suo pensiero sulla criminologia ambientale derivasse da una forma di "socialismo ecologico", da lui ribattezzata "alleanza verde/rossa", i cui esponenti tendono ad enfatizzare le disuguaglianze di ricchezza e di potere all'interno della società, comportando ad un maggior degrado ambientale, con i poveri e gli esclusi a sopportarne il peso (Potter *et al.*, 2016).

La visione di Lynch si basa quindi principalmente sul ruolo ricoperto dalla politica e dalla società, trovando in loro la causa delle conseguenze di tali atti.

White, invece, ha una visione più "legale" della disciplina e meno sociale. Lo studioso infatti aveva

riportato due definizioni, una del 2008 ed una nel periodo 2014/2015.

La definizione più vecchia risultava ermetica e concisa, e riportava di come la criminologia ambientale fosse la disciplina che si occupa dello studio del danno ambientale, delle leggi ambientali e della regolamentazione ambientale da parte dei criminologi (Potter, *et al.*, 2016).

La seconda amplia questo concetto e lo rende più complesso, in quanto «dovrebbe includere concezioni sia "legali" che "non legali" di crimini e di danno. Accanto ai crimini ambientali più comuni e noti […] tale definizione dovrebbe ricomprendere anche quei casi di danno ecologico che la legge penale in vigore non definisce come reati.» (Natali, 2015, p. 26).

Vi è quindi un'espansione della visione di White, che non si limita più solo ad un'interpretazione legale, ma fa rientrare nel fenomeno anche quei fatti e fenomeni che non sono riportati dalla legge penale.

L'ultimo autore, Stretesky, insieme a Lynch ed altri ricercatori, sviluppa un modello teorico secondo cui i danni e le problematiche ambientali sono legate alla mentalità capitalistica di aumentare e accrescere continuamente la produzione, ipotizzando quindi, verrebbe da pensare, l'idea che i danni ed i crimini ambientali siano determinati da un fattore prettamente di tipo economico, industriale (Potter *et al.*, 2016).

Stretesky non dà una definizione esaustiva di criminalità ambientale come hanno fatto i suoi colleghi, ma cerca comunque di definire il concetto di *green crime*, che identifica come «[...] un'azione che (1) può o meno violare norme esistenti e la legislazione ambientale; (2) ha quale effetto un danno ambientale identificabile; e (3) è riconducibile all'azione dell'uomo.» (Natali, 2015, p. 25).

Pertanto, la branca maggiore della criminologia ambientale ritiene che questa si debba focalizzare soprattutto su quei crimini che hanno come origine l'uomo, più precisamente il sistema politico-economico, ritrovando nel capitalismo la fonte primaria di questo problema. I crimini inoltre possono essere considerati tali pur non essendo iscritti nell'ordinamento giuridico.

Ciò lo si ritiene corretto, ma solo in parte. Gli autori di riferimento, abbiamo citato prima, sono tutti di origine anglosassone, il che non dovrebbe stupire se la loro interpretazione primaria del fenomeno si basa e si concentra quasi ed esclusivamente solo su questi aspetti, poiché molti crimini ambientali nei loro contesti di provenienza hanno spesso come protagonista principale aziende o industrie. Non tengono ad esempio conto della possibilità che questo fenomeno sia più diffuso, sembra che non ipotizzino la presenza in questo settore della criminalità organizzata, anche di stampo mafioso, di cui tratteremo più approfonditamente dopo.

Il che appare come una mancanza, poiché, anche se rispetto alla maggioranza dei casi trattati quelli che coinvolgano la criminalità organizzata siano inferiori, questo non vuol dire che non vadano presi in considerazione, anzi.

Osservando con maggior attenzione la letteratura internazionale inerente alla *green criminology*, si noterà di come l'attenzione non sia rivolta più solo verso quei crimini che toccano e riguardano principalmente l'uomo, bensì si stia spostando anche sulla flora e la fauna, quest'ultima in particolare.

Ad esempio, all'interno della pubblicazione da loro curata, Potter, Nurse ed Hall inseriscono svariati capitoli che trattano di crimini ambientali perpetrati nei confronti di animali selvatici, ad esempio i

rinoceronti, cacciati per i loro corni, o le tigri[7], le cui parti, una volta uccise, vengono impiegate per la medicina tradizionale Asiatica, o più semplicemente per il pellame, i denti e talvolta anche le ossa (Potter *et al.*, 2016).

Allo stesso modo, questo tipo di visione ed ampliamento è stato riportato anche nel testo curato da Walters, Solomon Westerhuis e Wyatt, nel primo capitolo, in cui Rob White include anche le specie animali e vegetali, sebbene lui inquadri il tutto in un contesto di *species justice* (White, 2013).

Questa visione trova in parte un collegamento con quanto analizzato da Legambiente in Italia attraverso il fenomeno delle zoomafie[8], eppure pare doveroso sottolineare di come si abbia avuto la sensibilità di trattare attivamente in questa branca di studio i crimini e le violazioni nei confronti degli animali e della flora, ma non si sia riusciti a fare un passaggio in più e ad inserirvi fenomeni assai più ampi, come il ruolo delle organizzazioni criminali[9], anche di stampo mafioso; attualmente sembra che la criminologia ambientale si stia spostando sempre di più verso l'aspetto ecocentrico della disciplina per quanto riguarda la ricerca, pur non abbandonando l'altra interpretazione, ovvero quella antropocentrica, ma non facendola fruttare appieno.

Uno spostamento di questo tipo comporta un necessario cambiamento anche nella visione vittimologica, in cui non si identifica più solo l'essere umano nel ruolo di vittima, sebbene questo sia oggetto della maggior parte della letteratura di settore, ma vi si fanno rientrare anche gli animali e la flora (White, 2011).

Con ciò, si tiene a dire che la criminologia ambientale si stia effettivamente ampliando, sebbene presenti ancora dei limiti: è necessario quindi uno sviluppo della visione ed un approfondimento su tematiche che ancora oggi non sono entrate attivamente nel campo di ricerca, salvo qualche cenno o case study, questo sia per permettere una comprensione maggiore del fenomeno sia per poterlo contrastare più attivamente e con mezzi più efficaci.

2. Ecomafie: sul concetto di "Mafie"

Abbiamo visto poc'anzi che la criminologia ambientale non prende minimamente in considerazione, all'interno delle sue definizioni, il fenomeno delle ecomafie e l'impatto che la criminalità organizzata di stampo mafioso, e non, può avere sull'ambiente.

Eppure, per quanto riguarda almeno il nostro Paese risulta una questione assai importante e purtroppo diffusa.

Per capire però effettivamente la problematicità e la pericolosità della questione, si partirà dall'origine della sua parola, passando dalle teorie sulla sua nascita per arrivare alla sua definizione da parte del codice penale che ne racchiude il cuore e soprattutto ne illustra il metodo.

Sarà inoltre importantissimo analizzare la possibilità di ampliare il concetto non solo di crimini ambientali, partendo ovviamente dal significato originale di ambiente, ma anche, di conseguenza, di ecomafia.

Per quanto concerne quindi il fenomeno della criminalità organizzata, appare evidente cercare di capire cosa voglia dire il termine "Mafia". La sua origine e significato appaiono tutt'oggi oscuri:

[7] Poichè il capitolo tratta delle tigri situate nella foresta delle Sundarbans, la più grande foresta di mangrovie del mondo, al confine tra Bangladesh ed India, si fa riferimento alla tigre del Bengala. Si tende a fare questa precisazione in quanto attualmente sono vive sei differenti specie di tigri.

[8] Le zoomafie verranno brevemente definite di seguito.

[9] A onor del vero, all'interno della letteratura citata si sono intravisti alcuni riferimenti alla criminalità organizzata, ma questi rappresentavano solo una minima parte dell'elaborato, non trattandola ed analizzandola a dovere.

l'origine parrebbe provenire dalla lingua araba, mentre il suo significato, se si consulta il Dizionario (o Vocabolario) Siciliano, del 1985, indicherebbe "Bellezza, baldanza" (Renda, 1998). Noi sappiamo perfettamente che le organizzazioni mafiose non hanno alcuna connotazione positiva, eppure questa credenza è stata a lungo diffusa. Talvolta le organizzazioni stesse sono state glorificate ed il loro peso sminuito, basti pensare ad esempio al mito sulla nascita di tre delle associazioni italiane più note (Cosa Nostra, 'Ndrangheta e Camorra) per mano di tre cavalieri spagnoli costretti a fuggire dalla Spagna dopo aver commesso un omicidio per ripristinare l'onore della sorella. Dall'altra parte, il fenomeno, soprattutto nei primi tempi, e talvolta tutt'oggi, è stato fortemente sminuito, minimizzato, talvolta anche negato[10].

Il perché poi queste associazioni siano nate, cresciute e abbiano piantato forti radici soprattutto al Meridione è stato oggetto di analisi da parte di vari studiosi. Alcuni hanno rintracciato la sua causa nel corredo genetico della popolazione del meridione: Alfredo Niceforo, tra l'altro siciliano, descrive il popolo della Trinacria come una "razza maledetta" e considera il Mezzogiorno un paese meno evoluto e civile, arrivando addirittura a definirla «(un') "Italia barbara contemporanea", con uno scarso sviluppo sociale, una struttura morale primitiva, tipica delle società inferiori [...], "l'Italia del sud rappresenta - di fronte all'Italia del Nord - un vero e proprio atavismo sociale"» (Sicurella, 2017, p. 22).

Altri, come ad esempio Banfield e Putnam, rintracciano questo consolidamento nel Sud Italia nel tipo di struttura sociale e culturale: il primo, infatti, conia l'espressione "familismo amorale", intesa come un'incapacità, da parte degli abitanti, di agire insieme, in maniera costruttiva, per il bene comune. Quindi ritiene la gente del Mezzogiorno non formata, non "acculturata" al bene comune ed alla condivisione, al supporto reciproco (Banflield, 2010).

Il secondo, invece, attraverso uno studio degli anni '90 al cui centro vi è il concetto di "cultura civica", mostra le due facce della Penisola: il Centro-Nord si caratterizza per la solidarietà e il rispetto delle leggi, mentre il Sud per la corruzione, l'individualismo, l'indifferenza (Putnam, 1996).

Altri ancora hanno evidenziato come la posizione geografica non abbia favorito uno scambio di idee e di valori: rispetto alle regioni del Nord, che si

[10]Questo atteggiamento fin dal passato è stato evidenziato anche da figure politiche di un certo livello, basti pensare a quanto l'ex Senatore Girolamo Li Causi, il 26 Ottobre 1951, ricordò durante la 704esima seduta del Senato, alcune parole riportate dall'allora Ministro dell'Interno Mario Scelba, in un differente momento, in merito alla Mafia: "Ma il ministro Scelba è venuto sorridendo a dirci che la mafia non esiste, e che nel linguaggio dei siciliani si usa il diminutivo « mafiosetta » per indicare una ragazza precoce e un po' altera."
(URL: https://www.senato.it/service/PDF/PDFServer/BGT/487606.pdf , p. 9)
In tempi più recenti un'altra figura politica si è espressa in merito, l'ex senatore Marcello Dell'Utri, che aveva dichiarato in un'intervista tenuta da Chiambretti "Non esiste la mafia. […] No, non esiste la mafia. La mafia è un modo d'essere, di pensare. […]" (URL: https://web.archive.org/web/20151102035644/http://archiviostorico.corriere.it/1997/ottobre/02/Dell_Utri_Chiambretti_mafia_modo_co_0_9710022934.shtml e https://www.youtube.com/watch?v=WQ2NdOMBss0&ab_channel=MrAlfonsino (Min 1.01-1.02).)
Allo stesso modo la Relazione al Parlamento della Direzione Investigativa Antimafia del Secondo Semestre del 2019 evidenzia e sottolinea come il fenomeno sia tutt'oggi sottovalutato e sminuito.
(URL: https://direzioneinvestigativaantimafia.interno.gov.it/semestrali/sem/2019/2sem2019.pdf)
All'interno della Relazione, si riportano anche le parole del Procuratore Generale della Repubblica di Torino, Dott. Francesco Saluzzo, durante l'inaugurazione dell'anno giudiziario del 26 gennaio 2019: "[...] quel che mi preoccupa è la persistente sottovalutazione del fenomeno che si coglie nell'opinione pubblica… Questo atteggiamento ha aiutato ed aiuta le organizzazioni mafiose. Non basta la risposta giudiziaria…, occorre una presa di coscienza ed un atteggiamento di ripulsa e di rigetto delle persone, delle comunità e delle istituzioni…"
(URL: https://direzioneinvestigativaantimafia.interno.gov.it/semestrali/sem/2019/2sem2019.pdf , p. 32)]

trovano a confinare direttamente con altri Paesi e culture, il Meridione è circondato dal mare e quindi maggiormente isolato (E. Felice, 2016; S. Sicurella, 2017).

Ciò che però caratterizza veramente il fenomeno mafioso è il suo metodo, metodo che è stato descritto in maniera estremamente esaustiva all'interno dell'articolo 416*bis* del Codice Penale, introdotto con la Legge Rognoni-La Torre del 1982. Si legge infatti al comma 3:

«L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono 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» (Brocardi.it).

Il nucleo stesso delle organizzazioni, quindi, risiede nella forza, nell'intimidazione, nell'omertà, nell'assoggettamento, in quell'unione, in quel legame che va a instaurarsi tra l'organizzazione stessa ed il neofita; ma si vede anche la violenza sottile perpetrata nei confronti della popolazione, attraverso minacce, intimidazioni e quel silenzio a cui sono costretti i cittadini per paura di possibili ritorsioni nei loro confronti e dei loro cari.

2.1 Ecomafie: cosa sono e come potrebbero essere

Tra i tanti e variegati settori di interesse delle associazioni mafiose vi è ovviamente anche l'ambiente e questo è stato evidenziato per la prima volta da Legambiente nel 1997, attraverso la pubblicazione del primo Rapporto Ecomafie.

Anche in questo caso, però, innanzitutto indicheremo quale sia il nostro obiettivo, e lo faremo sempre attraverso un'analisi etimologica, in questo caso del termine ecomafia.

La parola in questione è un neologismo, composto da due parole differenti che esistono autonomamente all'interno della lingua italiana, di cui, la prima, *eco*, è di derivazione greca.

Il prefisso eco, infatti, trova la sua origine nella parola greca *òikos*, col significato primario di casa, ambiente in cui si vive. Anche in questo caso, quindi, non si dovrebbe limitare il suo campo di riferimento solo a ciò che è naturale, ma lo si dovrebbe estendere, ampliare, dovrebbe essere in grado di includere l'ambiente in cui si vive, ovvero tutto ciò che ci circonda.

In merito a questo, si deve riconoscere che Legambiente, all'interno dei suoi rapporti, ha trattato e analizzato vari aspetti del fenomeno, permettendo quindi un incremento dei soggetti ambientali, ma li riteniamo comunque non sufficienti.

All'interno dei suoi rapporti, l'associazione si focalizza su sei settori d'interesse: il traffico illecito di rifiuti, il ciclo del cemento, il traffico di animali e specie protette (le c.d. zoomafie), il traffico illecito di beni artistici e culturali (le c.d. archeomafie), il settore agroalimentare (le c.d. agromafie) e gli incendi boschivi.

Tra questi, quello che più risulta essere florido e soprattutto sotto l'attenzione dei media e degli organi di polizia giudiziaria, è il settore del traffico illecito di rifiuti. Questo verrà analizzato prendendo in considerazione due sue sottocategorie, il traffico di rifiuti su terra e quello che coinvolge il mare, attraverso il caso delle navi dei veleni e soprattutto

delle navi a perdere; ci si soffermerà sulla loro storia e sulla loro situazione attuale, anche grazie ad interviste di operatori che lavorano sul campo[11].

Il fenomeno del traffico illecito di rifiuti ebbe inizio intorno agli anni '80, quando alcuni clan della Camorra si resero conto di poter guadagnare dai rifiuti, attraverso la falsificazioni di documenti, anche di controllo (Cianciullo, Fontana, 2012): fu così che si organizzarono ed incominciarono ad importare dal Nord Italia rifiuti, anche pericolosi, da smaltire illegalmente nel Sud del Paese, attraverso procedimenti come il ritombamento, il riversamento in discariche abusive o gli incendi[12].

La questione inizierà a venire a galla solo negli anni '90, quando un autotrasportatore venne ricoverato in ospedale in quanto contaminato da alcune sostanze nocive fuoriuscite dal suo container, che stava andando a smaltire in una discarica abusiva tra i comuni di Qualiano e Villaricca[13]. Questo evento fa attivare la Procura della Repubblica di Napoli, attraverso l'Operazione Adelphi, che riuscirà a portare finalmente alla luce ciò che stava accadendo nella "Terra dei Fuochi".

Allo stato attuale verrebbe da pensare che una volta avviato questo processo nelle zone del Meridione tutt'oggi sia lì che vi sia il maggior numero di casi di traffici illeciti, ma non è così. Se si ascoltano le parole del Comandante 1, si noterà come la situazione si stia invertendo:

> [...] *(il Nord) è la parte più industriale di questo Paese, quindi per una mera questione statistica, ovviamente è più probabile che un impatto sull'ambiente avvenga nel Nord Italia, (inoltre) è la parte d'Italia che produce più rifiuti e quindi è quella che ha più criticità; è quella anche che attira più rifiuti perché è quella che ha più impianti di trattamento rifiuti e di termovalorizzazione (sono quelli che attirano i rifiuti), la sola Lombardia ha 12 impianti su 38 che sono in tutta Italia attivi sul momento, e quindi diciamo che, statisticamente, una buona fetta interessi il Nord Italia: non significa che il Nord Italia sia la parte più colpita da determinati interessi criminali, è una pura questione statistica, molto spesso; di contro bisogna dire che in molte delle nostre attività scopriamo che i rifiuti che vengono gestiti illecitamente al Nord, provengono dal Centro-Sud, perché non ha impianti.* [...] (Comandante 1, uomo, 22 Febbraio, 2021; videochiamata, Milano)

Il Comandante illustra anche il caso degli incendi che si sono verificati in Veneto e per cui i media avevano iniziato a dare titoli allarmistici, vaneggiando sul fatto che la regione stesse diventando la nuova Terra dei Fuochi. Ha smentito subito la faccenda, sottolineando come il modus operandi non corrispondesse a quello di solito impiegato e riportando anche come, attraverso un metodo investigativo diverso, siano riusciti ad individuare in quegli incendi l'anello finale del processo di traffico illecito di rifiuti, permettendo così, nel solo periodo 2019-2020, di superare i 60 arresti. Attualmente, anche il fenomeno degli

[11]Gli intervistati che contribuiranno alla stesura dell'articolo sono tre figure, due appartenenti all'Arma dei Carabinieri, di cui una ha rivestito anche un ruolo politico, e la terza invece presta servizio presso la capitaneria di Porto in Calabria. I due carabinieri hanno titoli ed operano in gruppi differenti, ci rivolgeremo a loro come Comandante 1 e Generale 1. Il membro della Capitaneria di Porto verrà denominato Comandante 2.

[12]Per maggiori dettagli, si rimanda a: Commissione parlamentare di inchiesta sulle attività illecite connesse al ciclo dei rifiuti (istituita con legge 6 febbraio 2009, n. 6), Relazione territoriale sulle attività illecite connesse al ciclo dei rifiuti nella regione campania, Approvata dalla Commissione nella seduta del 5 febbraio 2013. URL: https://www.senato.it/service/PDF/PDFServer/BGT/698083.pdf

[13]Si veda la Relazione al Parlamento della Direzione Investigativa Antimafia del Primo Semestre del 2019 (URL: https://direzioneinvestigativaantimafia.interno.gov.it/semestrali/sem/2019/1sem2019.pdf , p. 595)

incendi sta andando a scemare, mentre si predilige la rotta estera[14].

I fenomeni invece che caratterizzano il mare sono due: le navi dei veleni e le navi a perdere.

Le navi dei veleni si caratterizzano per essere navi che vengono caricate di rifiuti e poi spedite in altri Paesi per scaricarli lì, in modo da essere "smaltiti".

Le navi a perdere invece sono navi che vengono sempre caricate di rifiuti, ma che, una volta giunte ad una certa distanza dalla costa, vengono fatte affondare volutamente[15].

Entrambe le tipologie di navi sono state per tempo sotto l'attenzione dei media, dell'opinione pubblica e degli investigatori, si ricorda infatti che il Comandante De Grazia stava lavorando ad un caso riguardante una di queste navi, la Rigel,[16] così come anche tra le navi dei veleni spicca la Jolly Rosso, poi denominata solo Rosso (Bocca, 2008). Per tutti questi casi non si arriverà mai ad una condanna, vuoi per archiviazione del caso, vuoi per un arresto delle indagini. Ma non solo. Per quanto riguarda le navi a perdere, come spiega il Comandante 2, investigare su questo tipo di reato è assai difficile:

> *Nei fondali dove magari ci sono (le navi), siamo in acque internazionali, dopo le 12 miglia nautiche (1852 metri x 12, quindi 22,224 m dalla linea delle acque interne, non dalla costa); dopo la convenzione di Montego Bay, sono state stabilite le fasce di mare e dopo le 12 miglia sono acque internazionali, quindi, non abbiamo proprio il diritto e l'autorità per andare a vedere. Se però ha bandiera italiana, allora si può andare a controllare ma si agisce Solo come Stato di bandiera della nave.*
>
> (Comandante 2, uomo, 28 Settembre, 2021, Reggio Calabria)

Vi sarebbe quindi un'oggettiva impossibilità fisica nell'investigare su questi reati.

In tempi più recenti invece, le cose sono cambiate. Come riporta sempre il Comandante 2, ci sono dei sistemi e delle procedure che permettono di controllare le navi in transito e non solo:

> *Sfatiamo subito un mito: se ci sono navi che si affondano, risalgono agli anni '90, oggi è molto difficile per vari motivi: oggi le navi hanno dei sistemi di tracciamento, quindi sappiamo "vita, morte e miracoli", perciò quando una nave parte e poi transita, noi lo sappiamo. Ora c'è un sistema all'interno delle navi denominato A.I.S (Automatic Identification System, in italiano Sistema di Identificazione Automatico) che ci permette di sapere da dove parte, cosa porta, dove va, tutto. È un sistema che permette di localizzare la nave: questa in pratica emette un segnale che viene captato da una serie di antenne che sono sul territorio. Le navi che fanno cargo lo sono Tutte, anche quelle che sono di lunghezza uguale o superiore ai 15 m. Rispetto agli anni 80-90 oggi il traffico navale è tutto controllato. La Guardia Costiera ha un sistema più sofisticato che è il sistema Pelagus, un software che permette di raccogliere, elaborare, memorizzare, mostrare e distribuire i dati originati da molteplici sorgenti e sensori relativi alle tracce delle imbarcazioni e, più in generale, ai dati marittimi; traccia la rotta, mi tiene l'archivio, quindi si può sapere dove è andata l'imbarcazione[...].*

[14]Comandante 1, uomo, 22 Febbraio, 2021; videochiamata, Milano. Con rotta estera, il Comandante fa riferimento al fatto che i rifiuti ora piuttosto che smaltirli illegalmente in Italia, si preferisce spedirli all'estero per essere smaltiti, ovviamente sempre illecitamente.

[15]Per approfondimenti si veda: https://navideiveleni.legambiente.it/navi-a-perdere/storia.php

[16]Per approfondimenti si veda: Anna Foti, 2021, Rigel, la nave scomparsa con il suo carico e i suoi segreti il 21 settembre 1987, Lacnews24.it, 21 settembre; URL: https://www.lacnews24.it/cultura/rigel-la-nave-scomparsa-con-il-suo-carico-e-i-suoi-segreti-il-21-settembre-1987-_143068/

(Comandante 2, uomo, 28 Settembre, 2021, Reggio Calabria)

Vi è quindi un monitoraggio ed un controllo costante delle navi, di cui si sa adesso il contenuto, la rotta, il punto di partenza e di arrivo, tutto. Qualora ci fossero delle anomalie nel traffico navale, la Guardia Costiera lo saprebbe e potrebbe subito mobilitarsi.

Si è vista quindi la situazione più o meno attuale delle ecomafie e due dei fenomeni più noti, eppure c'è modo di andare oltre a questo aspetto, e lo si può fare se si prende in analisi un documento proveniente dalla Commissione Parlamentare di Inchiesta sui fenomeni della contraffazione, della pirateria in campo commerciale e del commercio abusivo, in particolar modo il Resoconto Stenografico Audizione 78. della seduta di Martedì 6 Giugno 2017 dell'allora Ministro della Giustizia Andrea Orlando[17].

All'interno del documento, che dalla provenienza sembrerebbe più richiamare il Ministero dell'Economia che non quello dell'Ambiente, emergono informazioni molto importanti, sia per quanto concerne l'aspetto prettamente economico, soffermandosi soprattutto sulle perdite del Paese legate alla produzione di oggetti contraffatti, sia su quali potrebbero essere questi oggetti che vengono prodotti con materiali scadenti, tra cui vi sono: «capi di maglieria realizzati con pelo di coniglio anziché confezionati con il pregiato kashmir dichiarato dalle etichette, cosmetici e profumi contraffatti con alte percentuali di toluene e di benzene, termocaloriferi assemblati con fibre di amianto, rubinetti che rilasciano metalli pesanti come il piombo, giocattoli contraffatti contenenti ftalati, gioielli contraffatti con alta concentrazione di nichel, scarpe e pelletteria con anomali livelli di cromo esavalente, sigarette contraffatte con valore di catrame, piombo e arsenico centinaia di volte superiori alla norma.» (Commissione parlamentare, 2017, p. 5).

Come si legge sempre all'interno del documento, «[...] sembra inoltre emergere nel settore un fitto intreccio di interessi di Cosa Nostra, dei clan camorristici e delle 'ndrine calabresi [...]» (Commissione parlamentare, 2017, p. 7) questo a dimostrazione che le mafie agiscono e si interessano anche a quei settori ambientali, in senso latino, ma che non vengono considerati tali.

Questo documento rappresenta un primo passo, un primo tassello per dimostrare come le mafie e la criminalità ambientale tutta non vadano viste solo in relazione agli aspetti prettamente naturalistici, ma anche, e forse soprattutto, a quegli elementi che ci circondano e con cui interagiamo tutti i giorni senza avere il minimo sospetto. Questo documento servirebbe a dimostrare come anche i crimini che sono disciplinati all'interno di un altro codice o di un'altra area tematica possano essere ritenuti crimini ambientali, in quanto oggetti e prodotti alterati possono poi entrare in contatto con le persone nell'ambiente che li circonda e con cui interagiscono.

3. Diritto ambientale: un mondo estremamente vasto

Tentare di riassumere in poche pagine il diritto ambientale è un'impresa impossibile.

Ciò che però si può fare è dare un'idea del diritto che riguarda la tutela dell'ambiente, sia dal punto di vista nazionale che internazionale, e soprattutto, evidenziare quelle organizzazioni, nostrane e non,

[17]Per approfondimenti si veda: Commissione parlamentare di inchiesta sui fenomeni della contraffazione, della pirateria in campo commerciale e del commercio abusivo, resoconto stenografico audizione 78. seduta di martedì 6 giugno 2017; url: https://documenti.camera.it/leg17/resoconti/commissioni/stenografici/pdf/64/audiz2/audizione/2017/06/06/leg.17.stencomm.data20170606.U1.com64.audiz2.audizione.0078.pdf

che si occupano di combattere i crimini ambientali sul campo.

Il punto di partenza però deve vedersi nella ricerca del significato di "bene giuridico ambiente". Ebbene, una materia acquisisce rilevanza e può essere definita un bene giuridico quando la cultura, la classe politica, soprattutto questa, e la mentalità della popolazione sono pronte a considerarla tale. E se si guarda in tempi recenti non si può assolutamente negare il fatto che questi temi non abbiano una rilevanza culturale, politica, sociale ed anche normativa, anzi.

Se si fa riferimento più specificatamente alla situazione italiana, si può notare come l'ambiente abbia comunque avuto un suo peso all'interno delle istituzioni: con la Legge 349 dell'8 Agosto 1986 venne istituito ufficialmente il Ministero dell'Ambiente, Ministero attualmente con portafoglio, quindi detentore di fondi con cui attuare e portare avanti riforme concrete; nella stessa legge, all'articolo 8, comma 4, venne dichiarata anche l'istituzione di un organo di prevenzione e repressione delle violazioni in materia di ambiente, ovvero il Nucleo Operativo Ecologico presso l'Arma dei Carabinieri[18]. In seguito nel 1994, con la Legge 61 del 21 Gennaio, il Parlamento istituì delle Agenzie a livello Regionale che si occupassero della questione ambientale, sotto vari e moltissimi aspetti, a livello territoriale, soffermandosi soprattutto sull'aspetto scientifico e di analisi, le ARPA (Agenzia Regionale per la Protezione Ambientale), così come anche nel 2008, venne istituito un altro organo, ovvero l'ISPRA, l'Istituto Superiore per la Protezione e la Ricerca Ambientale.

In Italia quindi un primo riconoscimento del valore e del bene ambiente sembra esservi sempre stato, ma ad esempio se si guarda il trattamento dell'ambiente all'interno della Costituzione, si noterà di come questo sia passato a lungo in secondo piano.

Nella prima versione del '48 della Carta Costituente era presente, infatti, un riferimento alla "tutela del paesaggio" all'art. 9, com. 2, ma tale definizione tocca solo in senso lato la tematica ambientale, in quanto il paesaggio viene tutelato, come riporta lo stesso comma, con il patrimonio storico e artistico della Nazione.

Alcuni interpreti hanno cercato di farlo rientrare in senso molto lato, ma è lampante il fatto che ambiente e paesaggio, soprattutto se ci si attiene al significato etimologico della prima parola, siano due cose differenti, con dei punti in comune, ma pur sempre diverse.

Un piccolo passo in avanti fu fatto nel 2001, con la riforma del Titolo V, in cui all'articolo 117, com. 2, lettera s), si riporta infatti che, «[…] Lo Stato ha legislazione esclusiva nelle seguenti materie: […] s) tutela dell'ambiente, dell'ecosistema e dei beni culturali. [...]» (Costituzione della Repubblica italiana, articolo 117), quindi vi è una prima introduzione della questione, ma riguarda la suddivisione delle competenze tra Stato e Regioni.

Nel 2019, l'allora Ministro dell'Ambiente Costa aveva annunciato l'arrivo di un Disegno di Legge che aveva l'intenzione di attuare questo piccolo ma necessario passo, e finalmente, l'8 Febbraio 2022, con la maggioranza dei due terzi dei voti dei suoi componenti, la proposta è stata ufficialmente approvata, in via definitiva, modificando così l'articolo 9 e 41 della Carta Costituzionale[19].

[18] Per approfondimenti si veda: https://www.gazzettaufficiale.it/eli/gu/1986/07/15/162/so/59/sg/pdf

[19] Per maggiori approfondimenti in merito alla riforma costituzionale in materia di tutela dell'ambiente, 2021, si veda: Dipartimento per le riforme istituzionali- Presidenza del Consiglio dei Ministri. URL: https://www.riformeistituzionali.gov.it/it/la-legge-costituzionale-in-materia-di-tutela-dell-ambiente/

A livello internazionale, la questione ambientale è sentita ancora di più: l'Europa rappresenta infatti il principale "produttore" di norme ambientali, la maggioranza del nostro ordinamento in materia proviene infatti da Direttive dell'Unione; a livello extraeuropeo, poi, i trattati internazionali, i meeting e le conferenze sulle questioni ambientali sono moltissimi, con l'unico problema che la maggioranza, fatta eccezione per il protocollo di Kyōto che proponeva delle scadenze e dei limiti, non sono vincolanti, ovvero non impegnano veramente gli Stati partecipanti, rendendo quindi queste attività spesso più di facciata che non utili ed efficaci.

Da queste vicende internazionali, tuttavia, soprattutto a livello europeo e di conseguenza poi a livello nazionale, degli aspetti positivi sono giunti lo stesso: per contrastare questo particolare tipo di fenomeno sono stati creati degli organi di polizia specializzati nel loro contrasto e l'Europa ha richiesto agli Stati Membri una normativa penale ambientale.

Il primo aspetto si sviluppa sia a livello Internazionale che nazionale.

Cronologicamente, il primo organo di sicurezza che si è occupato anche di crimini ambientali è stato l'Interpol: all'interno dell'agenzia ciò che risulta particolarmente importante, è la presenza di alcuni progetti che vedono l'Italia coinvolta in primo piano.

Il primo progetto è il *Pollution Crime Working Group (PCWG)*, un gruppo di lavoro in cui esperti delle diverse nazioni si incontrano annualmente per discutere le strategie operative e condividere le competenze; il gruppo attualmente sta supportando il programma sulla sicurezza ambientale dell'Interpol per contribuire nella creazione di una risposta coordinata a livello mondiale verso i crimini di inquinamento[20].

Il secondo progetto, anche se in questo caso sarebbe meglio definirlo programma, vede l'Italia assai più coinvolta rispetto al primo, in quanto è stato studiato e progettato appositamente per il contrasto alla 'Ndrangheta, l'INTERPOL Cooperation Against 'Ndrangheta (I-CAN), che si basa, come il primo, sulla collaborazione tra i diversi Stati per il contrasto a questo fenomeno[21]. Ciò che quindi dà speranza è sapere che ad un livello così alto dal punto di vista della sicurezza, ci sia un riconoscimento del fenomeno e l'intenzione da parte di più Stati di collaborare attivamente per il suo contrasto: è questo tipo di riconoscimento che fa comprendere quanto la presenza delle mafie a livello internazionale sia un problema di tutti, non limitandosi quindi alla sola e semplice popolazione italiana e che quindi sia necessario un suo studio ed inserimento nell'ambito della criminologia ambientale.

La seconda organizzazione a nascere è stata Eurojust[22] e anch'essa si occupa di aiutare «le amministrazioni nazionali a collaborare per combattere il terrorismo e gravi forme di criminalità organizzata che interessano più di un paese dell'UE.» (Unione Europea-Eurojust).

Ciò che maggiormente ci interessa, per quanto concerne questa organizzazione, è la Relazione sul progetto strategico in materia di criminalità

[20] Per approfondimenti si rimanda a: Pollution crime, Interpol. URL: https://www.interpol.int/Crimes/Environmental-crime/Pollution-crime

[21] Per ulteriori approfondimenti si veda: Interpol Cooperation Against 'Ndrangheta (I-CAN), Interpol. URL: https://www.interpol.int/Crimes/Organized-crime/INTERPOL-Cooperation-Against-Ndrangheta-I-CAN

[22] Per approfondimenti relativi all'Agenzia dell'Unione europea per la cooperazione giudiziaria penale, fondata nel 2002, si veda: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eurojust_it

ambientale, del Novembre 2014, citata nel Report Annuale di Eurojust, in cui il piccolo sotto-paragrafo 2.2.2 è dedicato proprio ai crimini ambientali. La relazione di Eurojust riporta che «[...] Essa pone in evidenza i principali problemi riscontrati dalle autorità nazionali nel perseguimento della criminalità ambientale e tenta di presentare suggerimenti volti al superamento di alcune di tali difficoltà, in particolar modo quelle collegate alla cooperazione transfrontaliera, con una particolare attenzione al traffico illecito di rifiuti [...].» (Eurojust, 2014, p. 38).

Ancora una volta quindi il tema ambientale è forte e presente sul piano internazionale.

Stessa cosa accade poi con Europol, attraverso il programma Empact, che, come riporta sempre il Comandante 1:

> *Esistono diversi progetti di collaborazione, uno di questi è la piattaforma Empact (l'Empact è molto effettiva perché sono azioni finanziate), è una piattaforma multidisciplinare, sostanzialmente nell'ambito dei suoi Policy Cycle quadriennali, l'Europa stabilisce attraverso la variazione dei SOCTA (i serious crime, sostanzialmente) quali sono le priorità; nell'ultimo quadriennio, 2017/2021 sono rientrati i crimini ambientali. Cosa significa questo? Che attraverso questa piattaforma sono state create delle azioni operative che coinvolgono diversi Stati, finalizzati al contrasto di questi reati ambientali. [...]*
>
> (Comandante 1, uomo, 22 Febbraio, 2021; videochiamata, Milano)

Per quanto concerne invece la situazione prettamente Italiana, avevamo accennato precedentemente ai NOE, i Nuclei Operativi che si occupano sul territorio nazionale del contrasto mirato a questi particolari tipi di reati.

Per quanto concerne invece la questione marittima, l'Italia può riporre la propria fiducia nel Corpo delle Capitanerie di Porto - Guardia Costiera.

3.1 Diritto penale ed ambiente: piccoli passi avanti, ma ancora troppe mancanze

Dal punto di vista dell'ordinamento penale, l'Europa aveva emesso la Direttiva 99/2008[23] che prevedeva e istituiva misure per una tutela ambientale più stringente in campo penale, in un primo momento il recepimento dell'Italia provocò non poche proteste e malcontenti, poiché la Direttiva indicava e fissava obiettivi che il Decreto Legislativo 121/2011 del 7 Luglio non rispettava affatto. Con quel Decreto Legislativo furono introdotte solo due particolari fattispecie di reato all'interno del Codice Penale, l'articolo 727-bis e 733-bis, rispettivamente, Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette e Distruzione o deterioramento di habitat all'interno di un sito protetto, quando il documento europeo proponeva molti più temi e con una rilevanza, ci verrebbe da dire, maggiore[24] (Gentile, 2017).

Fortunatamente nel 2015, con la Legge 68 ci fu un primo giro di boa: la Legge infatti prevedeva l'introduzione all'interno del Codice Penale di un titolo dedicato, il VI-*bis*, e degli articoli che

[23] Questa arrivò dopo due documenti precedenti: la Convenzione di Basilea, del 1989 e la Decisione quadro 80/2003/GAI che furono di grande ispirazione e stimolo per la stesura della Direttiva.

[24] La Direttiva infatti stabiliva alcune delle attività illecite da normare, tra cui vi erano: scarico, emissione o altro tipo di rilascio di materiali pericolosi nell'aria, nel terreno o nell'acqua; raccolta, trasporto, recupero o smaltimento di rifiuti pericolosi; spedizione di quantità rilevanti di rifiuti;gestione di impianti industriali che svolgono attività pericolose o che tengono in deposito sostanze pericolose (ad esempio fabbriche che producono vernici o sostanze chimiche); produzione, trattamento, immagazzinamento, accumulo, utilizzo, trasporto, importazione, esportazione o smaltimento di materiale nucleare e materiale radioattivo pericoloso; [...] URL: https://eur-lex.europa.eu/legal-content/IT/LSU/?uri=celex:32008L0099 .

disciplinassero proprio quei particolari tipi di reato legati all'ambiente, dal 452*bis* al 452*quaterdecies*. Tra questi articoli sono più presenti i riferimenti dati dalla Direttiva, infatti si trovano gli articoli 452*bis*, Inquinamento ambientale, 452*ter*, Morte o lesioni come conseguenza del delitto di inquinamento ambientale, 452*quater*, Disastro ambientale, 452*sexies*, Traffico e abbandono di materiale ad alta radioattività, 452*quaterdecies*, Attività organizzate per il traffico illecito di rifiuti.

Questo parrebbe quindi aver risolto tutti i problemi legati ai crimini ambientali, eppure, all'interno dell'articolato ci sono dei punti non chiari o comunque lacunosi.

Uno tra tutti, che si ritiene essere il più importante, è la dicitura, presente all'interno dell'articolo 452-quaterdecies, inerente agli "ingenti quantitativi"[25].

A quanto corrispondono "ingenti quantitativi"?

Il Comandante 1 si è espresso in merito alla questione:

> *[...]Perché nella pratica avviene che io, che individuo la società X, che sta trasportando, movimentando, gestendo illecitamente rifiuti, devo attendere e documentare carichi, su carichi, su carichi, perché se mi fermo dopo il primo carico, non gli posso dare il delitto più grave, il 452-quaterdecies. Anche se ho già tutti gli elementi per dire che è una struttura organizzata. E peggio ancora se ho una struttura mafiosa. Devo aspettare gli ingenti quantitativi. Io dovrei poter intervenire al primo carico in flagranza e contestargli tutto, ma la previsione degli ingenti quantitativi è anacronistica, anche perché, "ingenti" rispetto a cosa? È la struttura che deve contare, per dimostrare il 416-bis, [...] basta l'associazione; [...] nessuno mi chiede che devono poi aver fatto lo spaccio di almeno una tonnellata di sostanze stupefacenti. Ci deve essere un reato fine, punto. […] È come se io individuassi un rapinatore ma se non gli faccio fare almeno 20 rapine non lo posso arrestare. Nella realtà se lo scopro e ce l'ho lì lo prendo, non gli farò mai commettere neanche una rapina.*
>
> (Comandante 1, uomo, 22 Febbraio, 2021; videochiamata, Milano)

Non si può che essere d'accordo con quanto riportato dal Comandante 1, ma in merito alla questione si tiene anche a citare un ulteriore contributo, quello del Generale 1, il quale ha ricoperto anche un incarico ministeriale, e che ci ha concesso un'intervista il 22 Febbraio 2022.

Il Generale riporta infatti:

> *Ti racconto in termini investigativi: il concetto di ingente ci ha interpellato molto come investigatori e ci siamo posti le tue stesse domande, ma abbiamo risposto in questi termini: il concetto di ingente non è un concetto metrico, è un kilo? Una tonnellata? Dipende dalla tipologia di rifiuto, un metro cubo di amianto non è un metro cubo di RSU (rifiuti solidi urbani), quindi non è mai una tabella o una multi tabella, come molti chiedevano, perché sembra più una ricetta; inoltre è un concetto di natura territoriale, cioè ingenti in Valle d'Aosta è diverso da ingenti nella Terra dei Fuochi, ma non perché le persone sono diverse in quanto esposte alle ingiurie ambientali, ma perché esiste una densità di persone per chilometro quadrato diversa. Ingenti è anche rapportato a questi parametri sociali, ma anche alla tipologia di organizzazione, cioè per quella tipologia di organizzazione, ingenti vuol dire che quella organizzazione ha fatto molto con l'organizzazione che aveva, se poi quell'organizzazione è micro e ha*

[25] "Chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti è punito con la reclusione da uno a sei anni. [...]" URL: https://www.brocardi.it/codice-penale/libro-secondo/titolo-vi-bis/art452quaterdecies.html

fatto molto col micro, ha fatto ingenti; se ha fatto poco con una grande organizzazione criminale, non ha fatto ingenti; deve essere proporzionato. [...]

(Generale 1, uomo, 22 febbraio, 2022; videochiamata, Roma-Napoli)

Entrambi i contributi offrono validi spunti di riflessione: come affermato dal Generale 1, è vero che la pericolosità di un rifiuto varia in base al suo tipo, quindi è giusto non avere come riferimento una tabella fissa; altrettanto vero, però, come asserito dal Comandante 1, se si trova subito un'organizzazione che traffica rifiuti, non importa quanto sia grande o piccola o quanti rifiuti abbia effettivamente trasportato, va fermata subito, che sia in Valle d'Aosta o nel Lazio.

Oltre alla questione degli ingenti quantitativi, si era cercato anche di andare a modificare la Legge 68 attraverso una proposta di Legge del Generale 1, col Disegno di Legge Terra Mia.

Gli si è chiesto in seguito come fosse nata l'idea del DdL e perchè: *[...] io in tanti anni di investigazione, che ho speso quasi tutti per il contrasto ai crimini ambientali, ho visto da una parte l'evoluzione della normativa ambientale, che ha subìto un'accelerazione abbastanza recentemente, ma ho visto anche quali sono i limiti delle norme ambientali, che, secondo me, pur avendo fatto grossi progressi, non hanno colto un'esigenza, e qui rispondo alla tua domanda: quello che io notavo, facendo le indagini, è che la situazione che vedevo tra i cosiddetti ecocriminali mafiosi, cioè che hanno una matrice criminale organizzata, quindi quelli più "pericolosi", venivano posti sostanzialmente per la tipologia del reato ambientale, sullo stesso piano orizzontale del criminale o del delinquente ambientale di profilo e di spessore minore. [...] Quindi [...] distinguiamo, attraverso Terra Mia, il delinquente ambientale dall'ecocriminale organizzato, cioè, la criminalità organizzata deve avere una punibilità e dei termini di aggressività dello Stato, cioè di indagini e di capacità investigative dello Stato, che non devono essere spese inutilmente anche per il "delinquentuccio" ambientale. Per essere chiari: se io organizzo tutto un sistema di traffico illecito organizzato dei rifiuti, perché sono un "criminale incallito", ho bisogno che lo Stato utilizzi degli strumenti di investigazione e di punibilità diversi da quelli che prendono la spazzatura e la buttano fuori dalla finestra.*[26]

(Generale 1, uomo, 22 febbraio, 2022; videochiamata, Roma-Napoli)

Il Generale pone quindi uno spartiacque sul trattamento per quanto riguarda le indagini in campo ambientale. Proseguendo nell'intervista, gli è stato anche chiesto quali fossero le misure da lui proposte per contrastare con più forza gli ecocriminali:

[...] per i casi "gravi", cioè di criminalità organizzata, ho previsto degli strumenti normativi molto aggressivi, che sostanzialmente sono, 1) (forse il più aggressivo di tutti) ho pensato di allargare le maglie della normativa antimafia e portarla anche nel campo della normativa ambientale, affermando il principio che aggredire il territorio dove X vive vuol dire esercitare nei suoi confronti una violenza diretta talmente grave, perché incide sul suo bene principale, che è la qualità della vita, lo stato di salute della vita propria e dei suoi familiari. 2) Devo aggredire il tuo patrimonio, così come nella normativa antimafia, Integralmente, anche quello che tu hai distribuito tra soggetti prestanome, perché tu devi rispondere con tutto il tuo patrimonio in generale del danno cagionato al bene collettivo, perché è un'espressione di tutela della vita. 3) Vi è

[26] Quest'ultima affermazione del Generale fa riferimento ad una scena del film "Benvenuti al Sud".

poi il Daspo ambientale (come quello degli stadi), ha un senso molto politico, dal punto di vista strettamente tecnico è a cabotaggio molto limitato, ma ha un senso: riprende il daspo sportivo, non ti faccio entrare allo stadio, quindi se il soggetto X ha commesso violenza al territorio, implicita agli abitanti, è politicamente non degno di vivere su quel territorio, tecnicamente io lo escludo da esercitare la sua attività, qualunque essa sia, su quel territorio o sul territorio di sua residenza, perché chi commette questi reati, mediamente è un abitante di quel territorio, ed è la statistica che ce lo dice. È proprio in spregio al suo territorio.

(Generale 1, uomo, 22 febbraio, 2022; videochiamata, Roma-Napoli)

Proposte, quelle del Generale, che avrebbero potuto portare ad un cambiamento o comunque ad un suo inizio. Il Disegno di Legge alla fine non ha mai visto la luce per questioni politiche.

Pertanto, parrebbe che per quanto riguarda la questione prettamente normativa, non vi siano riferimenti o punti di appiglio che rafforzino la nostra tesi sul fatto che la tematica ambientale vada ampliata, ma questo può essere facilmente spiegato: come visto in precedenza, se si ampliasse come lo si intende noi, si andrebbero a toccare situazioni che sono attualmente normate da altre leggi, da altri codici. Non è che quindi non vi siano nell'effettivo norme che potrebbero essere adatte alle situazioni riportate poc'anzi, semplicemente si trovano in altri codici e leggi. Risulta inoltre necessario far notare una cosa: la normativa ambientale ed il rispettivo codice risultano già straordinariamente corposi, modificare un intero ordinamento normativo aggiungendo e/o spostando l'articolato risulterebbe solo dannoso e creerebbe confusione. Ciò che però è importante è riuscire a capire di come sia significativo ampliare lo sguardo e la propria interpretazione dei fenomeni.

4. Vittime di crimini ambientali: un riconoscimento ed un'inclusione necessari

La criminologia avrebbe dovuto viaggiare quasi di pari passo con la Vittimologia, ma questa ha visto la sua nascita negli anni del secondo dopoguerra, i cui "padri fondatori" si possono individuare in Hans Von Hentig, criminologo di formazione, e nell'avvocato Benjamin Mendelsohn: il primo è stato infatti l'autore nel 1948 del libro *The Criminal and his Victim*, in cui dedica il quarto ed ultimo capitolo al ruolo della vittima nella genesi del crimine, ovvero *The contribution of the victim to the genesis of crime*, ponendo quindi l'attenzione non più solo sul reo ma anche sulla vittima, seppur come elemento contribuente alla genesi e al verificarsi dell'azione criminale; il secondo, invece, svolgeva il ruolo di difensore di imputati di crimini sessuali, (Vezzadini, 2012) e fu proprio durante questo suo operato che riscontrò come la condizione di vittima sia dettata dalla società: è infatti questa che genera le vittime, in base ad esempio alle disuguaglianze e alle condizioni economiche che vi sono al suo interno[27].

In campo ambientale, la questione delle vittime risulta ancora assai delicata, poiché difficilmente queste si rendono conto di esserlo: se si prendono in esame le quattro fasi del riconoscimento dello stato di vittima sviluppate dal professor Emilio Viano, si riscontrerà che queste non sempre vengono affrontate, ma il problema sorge quando non si affronta neanche la prima fase, che è quella

[27]Per maggiori dettagli si rimanda a: S. Vezzadini (A cura di), I Centri di assistenza e supporto alle vittime di reato, Regione Emilia-Romagna

che aziona tutto il meccanismo di riflessione e di riconoscimento.

Le fasi sono infatti: la presenza di un danno, l'auto-riconoscimento della propria condizione, la richiesta di aiuto ed infine il riconoscimento di tale condizione da parte delle istituzioni e della società (Vezzadini, 2012).

Ed è proprio la prima che risulta necessaria per un primo passo verso il riconoscimento effettivo dello stato di vittima, ma nel caso dei crimini ambientali, questo non accade spesso: il danno subìto spesso viene percepito come un qualcosa di casuale, come un evento dovuto alla sfortuna, o al fato, assai difficilmente si prende in considerazione l'ipotesi che il danno sia effettivamente dovuto ad un'azione concreta fatta, tendenzialmente, con lo scopo di arricchirsi e con noncuranza, sia per quanto concerne le conseguenze sul piano prettamente ambientale, sia su quello relativo alla salute umana. Riuscendo infatti a scavalcare questo primo scoglio, un soggetto può iniziare a realizzare e a riconoscersi come vittima, può finalmente affermare che "quello che è successo non è giusto", ma anche questo trova degli ostacoli: emozioni contrastanti e sentimenti di vergogna, così come anche un'ulteriore sottovalutazione della situazione, poiché per quanto magari si sia riusciti ad individuare un danno, non è affatto detto che poi ci si percepisca come vittime, il problema potrebbe venir visto come lontano e non si riesce a coglierne la pericolosità effettiva (Viano, Monzani, 2014).

Qualora però si dovesse riuscire a superare le prime due fasi, la terza, la richiesta d'aiuto, per quanto concerne i crimini ambientali, risulta assai più facile. Come riporta infatti Monzani: «[…] sia le singole vittime sia associazioni o comitati delle stesse non hanno difficoltà nel richiedere un aiuto o un risarcimento per il danno subito.» (Viano, Monzani, 2014, p. 18), la difficoltà nel chiedere aiuto sorgerebbe più che altro quando il reato coinvolga anche associazioni di tipo mafioso, poiché, come riporta sempre Monzani, «dal momento che il pericolo costituito da un deposito di rifiuti tossico-nocivi potenzialmente dannoso per la salute sul lungo periodo può essere vissuto come meno grave rispetto a quello della potenziale ritorsione immediata della criminalità organizzata» (Viano, Monzani, 2014, p. 18).

La quarta fase, che chiama in campo le istituzioni, risulterebbe fondamentale per le vittime di reati ambientali, ma è solito che queste riconoscano effettivamente la presenza di un danno e di un reato, ma non «la vera e propria vittima intesa quale persona fisica,» (Viano, Monzani, 2014, p. 18), rendendo quindi il riconoscimento istituzionale parziale o talvolta nullo.

Pur essendo vittime "difficili" da identificare, è necessario assolutamente includerle negli studi della materia, è necessario riuscire ad aiutarle, a partire dal riconoscimento del loro stato di vittime, ed è assolutamente necessario sollecitare le istituzioni sulla loro presenza, sul fatto che coloro che subiscono il reato ed il danno sono persone vere, persone che hanno dei diritti e soprattutto che hanno una dignità.

Oltre a questo percorso di riconoscimento che può risultare particolarmente tortuoso, è importante sottolineare anche quali siano i fattori di rischio che possono portare a divenire un soggetto vittima di reati ambientali; sono fattori prettamente esterni alla persona, e Viano e Monzani li identificano ne: la posizione geografica, la pianificazione ambientale, l'attenzione della politica ambientale ed infine, il livello di cultura ambientale (Viano, Monzani, 2014).

Di questi, si vorrà analizzare soprattutto il primo e l'ultimo, poiché si ritiene siano i fattori di maggior interesse.

Si tiene prima a precisare una caratteristica fondamentale di questo tipo di vittime: sono altamente fungibili, ovvero facilmente scambiabili, sostituibili.

Abbiamo appena detto che i fattori di rischio sono prettamente esterni alla persona, infatti «una vittima è fungibile quando non possiede caratteristiche personali uniche, tali da farla preferire a ogni altra vittima in modo assoluto: essa non è diventata vittima per alcune sue caratteristiche personali e tali caratteristiche non hanno favorito, nemmeno inconsciamente, il comportamento criminoso.» (Viano, Monzani, 2014, p. 20), a sua volta, questa fungibilità è simbolo di una pericolosità sociale maggiore, in quanto «la pericolosità sociale di un autore di reato è direttamente proporzionale alla fungibilità delle sue vittime» (Viano, Monzani, 2014, p. 20).

Come riportava il Comandante 1, il rapporto tra reo e vittima nei crimini ambientali, non è 1:1 come può essere nell'omicidio, ma è di 1:X, evidenziando come la scelta delle vittime, non sia effettivamente una scelta, ma una pericolosa roulette russa che può coinvolgere chiunque.

La posizione geografica è senza ombra di dubbio il fattore di maggior peso: qualcuno che vive in campagna, nelle lande, lontano da aziende e da possibili pericoli (anche se in realtà con le questioni ambientali non si è mai veramente al sicuro) avrà sicuramente un rischio minore di essere vittima di un reato ambientale rispetto a qualcuno che vive ad esempio a Taranto, a causa dell'ILVA, così come anche avrà un rischio maggiore qualora viva nella Terra dei Fuochi, in Campania. Risulta essere inoltre un fattore di estrema importanza, in quanto, se si nasce, si cresce e si vive in un territorio, quello diventa casa, e lasciarlo appare difficile e doloroso: si è posti davanti alla scelta di restare dove vi sono le proprie radici e la propria vita, o di andar via per tutelare la propria salute. Si è posti quindi davanti ad un bivio per cui talvolta è difficile scegliere. Il livello di cultura ambientale, invece, rappresenta sia un fattore di rischio che, al contempo, un fattore di protezione: una buona cultura ambientale permetterà a chi la possiede di stare all'erta, di notare modifiche e anomalie, di riscontrare alterazioni nelle situazioni circostanti, ma favorirebbe anche un più rapido riconoscimento del danno e quindi faciliterebbe il processo di riconoscimento dello stato di vittima; d'altro canto, una formazione scarsa o nulla, permetterà di non notare queste differenze e quindi renderà il soggetto più facilmente incline a non percepire un pericolo.

4.1 Vittime: dalla teoria alla (triste) pratica

Abbiamo visto finora come il concetto di crimine ambientale sia ampio, sia da un punto di vista etimologico e documentale, e parrebbe quasi logico ipotizzare che anche le vittime di un reato ambientale debbano avere la stessa ampiezza, ovvero si dovrebbe ritenere vittima non solo la persona che subisce in un primo momento e direttamente il danno.

Se, anche qui, si cerca etimologicamente il significato primario della parola vittima, lo si può rintracciare sempre in due termini latini, *Vincīre* e *Vincĕre*. Il primo termine ha significato di legare, tenere fermo, richiamando a coloro, animali ed esseri umani, che venivano sacrificati alle divinità nell'antichità, mentre il secondo ha il significato di vincere, sconfiggere, prevalere, e richiama «la condizione esperita da colui che soggiaceva all'azione del vincitore lo sconfitto» (Vezzadini,

2012, p. 89). La vittima si identificherebbe quindi in quel soggetto che in un modo o nell'altro si trova «impossibilitato a reagire e destinato a piegarsi suo malgrado al volere del vincitore» (Vezzadini, 2012, p. 89).

Tale visione è riportata anche a livello internazionale, in cui la vittima viene spesso identificata come un elemento sacrificale a beneficio e vantaggio di un'entità più potente, di un bene superiore (Williams, 1996).

Ma nell'ordinamento odierno, come vengono effettivamente identificate le vittime?

All'interno del diritto penalistico italiano non si parla e non si utilizza mai il termine "vittima", bensì si fa riferimento alla "persona offesa dal reato", che ha la possibilità, per quanto stabilito dal Codice di Procedura Penale, di costituirsi parte civile in un procedimento penale[28].

Sebbene vi sia questa grande mancanza in Italia, a livello internazionale la questione risulta più complessa ma al contempo esaustiva: sono presenti infatti atti che trattano la materia delle vittime e che ne danno una definizione. Tra queste una risulterà di particolare interesse a sostegno della nostra tesi, ma si preferisce esporre prima tutte le versioni così da motivare puntualmente la scelta fatta.

Il primo che prenderemo in esame è la dichiarazione A/RES/40/34 della Nazioni Unite del 29 Novembre 1985. Nella Dichiarazione dei Principi Fondamentali di Giustizia per le Vittime di Reato e di Abuso di Potere si ritrova una definizione di "vittime del crimine", che vengono identificate in «[...] quelle persone che, sia singolarmente che collettivamente, abbiano subito dei danni, ivi compreso il ferimento sia fisico che mentale, la sofferenza emotiva, la perdita economica o l'indebolimento sostanziale dei loro diritti fondamentali, attraverso atti o omissioni che violano le leggi contro il crimine, in vigore negli Stati membri, ivi comprese quelle leggi che proscrivono l'abuso criminale di potere. In base alla presente Dichiarazione, una persona può essere definita vittima, anche in mancanza dell'identificazione, dell'arresto, del perseguimento della condanna dell'autore materiale del reato e indipendentemente dal fatto che ci sia qualche grado di parentela tra l'autore e la vittima. Il termine "vittima" comprende pure, ove del caso, la famiglia e parenti stretti o i dipendenti della vittima e le persone che hanno subito un danno nell'intervenire nel tentativo di soccorrere le vittime in pericolo o di evitare una eventuale vittimizzazione. I provvedimenti contenuti nella dichiarazione sono "applicabili ad ogni persona, senza distinzione [...]"» (Nazioni Unite, 1985)[29].

La seconda, invece, risale a venti anni dopo, e la si può ritrovare nella Decisione Quadro 2001/220/GAI del Consiglio d'Europa relativa alla posizione della vittima nel procedimento penale. Qui, all'articolo 1, lettera a) si legge infatti che la vittima è «[...] la persona fisica che ha subito un pregiudizio, anche fisico o mentale, sofferenze psichiche, danni materiali causati direttamente da atti o omissioni che costituiscono una violazione del diritto penale di uno Stato membro.» (Consiglio d'Europa, 2001).

La terza ed ultima la si ritrova nella Direttiva 2012/29/UE del Parlamento Europeo e del Consiglio, che va a sostituire la Decisione quadro appena vista; al suo interno, al Capo I, Articolo 2

[28]Per maggiori approfodimenti e dettagli si veda: https://www.brocardi.it/codice-di-procedura-penale/libro-primo/titolo-v/art74.html

[29]Per approfondimenti e lettura della definizione completa si rimanda a: Nazioni Unite - Dichiarazione dei Principi Fondamentali di Giustizia per le Vittime di Reato e di Abuso di Potere (A/RES/40/34) del 29/11/1985. URL: http://briguglio.asgi.it/immigrazione-e-asilo/2007/luglio/diritti-vittime-crimine.pdf

(che disciplina le definizioni), si può leggere subito alla lettera a) che si intende per vittima «i) una persona fisica che ha subìto un danno, anche fisico, mentale o emotivo, o perdite economiche che sono stati causati direttamente da un reato;

ii) un familiare di una persona la cui morte è stata causata direttamente da un reato e che ha subito un danno in conseguenza della morte di tale persona;» (Parlamento e Consiglio Europeo, 2012).

Dopo questo primo quadro generale, è indubbio ritenere che la prima definizione, quella del 1985, pur essendo la più vecchia, sia anche la più completa ed inclusiva: non solo riconosce ed enumera una vasta categoria di danni che possono essere subìti, ma individua la vittima sia singolarmente che collettivamente, ed è proprio nei crimini ambientali che spesso le vittime non sono singole, il rapporto non è 1:1, ma colpiscono un vasto numero di soggetti; introdurre quindi il termine "collettivamente", crea una comunità all'interno della comunità stessa che è stata colpita, consentendo un mutuo aiuto e soccorso, e soprattutto, potrebbe concedere quella forza di chiedere giustizia insieme.

Altro aspetto importante, presente però anche nella Direttiva del 2012, è il riconoscimento della famiglia come vittima ulteriore: si è visto nei casi di crimini ambientali di come le famiglie anche patiscano e soffrano stando a contatto con un familiare malato. È giusto e doveroso quindi riconoscerle come vittime a tutti gli effetti.

Ultimo punto di interesse, ma non per importanza, è il riconoscimento della vittima anche se non vi sia un colpevole, anche se questo non sia rintracciato e processato. Questo è molto significativo quando si trattano i crimini ambientali, in quanto non è sempre detto che il colpevole venga assicurato alla giustizia, ma questo non rende la vittima meno vittima. La situazione potrebbe però lasciare un sentimento di sconforto: vi è un riconoscimento del proprio stato di vittima, di persona che ha subito un danno, ma non si è riusciti ad avere effettivamente giustizia.

Si può ritenere, quindi, a tutti gli effetti che, se si vuole ampliare il proprio campo interpretativo dei crimini ambientali, lo si deve fare anche attraverso le vittime, e quindi una definizione ampia, ma pur sempre ben articolata, ed inclusiva, come quella del 1985, sia la migliore, poiché permette un riconoscimento effettivo, puntuale e chiaro.

Il professor Williams, criminologo, ha espresso un'opinione in merito alla definizione delle Nazioni Unite, e afferma come questa «fornisce un punto di partenza e sembra prevedere le probabili preoccupazioni di una visione ambientale.»[30] (Williams, 1996, p. 18); Williams infatti si sofferma soprattutto sull'importanza dell'aspetto delle "mancanze", delle omissioni e delle azioni prese con avventatezza in relazione ai crimini ambientali. Da ciò ricava infatti una definizione di chi sono le vittime ambientali, le quali vengono definite come «quelli della generazione passata, presente o futura che sono danneggiati a seguito di un cambiamento nell'ambiente chimico, fisico, microbiologico o psicosociale, determinato da un atto intenzionale o sconsiderato, individuale o collettivo, umano o di omissione»[31] (Williams, 1996, p. 21).

Una definizione che appare comprensiva di più generazioni, non soffermandosi solo su quelle passate e presenti, ma pensando anche alle vittime

[30] Testo originale: [...] (it) provides a starting point, and appears prescient of the likely concerns of an environmental view.

[31] Testo originale: those of past, present, or future generation who are injured as a consequence of change to the chemical, physical, microbiological, or psychosocial environment, brought about by deliberate or reckless, individual or collective, human act or act of omission

future, come i bambini[32], ma che si limita ancora una volta a vedere l'ambiente sotto una prospettiva di tipo prettamente naturalistico e, oseremmo dire, scientifico. Inoltre, la definizione data da Williams, perde molti degli elementi della definizione originale dell'85 che abbiamo visto invece essere perfettamente in sintonia con le vittime ambientali.

In generale, comunque, si può sostenere che si stia andando a cercare di inglobare e riconoscere come vittime ambientali sempre più soggetti, *e* questa comprensività la si può riscontrare anche nelle storie di vere vittime di crimini ambientali, sia innocenti che del dovere, di cui riteniamo doveroso parlare, non solo per rafforzare la nostra tesi, ma anche per rispetto verso di loro. Parleremo di alcune vittime illustri, che hanno ottenuto nel tempo il riconoscimento del loro status e del nesso causale che è stato finalmente provato per quanto riguarda il caso della Terra dei Fuochi.

Partendo dal secondo, nel 2015 l'Istituto Superiore di Sanità pubblica il rapporto Mortalità, ospedalizzazione e incidenza tumorale nei Comuni della Terra dei Fuochi in Campania (relazione ai sensi della Legge 6/2014)[33], in cui si evidenziava un'incidenza tumorale molto alta nella zona, e questo valeva sia per gli adulti che per i bambini.

Fu poi nel 2021 che si raggiunse una svolta. Un anno dopo la pubblicazione del rapporto sulla mortalità, nel Giugno del 2016, infatti, la Procura di Napoli e l'ISS avviano un lavoro di ricerca che si concluderà nel Febbraio del 2021 con la pubblicazione del Rapporto finale, (Dicembre 2020) Studio sull'impatto sanitario degli smaltimenti controllati ed abusivi di rifiuti nei 38 comuni del circondario della Procura della Repubblica di Napoli Nord[34], ed è proprio questo documento a dimostrare la relazione causale tra le condizioni di salute di un buono spicchio della popolazione interessata e lo smaltimento illecito di rifiuti. Questo documento rappresenterebbe l'ultima di quelle famose fasi del riconoscimento di Viano: il riconoscimento da parte delle istituzioni. Con questo documento finalmente si riconosce, a tutti gli effetti, a quelle persone lo status di vittima, e lo si dovrebbe riconoscere non solo a coloro che sono malati o che non ci sono più, ma anche ai loro familiari, ai loro amici, a tutti coloro che stanno soffrendo per questa situazione, come indicato dalla definizione del 1985.

Anche le vittime del dovere, o chi per loro, talvolta, hanno dovuto lottare per vedersi riconoscere questo status, e qui vi è anche la beffa, oltre al danno, perché molte di loro sono scomparse proprio in seguito alle loro indagini o alle loro ricerche della verità e della giustizia.

Come il caso di Domenico, detto Mimmo, Beneventano, che ha lottato ad Ottaviano insieme all'amico Pasquale Cappuccio denunciando negli anni '70, attraverso il loro impegno politico, la Camorra ed i suoi traffici illeciti. Sia Mimmo che Pasquale saranno poi assassinati per questo, rispettivamente nel 1980 e nel 1978 (Cianciullo, Fontana, 2012).

Doveroso poi citare anche il caso di Ilaria Alpi e del suo collega Miran Hrovatin, che sono stati assassinati entrambi in Somalia durante un'imboscata mentre indagavano su dei traffici

[32] Williams dedica una parte del suo lavoro all'analisi del fenomeno delle "vittime non ancora nate" (the unborn victims), sottolineando come i bambini non ancora nati possano essere riconosciute come vittime, come nei casi in cui «atti o omissioni, che interessano i genitori prima del concepimento, possono costituire vittimizzazione di un nascituro». (Williams, 2012, pp. 24-25)

[33] Si veda per approfondimenti e per il documento completo: https://www.quotidianosanita.it/allegati/allegato2334416.pdf

[34] Per maggiori dettagli e per visionare il documento completo si rimanda a: accordo di collaborazione scientifica tra istituto superiore di sanità e procura della repubblica di napoli nord (prot.n.1104 procuratore del 23 giugno 2016), url: https://www.procuranapolinord.it/allegatinews/A_42657.pdf

illeciti di rifiuti che coinvolgevano il Paese. Il loro caso risulta tutt'ora lacunoso e senza una vera risposta, tant'è che in merito è stata aperta una commissione parlamentare d'inchiesta[35] (Cianciullo, Fontana, 2012).

Una sorte diversa l'ha avuta invece il sostituto commissario di polizia Roberto Mancini, venuto a mancare nell'Aprile del 2014 dopo 12 anni di lotta contro il linfoma non-Hodgkin, diagnosticatogli nel 2002 dopo aver lavorato per anni al caso della Terra dei Fuochi. Lo Stato gli erogò per questo un indennizzo di 5.000 euro, riconoscendo il suo cancro come "causa di servizio", ma questo non fu abbastanza e Mancini iniziò una lotta contro lo Stato per chiedere giustizia, ma non ne vide mai l'esito. Solo dopo la sua morte, dopo proteste e dopo petizioni online, il Ministero, nel Settembre dello stesso anno, gli riconobbe lo stato di "vittima del dovere" e venne insignito della Medaglia d'argento alla Memoria consegnata dal Capo della Polizia[36].

E come non parlare poi del Comandante Natale De Grazia, anche lui insignito di una medaglia, la Medaglia d'oro al Merito di Marina alla memoria, la cui morte risulta tutt'oggi, a distanza di anni, sospetta, soprattutto se si considerano le dinamiche della sua morte e si tiene conto del fatto che il Comandante stesse indagando sulle navi a perdere (Cianciullo, Fontana, 2012; Bocca, 2008); in merito a ciò, come riportato dalla moglie Anna, «Natale non si sarebbe fermato e […] qualunque cosa stesse cercando, certamente l'avrebbe trovata. Non si sarebbe risparmiato e avrebbe compiuto fino in fondo il suo dovere [...].»(Il Reggino- Foti, 2021).

Anche per lui, come per Ilaria e Miran fu aperta una commissione parlamentare d'inchiesta[37] ed anche in questo caso non vi fu una risoluzione, anzi, si tornò a ribadire che il suo caso fosse (e lo è ancora oggi) un mistero.

5. Conclusioni

Con il presente articolo si è tentato di dimostrare come ci siano le basi per un effettivo cambiamento in merito alla questione ambientale, di come ci siano effettivamente i presupposti per una modifica vera e concisa della percezione dei crimini ambientali, non limitandosi solo al modo di pensare dei classici cittadini, ma anche, e soprattutto, degli studiosi, dei criminologi, degli storici, dei letterati, dei giuristi.

Si è dimostrato infatti che i presupposti per un ampliamento ed un inserimento di contenuti ed elementi di studio ci sono e sono forti, provenienti tra l'altro da fonti istituzionalmente rilevanti. Non mancano però, come si era già anticipato all'inizio, le difficoltà ed i limiti affinché questo si realizzi: si è visto infatti come la concezione ambientale, sia nel

[35]Per visionare i risultati della commissione d'inchiesta si rimanda a: Commissione parlamentare d'inchiesta sulla morte di Ilaria Alpi e Miran Hrovatin, Camera dei Deputati. URL: http://leg14.camera.it/_dati/leg14/lavori/documentiparlamentari/indiceetesti/022bis/001/INTERO.pdf

[36] Per conoscere più nel dettaglio la vicenda, si rimanda ai seguenti articoli giornalistici: Luca Ferrari, 2014, Morto il poliziotto che ha combattuto le ecomafie. Ucciso dalla leucemia dovuta ai veleni che ha respirato. Alfano dispone i funerali solenni per il commissario morto a 53 anni "per causa di servizio", La Repubblica, 30 Aprile URL: https://www.repubblica.it/cronaca/2014/04/30/news/morto_il_poliziotto_che_ha_combattuto_le_ecomafie_ucciso_dalla_leucemia_dovuta_ai_veleni_che_ha_respirato-84841398/#:~:text=Roberto%20Mancini%20era%20sostituto%20commissario,illecito%20di%20rifiuti%20in%20Campania. e Terra Fuochi, Roberto Mancini "vittima del dovere". Indagava su rifiuti tossici, 2015, Il Fatto Quotidiano, 14 Gennaio. URL: https://www.ilfattoquotidiano.it/2015/01/14/rifiuti-tossici-roberto-mancini-vittima-dovere-indagavaterra-dei-fuochi/1338594/

[37]Per visionare più nel dettaglio le indagini della commissione, si veda: Commissione parlamentare di inchiesta sulle attività illecite connesse al ciclo dei rifiuti (istituita con legge 6 febbraio 2009, n. 6), relazione sulla morte del capitano di fregata Natale de Grazia (Relatori: On. Gaetano Pecorella e On. Alessandro Bratti) Approvata dalla Commissione nella seduta del 5 febbraio 2013, Senato della repubblica. URL: https://www.senato.it/service/PDF/PDFServer/BGT/698102.pdf

passato che in letteratura, sia particolarmente incentrata sull'aspetto naturalistico; al contempo, si è trovato dal punto di vista criminologico una concezione del fenomeno sì ampio, ma particolarmente incentrato su una visione dualistica, in cui la *green criminology* è legata ad aspetti prettamente capitalistici ed industriali, e naturalistici, legati strettamente alla flora ed alla fauna. Tutto questo è perfettamente in linea con quanto potrebbe essere la criminologia ambientale se la si sviluppasse appieno, ma non la costituisce nella sua totalità.

Appare comunque evidente, come ulteriore limite, che questo possibile cambiamento nella pratica si realizzi molto lentamente o non si realizzi affatto: andare a modificare infatti le convinzioni e le interpretazioni delle persone è un processo lungo e che richiede tempo, per non parlare della possibilità di trasformare l'ordinamento giuridico, sia a livello nazionale che internazionale. Un'azione così considerevole e invasiva potrebbe portare solo confusione e destabilizzare gli addetti ai lavori, soprattutto nei primi tempi.

Un passaggio verso il cambiamento che si potrebbe fare è quello di correggere la denominazione, ovvero identificare la maggior parte dei reati ambientali che attualmente sono normati come reati contro l'ambiente "naturale". Quel "naturale" permetterebbe di dividerlo dall'altro ambiente, quello più "artificiale", che però in relazione all'uomo rappresenta il più frequentato e vissuto. In questo modo si saprebbe che esistono altri tipi di reati che coinvolgono l'ambiente, seppur non vi sia un testo che li raccolga tutti, in quanto spesso appartengono ad altre categorie di reati, come ad esempio la contraffazione che costituisce un reato economico.

Un possibile cambiamento su questo fronte potrebbe favorire un riconoscimento dello status di vittime a quelle persone che attualmente brancolano nel buio in quanto non riescono a identificare la natura del loro danno, così come potrebbe anche aiutarle a sviluppare forme di prevenzione e di difesa.

Con questo non si vuole quindi escludere l'ampliamento della visione vittimologica sostenuta da alcuni criminologi ambientali che ritenevano vittime anche gli animali e su cui hanno dedicato studi, anzi, la si vuole estendere ancora di più, integrare, seppur dal punto di vista prettamente antropocentrico e non ecocentrico come sostenuto da studiosi come White. L'approfondimento proposto andrebbe in automatico a far rientrare anche flora e fauna, poichè l'ambiente costituisce ciò che ci circonda, ma non ha valore solo per gli esseri umani, bensì per tutte le forme di vita, dalla più piccola fino alla più grande.

Confidiamo che attraverso queste pagine si sia riusciti a portare sufficienti prove a sostegno della tesi di partenza, ovvero che un ampliamento della visione ed interpretazione ambientale è possibile, e che queste, pur con enormi ostacoli e limiti, possano in futuro contribuire ad un'effettiva evoluzione degli studi inerenti alla criminalità ambientale, favorendone quindi un contrasto ancora più attivo ed efficace.

Bibliografia

1. Banfield E., *Le basi morali di una società arretrata*, Il Mulino, Bologna, 2010.
2. Bocca R., *Le navi della vergogna*, BUR-Rizzoli, Milano, 2008.
3. Cianciullo A., Fontana E., Dark *Economy. La mafia dei veleni*, Einaudi, Torino, 2012.
4. Corona G., *Breve storia dell'ambiente in Italia*, Il Mulino, Bologna, 2015.

5. Felice E., *Perché il Sud è rimasto indietro*, Il Mulino, Bologna, 2016.
6. Gentile D, *La questione rifiuti nell'ordinamento italiano. Genesi e fenomenologia delle ecomafie*, Aracne, 2017.
7. McNeill J., *Qualcosa di nuovo sotto il sole. Storia dell'ambiente nel XX secolo*, Einaudi, Torino, 2020.
8. Mosley S., *Storia globale dell'ambiente*, Il Mulino, Bologna, 2013.
9. Natali L., *Green Criminology. Prospettive emergenti sui crimini ambientali*, Giappichelli, Torino, 2015.
10. Potter G., et al., «The Geography of Environmental Crime», in Potter G. *et al.*, *The Geography of environmental crime. Conservation, wildlife crime and environmental activism*, Palgrave Macmillan, 2016, p. 1-10.
11. Putnam R., *La tradizione civica nelle regioni italiane*, Mondadori, Milano, 1996.
12. Renda F., *La storia della mafia*, Pietro Vittorietti, Palermo, 1998.
13. Sicurella S., *Da quel giorno mia madre ha smesso di cantare. Storie di Mafia*, Giappichelli, Torino, 2017.
14. Vezzadini S., *Per una sociologia della Vittima*, FrancoAngeli, Milano, 2012.
15. Vezzadini S. (a cura di), *I Centri di assistenza e supporto alle vittime di reato*, Regione Emilia-Romagna.
16. Viano E., Monzani M., *Madre Terra è stanca! Il saccheggio della natura per arricchire pochi e impoverire molti*, Libreriauniversitaria.it, 2014.
17. White R., The Conceptual Contours of «Green Criminology», in Walters R. *et al., Emerging Issues in Green Criminology. Exploring Power, Justice and Harm*, Palgrave Macmillan, 2013, pp. 17-33.
18. White R., *Transnational Environmental Crime. Toward an eco-global criminology*, Routledge Taylor & Francis group London and New York, 2011.
19. Williams C., «An Environmental Victimology», *Justice: a Journal of Crime, Conflict and World Order*, Vol. 23 (4 (66)), 1996, pp. 16-40.

Sitografia[38]

1. https://eur-lex.europa.eu/legal-content/IT/LSU/?uri=celex:32008L0099
2. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/eurojust_it
3. https://navideiveleni.legambiente.it/navi-a-perdere/storia.php
4. https://web.archive.org/web/20151102035644/http://archiviostorico.corriere.it/1997/ottobre/02/Dell_Utri_Chiambretti_mafia_modo_co_0_9710022934.shtml
5. https://www.brocardi.it/codice-di-procedura-penale/libro-primo/titolo-v/art74.html
6. https://www.brocardi.it/codice-penale/libro-secondo/titolo-v/art416bis.html
7. https://www.brocardi.it/codice-penale/libro-secondo/titolo-vi-bis/art452quaterdecies.html
8. http://www.comitatodegrazia.org/Blog/il-fiume-oliva-affogato-nei-rifiuti.html
9. https://www.gazzettaufficiale.it/eli/gu/1986/07/15/162/so/59/sg/pdf
10. https://www.legambiente.it/?s=abbatti+l%27abuso
11. https://www.legambiente.it/comunicati-stampa/i-dati-del-rapporto-ecomafia-2020-nel-2019-in-aumento-i-reaticontro-lambiente/
12. http://www.pratiarmati.it/caratteristiche-geotecniche/erosione-del-suolo/
13. https://www.quotidianosanita.it/allegati/allegato2334416.pdf
14. https://www.reggiotoday.it/cronaca/sversamenti-frantoi-controlli-e-denunce-nella-piana.html
15. https://www.salernotoday.it/cronaca/sversamenti-rifiuti-denunce-carabinieri-noe-15-ottobre-2019.html
16. https://www.youtube.com/watch?v=WQ2NdOMBss0&ab_channel=MrAlfonsino

[38] L'ultima visualizzazione dei link e dei documenti online è avvenuta in data 9 Dicembre 2022.

17. Accordo di collaborazione scientifica tra Istituto Superiore di Sanità e Procura della Repubblica di Napoli Nord (prot.n.1104 procuratore del 23 giugno 2016), procuranapolinor.it. URL: https://www.procuranapolinord.it/allegati news/A_42657.pdf
18. Anna Foti, 2021, Reggio, vedova De Grazia: «Attraverso la vita dei miei figli e il loro amore per la natura, rivedo il mio Natale», Il Reggino, 13 dicembre. URL: https://www.ilreggino.it/cronaca/2021/12 /13/reggio-vedova-de-grazia-attraverso-la-vita-dei-miei-figli-e-il-loro-amore-per-la-natura-rivedo-il-mio-natale/
19. Anna Foti, 2021, Rigel, la nave scomparsa con il suo carico e i suoi segreti il 21 settembre 1987, Lacnews24.it, 21 settembre; URL: https://www.lacnews24.it/cultura/rigel-la-nave-scomparsa-con-il-suo-carico-e-i-suoi-segreti-il-21-settembre-1987-_143068/
20. Commissione parlamentare di inchiesta sui fenomeni della contraffazione, della pirateria in campo commerciale e del commercio abusivo, resoconto stenografico audizione 78. seduta di martedì 6 giugno 2017; URL: https://documenti.camera.it/leg17/resoconti/commissioni/stenografici/pdf/64/audiz2/audizione/2017/06/06/leg.17.stencomm.data20170606.U1.com64.audiz2.audizione.0078.pdf
21. Commissione parlamentare di inchiesta sulla morte di Ilaria Alpi e Miran Hrovatin, Camera dei Deputati. URL: http://leg14.camera.it/_dati/leg14/lavori/documentiparlamentari/indiceetesti/022bis/001/INTERO.pdf
22. Commissione parlamentare di inchiesta sulle attività illecite connesse al ciclo dei rifiuti (istituita con legge 6 febbraio 2009, n. 6), relazione sulla morte del capitano di fregata Natale De Grazia (relatori: on. Gaetano Pecorella e on. Alessandro Bratti), approvata dalla Commissione nella seduta del 5 febbraio 2013, Senato della Repubblica. URL: https://www.senato.it/service/PDF/PDFServer/BGT/698102
23. Commissione parlamentare di inchiesta sulle attività illecite connesse al ciclo dei rifiuti (istituita con legge 6 febbraio 2009, n. 6), relazione territoriale sulle attività illecite connesse al ciclo dei rifiuti nella Regione Campania, approvata dalla Commissione nella seduta del 5 febbraio 2013. URL: https://www.senato.it/service/PDF/PDFServer/BGT/698083.pdf
24. Costituzione della Repubblica Italiana, Senato della Repubblica, articolo 117. URL: https://www.senato.it/istituzione/la-costituzione/parte-ii/titolo-v/articolo-117
25. Decisione quadro del consiglio del 15 marzo 2001 relativa alla posizione della vittima nel procedimento penale (2001/220/GAI), Eur-Lex. URL: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32001F0220&from=IT
26. Direttiva 2012/29/UE del parlamento europeo e del consiglio del 25 ottobre 2012 che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI, Giustizia.it. URL: https://www.giustizia.it/resources/cms/documents/sgep_tavolo18_allegato3.pdf
27. Eurojust Relazione Annuale, 2014, Eurojust. URL: https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_annual_report_2014_en.pdf
28. Interpol Cooperation Against 'Ndrangheta (I-CAN), Interpol. URL: https://www.interpol.int/Crimes/Organized-crime/INTERPOL-Cooperation-Against-Ndrangheta-I-CAN
29. La riforma costituzionale in materia di tutela dell'ambiente, 2021, Dipartimento per le riforme istituzionali- Presidenza del Consiglio dei Ministri. URL: https://www.riformeistituzionali.gov.it/it/la-legge-costituzionale-in-materia-di-tutela-dell-ambiente/
30. Luca Ferrari, 2014, Morto il poliziotto che ha combattuto le ecomafie. Ucciso dalla leucemia dovuta ai veleni che ha respirato. Alfano dispone i funerali solenni per il

commissario morto a 53 anni "per causa di servizio", La Repubblica, 30 aprile URL: https://www.repubblica.it/cronaca/2014/04/30/news/morto_il_poliziotto_che_ha_combattuto_le_ecomafie_ucciso_dalla_leucemia_dovuta_ai_veleni_che_ha_respirato-84841398/#:~:text=Roberto%20Mancini%20era%20sostituto%20commissario,illecito%20di%20rifiuti%20in%20Campania

31. Nazioni Unite - Dichiarazione dei Principi Fondamentali di Giustizia per le Vittime di Reato e di Abuso di Potere (A/RES/40/34) del 29/11/1985. URL: http://briguglio.asgi.it/immigrazione-e-asilo/2007/luglio/diritti-vittime-crimine.pdf
32. Pollution crime, Interpol. URL: https://www.interpol.int/Crimes/Environmental-crime/Pollution-crime
33. Relazione al Parlamento della Direzione Investigativa Antimafia del Primo Semestre del 2019. URL: https://direzioneinvestigativaantimafia.interno.gov.it/semestrali/sem/2019/1sem2019.pdf
34. Relazione al Parlamento della Direzione Investigativa Antimafia del Secondo Semestre del 2019. URL: https://direzioneinvestigativaantimafia.interno.gov.it/semestrali/sem/2019/2sem2019.pdf
35. Seduta 704 di Venerdì 26 ottobre 1951 (Seduta pomeridiana), Senato della Repubblica. URL: https://www.senato.it/service/PDF/PDFServer/BGT/487606.pdf
36. Terra Fuochi, Roberto Mancini "vittima del dovere". Indagava su rifiuti tossici, 2015, Il Fatto Quotidiano, 14 gennaio. URL: https://www.ilfattoquotidiano.it/2015/01/14/rifiuti-tossici-roberto-mancini-vittima-dovere-indagavaterra-dei-fuochi/1338594/

doi: 10.14664/rcvs/249

Agli albori della prevenzione situazionale: l'attualità dei sostitutivi penali di Enrico Ferri

À la naissance de la prévention situationnelle : l'actualité des substituts pénaux de Enrico Ferri

At the dawn of the situational prevention: the relevance of the penal substitutes of Enrico Ferri

*Natalia Coppolino**

Riassunto
Muovendo dalla legge di saturazione criminosa con attenzione alla multi-fattorialità causale del delitto, l'articolo si concentra sui sostitutivi penali, che compensano la mancanza di pene adeguate e promuovono la difesa sociale.
I concetti di punibilità e pena portano al confronto tra scuola classica e scuola positiva di criminologia, all'interno della quale Enrico Ferri si inserisce pur presentando elementi dissonanti ed innovativi. L'analisi dei sostitutivi penali proposti da Ferri in diversi ambiti (economico, politico, scientifico, legislativo/amministrativo, religioso, famigliare e educativo) sarà propedeutica all'esame della prevenzione sociale. Gli elementi innovativi individuati da Ferri sono stati sviluppati negli anni successivi da specialisti del design urbano per incidere sulla percezione di (in)sicurezza e di conseguenza sulla qualità della vita. Obiettivo dell'articolo è mettere in luce la correlazione tra la teorizzazione di Ferri e gli accorgimenti pratici di studiosi quali gli Ecologi di Chicago, Angel, Newman, Jacobs, Jeffery, Wilson e Kelling e così mostrare l'importanza e l'attualità della prevenzione situazionale del crimine. Uno spazio di riflessione verrà, infine, dedicato ad implementazioni contemporanee e prospettive future.

Résumé
A partir de la loi de « saturation criminelle », en prêtant attention à la nature causale multifactorielle de la criminalité, l'article se concentre sur les substituts pénaux, qui compensent le manque de peines adéquates et favorisent la défense sociale.
Les concepts de punissabilité et de peine conduisent à une comparaison entre l'école classique et l'école positive de criminologie. Enrico Ferri constitue l'un des penseurs les plus représentatifs de cette dernière, bien que son approche présente des éléments dissonants et novateurs. L'analyse des substituts pénaux proposés par Ferri dans différents domaines (champs économique, politique, scientifique, législatif/administratif, religieux, familial et éducatif) sera préparatoire à l'examen de la prévention sociale. Au cours des années suivantes, les éléments novateurs identifiés par Ferri ont été développés par des spécialistes de l'aménagement urbain dans l'objectif d'influer sur la perception de l'(in)sécurité et, par conséquent, sur la qualité de vie. Le but de l'article est de mettre en évidence la corrélation entre la théorisation de Ferri et les solutions pratiques adoptées par les sociologues de l'école de Chicago et d'autres chercheurs (Angel, Newman, Jacobs, Jeffery, Wilson et Kelling), et ainsi montrer l'importance et l'actualité de la prévention situationnelle du crime. Enfin, un espace de réflexion sera réservé aux implémentations contemporaines et aux perspectives futures.

Abstract
Starting from the law of criminal saturation in relation to the multifactorial causes of crimes, the article focuses on the penal substitutes that compensate for a lack of fair punishments and encourage the social defense against crime. The concepts of punishability and penalty lead us to the comparison between the classical and positive criminological schools. Ferri is one of the most famous representatives of the positive school, but in his works he introduces discordant and innovative elements. In order to examine social prevention, the article will focus on Ferri's suggestions in economic, political, scientific, legal/administrative, religious, domestic, educational fields. Moving from the innovations introduced by Ferri's work, urban design experts developed during the following years new items in order to affect insecurity perception and consequently improve the quality of life. The aim of the article is to highlight the correlations between Ferri's theorization and the practical suggestions proposed by the sociologists of the Chicago School and other researchers (Angel, Newman, Jacobs, Jeffery, Wilson and Kelling) in order to demonstrate the relevance and modernity of the situational prevention crime theory. Finally, it will be presented a reflection about contemporary implementations and future perspectives

Key words: prevenzione situazionale, desing ambientale, sostitutivi penali, sicurezza urbana

* Laureata in Scienze Criminologiche per l'investigazione e la sicurezza. Tutor Didattico in Sociologia della Devianza – Alma Mater Studiorum Università di Bologna.

1. Introduzione

Obiettivo principale dell'articolo è presentare la teoria dei sostitutivi penali proposta da Enrico Ferri, per ragionare così su alcuni accorgimenti specifici, che ripresi negli anni successivi divennero punti cardine della prevenzione situazionale del crimine.

Si procede in primo luogo all'analisi dei concetti fondamentali che animarono il dibattito creatosi tra gli studiosi appartenenti alle scuole classica e positiva. È proprio alla tradizione positiva che appartengono le riflessioni di Ferri, il quale concentrandosi sui temi «relativi all'uomo che delinque, al delitto e al dramma giudiziario che ne consegue» (Bisi, 2004, p. 20) si distingue in modo particolare per alcuni elementi innovativi per l'epoca, come l'attenzione alle vittime del reato ed alla prevenzione sociale.

Operato un breve confronto tra le scuole e posti in luce gli aspetti di continuità ed innovazione proposti da Ferri, sarà necessario soffermarsi sulla legge di saturazione criminosa quale premessa imprescindibile per comprendere la teoria dei sostitutivi penali.

Un'attenzione particolare verrà rivolta alla multifattorialità causale del delitto poiché qui si riscontrano gli elementi di base per la realizzazione della prevenzione sociale.

Muovendo da questi aspetti si procederà alla presentazione della teoria dei sostitutivi penali che abbracciano molteplici ambiti della vita dell'uomo singolo ed associato, si metteranno dunque in luce gli aspetti peculiari che successivamente convoglieranno nella prevenzione situazionale del crimine.

Nel tentativo di cogliere l'importanza delle riflessioni proposte da Ferri si presenteranno i suggerimenti di alcuni studiosi del *design* ambientale, che nella seconda metà del 1900 si concentrano sulla progettazione urbana come antidoto al dilagante senso di insicurezza che si stava diffondendo in città.

La città quale palcoscenico di ogni azione umana diventa luogo di attenzione particolare della sociologia, partendo dalle riflessioni sullo spazio urbano proposte dagli studiosi della Scuola Ecologia di Chicago, verranno presentati gli elementi principali del pensiero di Schlomo Angel, Oscar Newman, Jane Jacobs, Ray Jeffery, James Q. Wilson e George L. Kelling.

Questa breve rassegna sarà utile a mostrare come gli spunti teorici offerti da Ferri si siano evoluti nel corso del tempo.

In fase conclusiva verranno analizzati alcuni progetti realizzati in ambito urbano con l'obiettivo specifico di incidere sulla commissione di crimini per ridurre la percezione di insicurezza, rinsaldare i legami umani incidendo sull'anonimato ed in ultima istanza sulla qualità della vita.

È con questo spirito che nella seconda metà del 1900 prendono il via iniziative quali il *Chicago Area Project* ed il *Clean and Safe Neighborhood Program*, mentre più di recente si sono affermate nuove tecniche di sicurezza urbana (*community policing, neighborhood watch, social street*) delle quali si presenteranno brevemente le caratteristiche principali.

Il dibattito sulla prevenzione sociale, inaugurato in modo lungimirante da Ferri, continua a destare grande interesse in modo particolare se legato a progetti di rigenerazione urbana e co-progettazione partecipata, sui quali ci si soffermerà nella fase conclusiva dell'articolo.

2. Punibilità e pena: scuole a confronto

Per riuscire a cogliere pienamente l'aspetto innovativo di Enrico Ferri, espresso magistralmente

nella teorizzazione dei sostitutivi penali, risulta necessario operare, seppur brevemente, un confronto con la scuola classica sugli elementi inerenti ai concetti di: punibilità, pena, istituto della pena di morte, sistema carcerario, funzione dello stato, trattamento del reo, attenzione alla vittima.

È proprio nelle parole di Ferri che si individuano alcuni elementi di critica alla trattazione della scuola classica, quando egli afferma che i membri della scuola si fossero concentrati quasi esclusivamente sull'autore del reato, dimenticandosi di «una caterva ben più numerosa d'infelici, che stentano la vita intorno a noi miseramente, e che hanno la superiorità morale sui delinquenti, di essere e di rimanere onesti» (Ferri, 1886, p. 15).

Ferri sostiene che gli autori classici avessero prestato eccessiva attenzione agli individui che per la concomitanza di un sistema organico e psichico degenerato ed un ambiente sociale disfunzionale avessero commesso azioni criminose, ma poco interesse era stato riservato agli altri individui, che, pur vivendo nelle medesime condizioni, non avevano commesso alcun crimine.

Qui si inserisce la riflessione di Ferri sulla prevenzione sociale del delitto, argomento tralasciato dagli autori della scuola classica che si erano invece concentrati prevalentemente sull'aspetto repressivo, sulle caratteristiche della pena e sul perfezionamento dell'istituzione carceraria.

Ferri sottolinea un'ulteriore dimenticanza ovvero «che dietro al delinquente stanno le sue vittime e le loro famiglie e tutti gli onesti pure indirettamente offesi dal suo delitto» (Ferri, 1886, p. 20).

Messi in luce questi elementi principali, vediamo nello specifico la concezione del sistema penale in Ferri. Egli si concentra sulla figura del giurì che a suo dire dovrebbe essere abolita o ridimensionata, selezionando i giurati non sulla base del censo ma prendendo in considerazione professionalità e capacità di giudizio specifico. Propone, dunque, di nominare «giurì speciali nei reati d'indole tecnica (bancherotte, falsi, ecc.), coll'obbligo nei giurati di specificare le circostanze attenuanti» (Ferri, 1880, p. 53 - 54). Sarebbe inoltre opportuno: concedere meno libertà provvisoria ed amnistie, così da ridurre le occasioni di recidiva; abolire il maccanismo istruttorio; prediligere le citazioni dirette e direttissime; ridurre i ricorsi in cassazione per difetti di forma poco rilevanti; applicare rigorosamente il risarcimento civile (Ferri, 1880).

Sull'istituzione carceraria Ferri osserva che risulterebbe meno efficace nell'assolvere la sua funzione qualora «anziché essere un luogo di privazione, diviene un sito comodo di oziosità protetta e di criminosa compagnia» (Ferri, 1880, p. 54).

Gli autori della scuola classica si erano concentrati sul miglioramento del trattamento dei rei all'interno dell'istituto penitenziario, in un momento storico in cui le condizioni igienico-sanitarie erano particolarmente scarse e la tortura per estorcere confessioni una prassi quotidiana. Si vedano tra tutti i suggerimenti proposti da Bentham[1] per la realizzazione di un istituto carcerario che massimizzasse la visibilità delle celle.

A tal proposito Ferri suggerisce, piuttosto, una trasformazione delle carceri in «colonie agricole, con il lavoro ad aria libera e al sole, [come] forma migliore di segregazione dei condannati» (Il programma di lavoro della Commissione per la revisione della legislazione penale 1919, p. 2). La funzione rieducativa del carcere è fondamentale, soprattutto per i delinquenti occasionali che saranno chiamati a guadagnarsi da vivere lavorando

[1] Bentham J., *Panopticon ovvero la casa d'ispezione* (a cura di Foucault M. e Perrot M.), Marsilio, Venezia, 1983

quotidianamente all'interno del carcere, realizzando abiti o utensili consumati all'interno dell'istituto penitenziario medesimo o degli uffici pubblici (Ferri, 1886).

Per i delinquenti meno pericolosi si suggerisce la riabilitazione per il reinserimento all'interno del consorzio sociale (Il programma di lavoro della Commissione per la revisione della legislazione penale 1919).

Ferri riflette inoltre sulla forza lavoro del reo, sostenendo che lo Stato debba impedire al condannato di porre in essere altri reati ma non abbia «l'obbligo di mantenere gratis il delinquente, quasi per compensarlo di prestarsi, coattivamente, all'applicazione del castigo adeguato alla sua colpa» (Ferri, 1886, p. 35). All'interno dell'istituzione carceraria il reo dovrebbe guadagnarsi da vivere lavorando, come avrebbe dovuto fare in libertà, ciò «gioverà certo al miglioramento morale dei condannati, [ma] dovrà avere insomma per iscopo essenziale la riparazione dei danni, prima come pagamento del proprio mantenimento alla Stato, poi come risarcimento dei danni recati alle vittime del suo delitto» (Ferri, 1886, p. 37).

Nella riflessione di Ferri, dunque, lo scopo primario dell'istituzione carceraria è portare il reo a guadagnarsi da vivere lavorando e contemporaneamente a «riparare a quella grave fra le tre dimenticanze, che dissi proprie della scuola classica penitenziaria, per cui, una volta condannato il delinquente, si dimentica che egli lascia dietro di sé le vittime del suo delitto» (Ferri, 1886, p. 36).

La libertà condizionale, portata all'attenzione dagli studiosi della scuola classica, può essere utile per Ferri, qualora venga concessa non in forma gratuita ma ai soli rei distintisi per buona condotta che avessero con il proprio lavoro in carcere «risarcito le vittime o le loro famiglie, in tutto o in quella proporzione che il giudice e l'amministrazione carceraria potrebbero fissare secondo le condizioni delle vittime

stesse e le circostanze personali e reali del delinquente» (Ferri, 1886, p. 42).

Ferri propone delle misure alternative al carcere per gli autori di reati minori, i quali dovrebbero lavorare «in libertà, colla detrazione di una parte del salario a risarcimento dei danneggiati ed a pagamento di multe» (Ferri, 1886, p. 47).

In conclusione, così Ferri riassume il suo pensiero sulle pene e l'istituzione carceraria «siano miti le pene nei codici, ma l'applicazione ne sia severa ed inesorabile; e soprattutto coll'obbligo per tutti di lavorare e di pagarsi col lavoro, non i passatempi, ma anzitutto il proprio vitto nelle carceri» (Ferri, 1880, p. 55).

Ci si può riallacciare ai principi della scuola classica proposti da Beccaria, il quale sottolineava che la pena non doveva tormentare ed affliggere ma essere giusta, mantenendo la proporzione tra la natura del delitto e la pena «farà [così] un'impressione più efficace e più durevole sugli animi degli uomini e la meno tormentosa sul corpo del reo» (Beccaria, 1780, p. 55). Pene troppo severe avrebbero come conseguenza «la impunità stessa [che] nasce dall'atrocità dei supplicii» (Beccaria, 1780, p. 57).

Sull'importanza della severità della pena Ferri si inserisce sulla scia della scuola classica, laddove Beccaria, già aveva sottolineato l'importanza di una pena pronta e da realizzarsi nel minor tempo possibile così da essere giusta e utile, riducendo la distanza tra la commissione del reato e l'esecuzione della pena, poiché nel breve periodo l'associazione tra delitto e pena ad esso proporzionata rimane salda e funge, così, da deterrente (Beccaria, 1874).

Sul tema della pena Ferri sottolinea come pene pecuniarie proporzionali al reato commesso siano

meno violente e dirette delle pene fisiche ma abbiano un effetto più certo, esse sono «di facile ed economica attuazione, possono elevarsi in larga misura, compensare lo Stato delle ingenti spese per i servizi di pubblica sicurezza» (Ferri, 1880, p. 55).

È sul trattamento del reo che in parte Ferri si discosta dalla teorizzazione della scuola classica per via delle impostazioni di base differenti.

Gli esponenti della scuola classica, in maggioranza filosofi, giuristi, riformatori sociali, muovono da una concezione edonista dell'uomo, per cui l'individuo razionale, possessore di libero arbitrio cerca di massimizzare il piacere e minimizzare il dolore. Secondo un calcolo costi-benefici l'uomo decide di comportarsi in un modo piuttosto che in un altro ed è pertanto considerato moralmente responsabile delle proprie azioni.

Di contro, nella scuola positiva, composta per lo più da medici, scienziati, psichiatri, l'uomo è determinato nelle sue azioni da una serie di caratteristiche biologiche, psicologiche e sociali che ne comprimono gli spazi di libertà di scelta e responsabilità morale (Williams, McShane, 2002).

Questa differenza di base porta i primi a sostenere l'importanza dei diritti civili e dell'esecuzione della pena all'interno dell'istituto carcerario nel rispetto della dignità umana, mentre i secondi a ritenere che il sistema penale dovrebbe concretizzarsi nel trattamento scientifico-medico.

Ferri a tal proposito sottolinea che «per tutti i delinquenti considerati come esseri anormali; ma per i delinquenti che sono più pericolosi per le loro tendenze istintive o per malattie mentali o per alcolismo, ecc. i provvedimenti di difesa sociale saranno più efficaci, portando la loro segregazione ad un tempo indeterminato» (Il programma di lavoro della Commissione per la revisione della legislazione penale 1919, p. 2).

Come detto sopra, per i delinquenti meno pericolosi si potrà evitare la reclusione carceraria in favore di un risarcimento economico del danno alle vittime del reato commesso.

Lo stesso Ferri opera un confronto sulla funzione repressiva dello Stato, che nel pensiero degli autori classici ha sì un'utilità sociale ma basandosi sul concetto retributivo «deve consistere soprattutto nel far subire al delinquente un castigo proporzionato alla colpa morale. D'onde l'obbligo nello Stato di provvedere al mantenimento ed al miglioramento del delinquente, cui spetta il solo dovere di prestarsi all'applicazione del castigo, per la reintegrazione del diritto violato col suo delitto» (Ferri, 1886, p. 35).

Mentre per la scuola positiva «la punizione dei delinquenti […] altro non è che una funzione di difesa sociale contro i delinquenti» non imputati per la loro «colpabilità morale […] ma per la [loro] maggiore o minore temibilità […], che è una cosa positiva e positivamente determinabile» (Ferri, 1886, p. 35).

Infine, sulla pena capitale Ferri si trova in linea di pensiero con gli autori della scuola classica, allorché così si esprime «la pena di morte, o si restringe nel codice a pochissimi casi e si applica per eccezione, ed allora è un risibile spauracchio, che salva la società da qualche decina di assassini ed avvelenatori, ma non la difende dalle migliaia di omicidi e grassatori, e come tale è praticamente assurda e contrari alla serietà stessa delle leggi; o, se si deve mantenere, per essere logici converrebbe si applicasse inesorabilmente» (Ferri, 1880, p. 36).

Ferri mette in dubbio l'utilità della pena di morte poiché ritiene che «chi delinque o lo fa per passione, ed allora non pensa a nulla; o la fa con premeditazione, ed allora è mosso a delinquere non già da un ipotetico confronto tra l'estremo supplizio

e l'ergastolo a vita, ma dalla speranza di impunità» (Ferri, 1880, p. 35).

La scuola classica si basava su un'idea di società creata a seguito della sottoscrizione di un patto sociale in cui gli uomini, divenendo cittadini, cedevano una parte della propria libertà - e nello specifico la libertà di farsi giustizia da sé secondo la legge del taglione occhio per occhio, dente per dente - allo Stato per instaurare una convivenza civile che superasse la condizione di instabilità e paura perenne dettata dall'*homo homini lupus*, magistralmente teorizzata da Hobbes nel suo *Leviatano*[2].

Sul punto Beccaria, accolta questa idea di società, sosteneva che nessun essere umano avrebbe mai attribuito ad un suo simile il diritto di trucidarlo, inoltre «non è il terribile ma passeggiero spettacolo della morte di uno scellerato, ma il lungo e stentato esempio di un uomo privo di libertà, che, divenuto bestia di servigio, ricompensa colle sue fatiche quella società che ha offesa, che è il freno più forte contro i delitti» (Beccaria, 1780, p. 61 - 62).

Anche Lombroso inizialmente a favore divenne un avversario della pena di morte, allorché dopo lunghe riflessioni, prendendo in considerazione esclusivamente l'interesse sociale, essa «potrebbe essere utile soltanto se fosse applicata frequentemente, mentre sarebbe una barbarie se applicata raramente […]. Perciò quello che accade non è altro che uno spettacolo pubblico orribilmente dannoso» (Lombroso, 1906, p. 1).

Posti in luce alcuni elementi di continuità e discontinuità tra il pensiero di Ferri e degli esponenti della scuola classica, si può concludere questa breve rassegna con una metafora, che verrà ripresa successivamente da altri autori (si veda ¶ 4), proposta dallo studioso sulla figura del legislatore che nel conservare intatto il corpo sociale, «deve imitare il medico che vuol mantenere sano il corpo individuale: ricorrere il meno possibile alle misure violente della chirurgia, fidare in limitata misura nell'efficacia spesso problematica dei farmaci e affidare invece nei sicuri servigi dell'igiene» (Ferri, 1880, p. 56).

3. Tra saturazione criminosa e multifattorialità causale del delitto

«Come in un dato volume di acqua, ad una data temperatura, si scioglie una determinata quantità di sostanza chimica, non un atomo di più non uno di meno; così in un dato ambiente sociale, con date condizioni individuali e fisiche, si commette un determinato numero di reati, non uno di più non uno di meno» (Ferri, 1929, p. 345).

Con queste parole Ferri condensa la legge di saturazione criminosa che pone in luce gli elementi caratteristici del suo pensiero, una commistione tra ambiente sociale e caratteristiche individuali e fisiche che concorrono nel determinare il tasso di criminalità di una società.

Il tasso di criminalità non resta invariato nel tempo ma può subire dei cambiamenti «nella sociologia criminale, come nella chimica, alla normale e costante saturazione può sopravvenire una eccezionale e passeggiera soprasaturazione, per quella delinquenza riflessa o complementare, che pullula dietro la delinquenza principale, come nel campo biologico i parassiti si attaccano ad altri corpi e come nel campo economico dietro le grandi industrie germogliano tante industrie minute e secondarie» (Ferri, 1880, p. 30 - 31).

Si pone, così, in luce la multifattorialità causale del delitto, riprendendo ancora una volta le parole di Ferri «se come provano la biologia e la psicologia, l'uomo, sotto qualunque aspetto lo si consideri, è

[2] Hobbes T., *Leviatano*, (Saggio introduttivo Galli C., traduzione Micheli, G.) Bur Rizzoli, Milano, 2011

tanto il prodotto dell'atmosfera fisica e sociale, quanto del suo organismo, è facile vedere che il reato, come ogni altra azione umana, deve provenire da cause fisiche, sociali ed individuali» (Ferri, 1880, p. 33).

In questa affermazione si esemplificano le radici del pensiero di Ferri, legato alla scuola positiva - che accosta il delitto alla patologia, ben delineato da Lombroso - ed al contempo aperto alla società, o meglio, aperto alle future interpretazioni sociologiche della devianza in cui si prende in considerazione il contesto sociale come matrice del comportamento deviante-criminale.

È qui d'obbligo riferire l'equazione proposta da Lewin nella sua teoria del campo, che ben riassume questi aspetti, allorché egli afferma che il comportamento dell'uomo, e dunque, anche il comportamento criminale, possa essere interpretato come una funzione della persona e dell'ambiente C= f (P, A). Entrano dunque in gioco, tanto la dimensione personale del soggetto, nelle sue componenti piscologiche ed interiori, quanto lo stato della persona medesima in un arco spazio-temporale, situazionale definito (Balloni *et al*., 2019).

Non bisogna dimenticare che Ferri, seppur innovatore, appartiene, come detto in apertura di questo articolo, alla corrente positiva o bio-antropologica nello studio della criminalità; pertanto, egli presta comunque una certa attenzione ai fattori antropologici nella genesi del delitto. Quei fattori che si riconducono alle caratteristiche del delinquente quali anomalie del cranio e del cervello, si ricordi a tal proposito la fossetta occipitale mediana individuata da Lombroso durante l'autopsia del cranio del brigante Vilella e considerata prova principe dell'ereditarietà del crimine da ricondurre alla forma dell'atavismo. Rientrano in questa categoria le anomalie della sensibilità, dell'intelligenza e della modulazione dei sentimenti e le peculiarità personali (Ferri,1926).

Ricordando che il delitto è un «fenomeno bio-psico-sociale di origine complessa che assume modalità e caratteristiche differenti in rapporto alle persone e alle circostanze» (Bisi, 2004, p. 24), si tengono qui da parte i fattori bio-antropologici, per concentrarsi su altre due categorie ben analizzate da Ferri, che intrecciandosi interferiscono sull'andamento dei delitti.

Da un lato «cagioni lente e generali», al di fuori del campo d'azione del legislatore, relative all'ambiente naturale e sociale «quali il clima, le stagioni, le meteore, la razza, i costumi, le credenze religiose, la opinione pubblica, il carattere nazionale, la popolazione, la fertilità e disposizione del suolo, il generale assetto economico, l'età, il sesso, lo stato civile, la classe sociale, la professione degli individui» (Ferri, 1880, p. 4).

Dall'altro piccole cause relative all' «organismo legislativo, politico, amministrativo, economico, religioso, famigliare, educativo» sulle quali un intervento preventivo può effettivamente incidere, andando, in ultima istanza, a modificare il tasso di criminalità (Ferri, 1880, p. 5).

I cosiddetti fattori cosmotellurici, inerenti alle caratteristiche dell'ambiente fisico che circonda l'individuo fanno riferimento, come detto, alle condizioni climatiche, alla temperatura esterna, alla produzione agricola (Ferri, 1926). Sul clima Ferri conclude, attraverso lo studio delle statistiche criminali francesi dal 1826 al 1878 «che i reati contro le persone prevalgono nei climi meridionali e nei mesi caldi, mentre quelli contro le proprietà aumentano nei climi settentrionali e nella stagione invernale» (Ferri, 1880, p. 5 - 6).

Un altro aspetto peculiare, notato da Ferri e che verrà approfondito da alcuni studiosi del *design*

ambientale (si veda ¶ 4), concerne l'alternarsi del giorno e della notte «nelle notti lunghe e nei giorni oscuri dell'inverno sono favoriti i furti violenti, le violazioni di domicilio, la falsa moneta» (Ferri, 1880, p. 7).

Una certa attenzione viene prestata alla fertilità del suolo, utile alla produzione di prodotti alimentari, difatti, «dove e quando il suolo sia assai fertile, la facilità e sovrabbondanza di alimentazione aumenta i reati contro le persone, per la maggiore espansività di forza muscolare e nervosa degli individui, mentre scema i reati contro la proprietà» (Ferri, 1880, p. 11). Alla produzione agricola si lega questa ulteriore riflessione di Ferri «ma la più grande e più eloquente parte di tali cause mi pare stia nel triplicato consumo dell'acquavite, dell'assenzio, dell'alcool in genere, che porta con sé i due flagelli, egualmente terribili dei reati e dei suicidii» (Ferri, 1880, p. 25).

Ai fattori propri della terra si legano aspetti concernenti le differenze di etnia, pertanto, nei vari popoli si riscontrerà una criminalità specifica «mentre presso gli uni prevalgono i reati violenti, presso gli altri preponderano le frodi, e degli uni sarà proprio il vagabondaggio, quasi sconosciuto agli altri e via via» (Ferri, 1880, p. 8).

Ed ancora, le particolari condizioni sociali, in cui il soggetto si trova a vivere che comprendono ad esempio la densità di popolazione per cui i tassi di criminalità seguono «l'aumento continuo della popolazione per l'accresciuto numero di possibili delinquenti e di rapporti giuridici violabili col reato, e dovrà scemare quando una regione vada spopolandosi per emigrazioni, guerre, disastri, epidemie» (Ferri, 1880, p. 11).

Questa riflessione si intreccia alla diffusione delle risorse economiche «dove si ha minore ricchezza vi è minore agglomero di persone, e specialmente di quelle pericolose e recidive, che occorrono altrove[3] per meglio delinquere» (Ferri, 1880, p. 23 - 24) un aspetto peculiare, quello della relazione tra densità di popolazione e tasso di criminalità rivisto in ottica contemporanea da Angel con la funzione di *land use* (si veda ¶ 4).

Il cambiamento di usi e costumi ha influenzato la minore frequenza di alcuni reati di sangue, così come «il movimento economico, nella sua parte estranea ad ogni volontà legislativa, pel quale tanta preponderanza acquistarono le proprietà mobili sulle immobili, ha dovuto modificare la criminalità, all'infuori delle pene, nel senso di un aumento nei furti, frodi, appropriazioni indebite» (Ferri, 1880, p. 11).

In conclusione, riprendendo le parole di Ferri «ogni età, sesso, stato civile, professione e classe sociale ha, […], una propria criminalità specifica, determinata da peculiari condizioni fisiologiche, psichiche e sociologiche, che influiscono sull'andamento periodico di reati, all'infuori delle diverse pene minacciate ed eseguite» (Ferri, 1880, p. 11). Si mostra la necessità di sottolineare ancora una volta la lungimiranza di Ferri, in un momento storico in cui con facilità si sosteneva la validità dell'equazione povertà=criminalità, la forza della sua affermazione pone i prodromi per uno studio specifico sulla criminalità operata anche dagli appartenenti alle classi

agiate, i cosiddetti colletti bianchi, analizzati nell'opera di Edwin Sutherland[4].

Ferri non nega l'importanza della pena, ma ne attenua la potenza, essa esplica la sua maggior forza

[3] Il fenomeno del *displacement* dell'attività criminale non rientra nell'argomentazione di questo articolo ma corre l'obbligo di sottolineare l'attualità del tema meritevole di ulteriore riflessione, per una prima trattazione Felson M; Clarke R.V, *Opportunity Makes the Thief: Practical theory for crime prevention* Barry Webb Home Office Policing and Reducing Crime Unit, London, 1998

[4] Sutherland E.H, *White Collar Crime: The Uncut Version*, Yale University Press, New Haven, 1893

come minaccia psicologica all'azione individuale, potrà dunque opporsi o applicarsi con efficacia ai soli delinquenti occasionali, ma «non potrà evidentemente ostare ai fattori naturali e sociologici del crimine, quali sono il clima, le meteore, la fertilità del suolo, la razza, l'aumento della popolazione, i costumi, le crisi finanziare e politiche» (Ferri, 1880, p. 33).

È dunque in questa fase di analisi che Ferri introduce il concetto di sostitutivi penali (si veda ¶ 3), riprendendo l'idea di Minghetti relativa ai succedanei economici utilizzati per ovviare alla mancanza di prodotti principali nel soddisfacimento dei bisogni, nel campo criminale essi «debbono divenire i primi e principali organi di quella funzione sociale dell'ordine, a cui le pene servono ancora, ma in via secondaria» (Ferri, 1880, p. 41).

Non bisogna, tuttavia, cadere nell'errore interpretativo per cui la piena attuazione dei sostitutivi penali si finalizzi nell'eliminazione della criminalità dalla società, poiché «sempre vi ha un minimum di delinquenza, imposto dalla legge di saturazione criminosa ed inevitabile malgrado qualsiasi provvedimento» (Ferri, 1880, p. 57). Anche Durkheim aveva sottolineato questo aspetto, quando ne *Les règles de la méthode sociologique* affermava che il delitto anche se deplorevole è un fatto sociale normale. «È normale […] che si abbia una criminalità, purché questa raggiunga e non oltrepassi, per ogni tipo sociale, un certo livello» (Durkheim, 1981, p. 117).

Occorre, inoltre, rimarcare che Ferri nella sua dissertazione non sostiene la preminenza della prevenzione sulla repressione, si tratta di «due momenti di una sola ed identica funzione, compiuta da un medesimo organo sociale. Unico scopo la conservazione dell'ordine: unico problema lo stabilire i modi più efficaci ad ottenerla» (Ferri, 1880, p. 59).

La componente repressiva era stata ampiamente analizzata, nelle sue sfaccettature penali, deterrenti e del trattamento del reo dalla scuola classica, minore interessa aveva invece ottenuto l'aspetto precauzionale sul quale Ferri insiste, nel tentativo di riequilibrare la bilancia e così realizzare la prevenzione sociale il cui scopo è quello di impattare sulle «remote origini del delitto, per impedirne anche i più lontani germi, e con mezzi del tutto indiretti e basati sul libero gioco delle leggi psicologiche e sociologiche» (Ferri, 1880, p. 58).

Questo ragionamento porta Ferri ad affermare che sul tasso di criminalità di un popolo «influiscono […] prima e più assai del Codice penale, le leggi economiche, amministrative, politiche, civili e quelle di procedura penale. Però il ministero punitivo, se è soltanto la metà meno importante di una stessa funzione, la difesa dell'ordine, che deve poi esercitarsi nel contesto armonico delle altre funzioni sociali, ne resta pur sempre l'ultimo ed imprescindibile ausiliario» (Ferri, 1880, p. 60 - 61).

4. I sostitutivi penali

«La minuta esperienza della vita quotidiana nella famiglia, nella scuola, nelle associazioni come la storia delle vicende dei popoli ci ammaestrano, che per rendere meno perniciosa l'irruzione delle passioni più giova il prenderle di fianco, che non l'opporvisi di fronte» (Ferri, 1880, p. 40), così Ferri introduce la seconda parte del suo scritto sui sostitutivi penali, nella quale presenta una serie di suggerimenti che riducano le occasioni di commettere un crimine, alle quali «inutilmente si oppongono le pene, che hanno una presa così limitata sugli impulsi delittuosi» (Ferri, 1880, p. 41).

«La pena è confinata ad essere uno tra i tanti mezzi possibili per combattere il crimine» (Bisi, 2004, p. 89), compreso dunque che le pene da sole non riescono ad impedire la commissione di atti criminali occorre allora affiancare ad esse una serie di espedienti che possano in ordine diverso incidere sulla criminalità e sul mantenimento dell'ordine sociale.

Ferri si appella al legislatore, invitandolo a rendersi «padrone di una gran parte dei fattori del crimine e specialmente di quelli sociali, per influire così in modo indiretto, ma più sicuro, sull'andamento della criminalità» (Ferri, 1880, p. 41).

In campo economico Ferri suggerisce che il sistema si incentri sui principi del libero scambio, questo eviterebbe il susseguirsi di carestie ed il rialzo del prezzo dei beni alimentari.

La libertà di emigrazione viene vista come una «valvola di sicurezza, che libera il paese dagli elementi più torbidi» (Ferri, 1880, p. 42). Vengono ancora suggeriti: il pareggiamento delle tariffe doganali, un sistema tributario proporzionale ai guadagni, l'utilizzo della moneta metallica al posto di quella cartacea per evitarne la falsificazione, stipendi proporzionati per i dipendenti pubblici così da ridurre corruzione e concussione (Ferri, 1880).

È proprio in campo economico che Ferri inserisce alcuni suggerimenti che rientrano a pieno titolo nell'ambito della prevenzione situazionale, come si vedrà nel paragrafo successivo, allorché così si esprime «la fabbricazione di case e vie ampie, la estesa illuminazione notturna, la soppressione dei ghetti prevengono molto meglio delle guardie di P.S le grassazioni[5], i furti, il manutengolismo[6], le ricettazioni dolose» (Ferri, 1880, p. 45).

Ferri anticipa i concetti di visibilità, territorialità ed appartenenza esposti successivamente da Newman quando scrive che «molti furti sarebbero impediti se tutte le case in città si fabbricassero in modo che per entrare negli appartamenti si dovesse passare attraverso il camerino del portinaio» (Ferri, 1880, p. 45).

In campo politico suggerisce di garantire la libertà di opinione, che permetterebbe ai membri della società di sfogarsi in modo meno violento, andando ad evitare la commissione di reati politici, ribellioni, guerre civili. A tale scopo sarebbe inoltre utile una riforma elettorale «in armonia coi bisogni e le tendenze del paese» (Ferri, 1880, p. 46).

Il progresso della scienza ha portato alla scoperta di nuovi strumenti che possono essere utilizzati per la commissione di reati, ad esempio, le armi da fuoco e nuovi veleni, pur tuttavia, è lo stesso progresso scientifico a fornire prima o poi «un antidoto molto più efficace che non la più severa repressione» (Ferri, 1880, p. 47).

In ambito legislativo/amministrativo si apre alla possibilità di una legislazione testamentaria che scoraggi la commissione di crimini per ottenere un'eredità; una maggiore facilità del consenso paterno alle nozze ed il riconoscimento dei figli naturali inciderebbero sul numero di concubinati, infanticidi, procurati aborti (Ferri, 1880).

I reati di bancarotta fraudolenta verrebbero ridotti da un complesso di leggi commerciali che regolassero i rapporti tra falliti e creditori, la procedura dei fallimenti e i metodi di riabilitazione. Ancora, la proibizione del porto d'armi, gli orfanotrofi e le ruote per l'abbandono degli infanti presso gli istituti religiosi; «una religione indirizzata al benessere generale e non di una casta, [possono] essere ostacolo ai reati» (Ferri, 1880, p. 49).

[5] Nel linguaggio dell'epoca, si legga oggi "aggressione a mano armata"

[6] Nel linguaggio dell'epoca, si legga oggi "concorso in azioni illecite"

Nell'ordine familiare «l'ammissione del divorzio; il matrimonio degli ecclesiastici; […]; la facilitazione delle nozze a certe persone e la proibizione a certe altre, diminuirebbero le schiere dei delinquenti coll'impedire, per quanto possibile, la funesta eredità delle malattie e del delitto, ed eviterebbero le bigamie, gli adulterii, i concubinati, gli omicidii» (Ferri, 1880, p. 50), tornano qui alcuni elementi precipui della scuola bio-antropologica del crimine.

In campo educativo occorrerebbe affiancare ai classici insegnamenti anche degli approfondimenti morali «che provengono […] dalla potente scuola dell'esempio» (Ferri, 1880, p. 51) che dovrebbe coinvolgere ogni istituzione del governo, la stampa, le feste pubbliche, il teatro. Anche Beccaria aveva sottolineato l'importanza di perfezionare l'educazione nella prevenzione della criminalità, considerato il mezzo più sicuro ma al contempo più difficile da realizzare.

Proprio in riferimento al teatro, Ferri suggerisce di farvi accedere le classi popolari ad un prezzo limitato o gratuitamente, torna, alla mente quanto espresso secoli prima da Giovenale «[populus] duas tantum res anxius optat panem et circenses» (Giovenale, 1846, p. 106), il quale osservando lo scorrere della vita ai suoi tempi aveva notato che la classe al potere per assicurarsi il consenso politico offriva grano a prezzi calmierati ed organizzava grandi spettacoli pubblici: lotte tra gladiatori, corse dei carri, accesso alle terme.

Ferri insiste sull'importanza dell'educazione a partire dall'infanzia, con scuole che accolgano i bambini appartenenti alle classi più povere, ad esempio, in colonie agricole «anziché aspettare che il male sia fatto gigante per poi ricorrere al doppio ed inutile provvedimento della penalità» (Ferri, 1880, p. 52).

Questi esempi mostrano quanto nella prevenzione del crimine giochino un ruolo di prim'ordine i fattori sociali, «che dipendono dal diverso ordinamento legislativo, in ogni meato dell'organismo sociale» (Ferri, 1880, p. 52). In fase preventiva le leggi penali hanno minor influenza rispetto «alle leggi di ordine economico, politico, scientifico, amministrativo, famigliare, religioso, educativo» (Ferri, 1880, p. 53), è su questi fattori che il legislatore dovrebbe concentrarsi per incidere sul tasso di criminalità.

L'importanza riservata agli accorgimenti di natura sociale ha portato molti studiosi nel secolo successivo a concentrarsi sul *design* urbano, sulla possibilità, modificando lo spazio che ci circonda, di incidere sul tasso di criminalità, devianza ed inciviltà ed in ultima istanza sulla percezione di (in)sicurezza e sulla qualità della vita.

5. L'eredità dei sostitutivi penali nel *design* urbano

I suggerimenti offerti da Angel, Newman, Jacobs, Jeffery in campo architettonico, la teoria delle finestre rotte proposta da Wilson e Kelling per realizzare la prevenzione sociale del crimine coinvolgendo amministrazioni, cittadini, associazioni sono solo alcuni esempi che ci permettono di osservare la grande attualità del pensiero di Ferri.

È tra la fine del 1800 e i primi decenni del 1900, a seguito dei grandi cambiamenti che avevano investito la società del tempo, che gli studiosi, soprattutto, nel contesto americano iniziarono a prestare particolare attenzione alla città.

Con la nascita della scuola ecologica di Chicago vengono sistematizzati gli studi sulla città, considerata un laboratorio attivo, un caleidoscopio di aree naturali in cui i problemi sociali (alcolismo,

spaccio e consumo di droga, prostituzione, vagabondaggio) tendono a presentarsi maggiormente in una specifica area della città dove si riscontra un alto tasso di disgregazione sociale (Park *et al.*, 1925).

Chicago negli anni '20 presentava circa 35 gruppi nazionali differenti, difatti in seguito agli ingenti flussi migratori interni (dalle campagne alle città) ed esterni (prevalentemente da Europa e Sud Est Asiatico) si trovano a condividere lo stesso spazio persone con caratteristiche sociali, etniche, culturali, economiche differenti.

La città godeva di grande attrattiva per la possibilità di ottenere un lavoro in una delle industrie principali: trasformazione di materie prime in merce, allevamento e macellazione del bestiame, coltivazione dei prodotti agricoli, realizzazione della rete ferroviaria, di fornitura dell'acqua e dell'energia elettrica.

Park, Burgess e Mckenzie nel celebre testo *The City* affermano di volersi occupare dell'ecologia umana, ovvero dello studio delle relazioni spazio-temporalmente situate tra gli esseri umani «as affected by the selective, distributive, and accommodative forces of the environment. Human ecology is fundamentally interested in the effect of position, in both time and space, upon human institutions and human behavior» (Park, *et al.*, 1925, p. 63-64), è qui netto il parallelismo con l'intenzione espressa precedentemente da Ferri, che sottolineava l'importanza dell'ambiente nelle scelte degli individui.

La città è il prodotto della natura umana, un organismo in continuo mutamento, il cui sviluppo segue uno schema a cerchi concentrici dove si susseguono processi di invasione e successione delle aree adiacenti. Riprendendo brevemente lo schema, la città sembra essere organizzata a partire dal cerchio più interno in: distretto economico-commerciale; zona in transizione caratterizzata dalle industrie e da una massiccia presenza di immigrati di prima generazione, con potere economico basso che pertanto si trovano a vivere in scarse condizioni residenziali ed igieniche all'interno degli *slums*; terza zona abitata da immigrati di seconda generazione che hanno raggiunto uno *status* socio-economico più elevato; quarto cerchio è il più esclusivo, con la presenza di appartamenti e villette monofamiliari; ultima zona che circonda la città ed è frequentata dai lavoratori pendolari (Park, *et al.*, 1925).

Come detto in apertura di questa sezione, Shaw e Mckey hanno riscontrato una maggiore presenza dei problemi sociali nel secondo cerchio di questo schema, mentre l'incidenza della criminalità tende a diminuire spostandosi nei cerchi più esterni (Shaw, Mckay 1931).

Tra i principali esponenti delle teorie sociologiche sulla genesi del crimine, gli ecologi hanno osservato come «basso status economico, mescolanza di gruppi etnici diversi, alta mobilità dei residenti verso e fuori dal quartiere, nuclei familiari disagiati o spezzati» (Williams, McShane 2002, p. 60) incidano sulle relazioni primarie che risultano deboli, il vicinato poco coeso ed instabile e dunque il controllo sociale informale non riesce a svolgere pienamente la propria funzione. Dunque, la disorganizzazione sociale, spesso accostata al conflitto culturale[7] poteva spiegare i tassi di criminalità.

Una particolare attenzione era stata riservata alla struttura della città anche da parte di Harvey

[7] Processo sociale innescato dalle differenze di valori e culture presenti tra diversi gruppi di individui. Per un approfondimento sul tema specifico Wirth, L, *Culture conflicts in the immigrant family*, Sociology Department, University of Chicago, Chicago, 1925; Culture conflict and misconduct, «Social Forces», vol. 9, 1931, p. 484-492; Sellin, T, *Culture conflict and crime*, Social Science Research Council, Bulletin 41, New York, 1938

Zorbaugh, il quale studiando il quartiere di Lower East Side individua sei aree naturali[8]: Gold Coast la zona più esclusiva ed elegante della città; l'area degli appartamenti in affitto; Bohemia o Towertown il quartiere degli artisti; North Clark; Slum o Hoboemia dove "dimorano" i vagabondi; Little Sicily (Zorbaugh, 1929).

Ancora una volta si vuole sottolineare la lungimiranza di Enrico Ferri che nella famosa difesa dei contadini Mantovani del 1886, oltre a sottolineare che l'azione dei contadini fosse stata dettata dalle condizioni economiche e di vita nelle quali versavano, dando quindi spazio ai fattori sociali, aveva attraverso rilievi pratici e studi sulle caratteristiche geologiche ed agrarie del territorio, diviso l'area di riferimento in 3 zone. Incrociando i dati reperiti era riuscito ad osservare che l'agitazione contadina si era sviluppata prevalentemente nella terza area in cui le risaie dovevano produrre nutrimento per 140 persone, a fronte delle 80 della prima zona. Dunque si sottolinea l'importanza tanto del fattore ambientale che territoriale nello sviluppo di azioni devianti o criminali (Balloni *et al*., 2019).

Dagli studi degli ecologi di Chicago, che perdurarono per tutti gli anni '40, si svilupparono due direttive teoriche principali: l'etichettamento[9] e il controllo sociale / anomia[10].

Dalla prospettiva inaugurata dagli ecologi di Chicago tra gli anni '60 e '70 si sviluppò una corrente di studi denominata *design* ambientale la cui aspirazione principale era prevenire la criminalità o ridurne il tasso, modificando l'ambiente circostante l'individuo.

Su questi temi aveva già riflettuto Ferri quando sul finire del 1800 sottolineava che ad un luogo con una modesta presenza di persone, un potenziale criminale avrebbe preferito un luogo con una concentrazione di persone più alta per porre in essere l'atto criminale. Nel 1968 Schlomo Angel riflettendo ancora su questo aspetto afferma che il potenziale criminale, in qualità di soggetto razionale attraverso un calcolo costi-benefici, nel quale va a soppesare il potenziale guadagno, le eventuali perdite, la possibilità di essere scoperto e reso alle forze dell'ordine, deciderà se e dove compiere l'azione criminale.

Angel, notando la relazione tra attività criminale e livelli di uso della strada, ha proposto la funzione di *land use* per cui ad un basso livello di utilizzo della strada ovvero ad un basso livello di densità di popolazione nei luoghi pubblici, corrisponderà un basso livello di crimini. Il territorio risulta, infatti, poco attrattivo per il potenziale criminale, i potenziali rischi sono maggiori del potenziale guadagno; il soggetto sarà quindi poco incentivato a porre in essere l'azione criminale in quel luogo, in quel determinato momento (Angel, 1968).

All'aumentare del livello di utilizzo della strada, aumenteranno le potenziali vittime e di conseguenza il possibile guadagno per cui il tasso di criminalità tenderà a salire, il criminale potrà nascondersi tra la folla, far perdere le proprie tracce ed evitare di finire tra le maglie del controllo sociale formale. Superata la *critical intensity zone*, il punto in cui si registra il maggior numero di crimini, la curva tenderà ad abbassarsi, poiché le persone che frequentano la

[8] Dove per area naturale Zorbaugh intende un quartiere o un distretto urbano emergente dall'intersezione di confini geografici e caratteristiche culturali della popolazione (Zorbaugh, The Natural Areas of the City 1926). A differenza di Park, Burgess e Mckenzie che la definiscono come una porzione di spazio interna alla città caratterizzata da "an orderly and typical grouping of its population and institutions" (Park *et al*. 1925, 1)

[9] Per approfondire Becker, H.S., *Outsiders: Studies in the sociology of deviance*, Free Press, New York, 1963

[10] Per un approccio iniziale Durkheim, É., *Les ègles de la méthode sociologique*, Alcan, Paris, 1895; Merton, R. K. *Anomie, anomia and social interactions: Contexts of deviant behavior*, in M.B. Clinard (a cura di) Anomie and deviant behavior, Free Press, New York pp. 213-242, 1964

zona impediranno al soggetto di portare a termine l'azione criminosa con successo (Angel, 1968).

Il concetto di prevenzione sociale avanzato da Ferri viene qui rivisto nell'ottica del *design* ambientale, «the physical environment can exert a direct influence on crime settings» (Angel, 1968, p. 15) per cui Angel propone la creazione di spazi multiuso, in cui gli utenti possano recarsi in diverse fasce orarie ed assicurare così il controllo sociale informale. Si ritorna sull'importanza delle relazioni umane, già messa in luce dagli ecologi di Chicago come fattore utile a combattere la disgregazione sociale.

Negli stessi anni veniva ad affermarsi l'ampia riflessione offerta da Oscar Newman, architetto statunitense autore di progetti di edilizia pubblica, il cui obiettivo primario era riqualificare aree urbane degradate. «The urban environment is possibly the most cogent ally the criminal has in his victimisation of society» (Newman, 1973a, p. 2) pertanto Newman cerca di intervenire sugli spazi urbani in modo da renderli controllabili, piuttosto che dagli agenti di polizia, dagli stessi cittadini che condividono lo spazio di vita quotidiana (Newman, 1973a).

Affinché i residenti diventino operatori di prevenzione sociale è necessario estendere la loro area di influenza ed ampliare le opportunità di porre in essere la sorveglianza naturale attraverso l'utilizzo di barriere reali e simboliche, andando a realizzare il cosiddetto spazio difendibile (Newman, 1973a). Per far ciò è necessario progettare le aree urbane in modo da permettere ai residenti di controllare le zone circostanti, implementando barriere fisiche (cancelli, siepi, mura, edifici) o barriere simboliche (varchi, illuminazione, diversificazione strutturale) che segnalino il passaggio tra spazi pubblici, semi-privati e privati.

Il senso di appartenenza dei residenti è fondamentale «for preserving a safe and well maintained living environment» (Newman, 1973b, p. 4).

L'illuminazione, già individuata da Ferri come deterrente alla commissione di crimini, è vista da Newman come elemento fondamentale per segnalare gli ingressi al quartiere o agli edifici.

Un altro scopo da perseguire è «restructure the physical layout of communities to allow residents to control the areas around their homes» (Newman,1996, p. 9). Newman progetta piccoli quartieri costituiti da villette a schiera, con *layout* e materiali simili per dare senso di continuità tra gli spazi, rendere riconoscibili i luoghi e favorire la creazione di legami umani.

Si dovrebbero evitare intercapedini o spazi interstiziali tra gli edifici per ridurre le vie di fuga od occultamento per i potenziali criminali e progettare edifici, scale, corridoi, ascensori ben visibili (Geason,Wilson, 1989).

Un ulteriore contributo è stato offerto negli stessi anni da Jane Jacobs, la quale inizia ad interrogarsi sulle vivibilità delle città, sostenendo che una strada utilizzata in modo corretto sia percepita come sicura, di contro una strada deserta e poco frequentata venga percepita come insicura (Jacobs, 1961).

Per favorire il controllo sociale informale e dunque la prevenzione della criminalità sarebbe opportuno incentivare la diversità di usi all'interno di una zona, progettando quartieri con edifici vecchi e nuovi. I vari edifici avendo un costo di vendita o affitto diverso potranno così ospitare residenti o esercizi commerciali con potere economico differenti.

Sarebbe altrettanto importante progettare edifici con ampie finestre che si affaccino direttamente sulle strade, i famosi *eyes upon the street*, così da

permettere ai residenti di osservare ciò che accade lungo le strade del quartiere, fungendo da deterrente per i potenziali criminali che potranno essere visti nell'atto di commettere un illecito.

La diversità si esprime anche nel creare le condizioni affinché persone con caratteristiche sociali, economiche e culturali differenti possano condividere gli spazi, creare legami umani, vivere il quartiere ad orari differenti e così realizzare il controllo sociale informale diffuso: «on successful city streets, people must appear at different times» (Jacobs, 1961, p. 152).

Un altro elemento fondamentale risulta essere la costruzione di parchi di quartiere, incastonati all'interno dello spazio urbano, circondati da edifici, con ricchezza e diversità di flora come luoghi di aggregazione intergenerazionale. Lo sviluppo di legami umani è ritenuto un fattore fondamentale per incrementare la percezione di sicurezza, andando a scardinare la paura dell'alter sconosciuto.

Il tutto riporta a quella funzione di *land use* proposta da Angel ed anticipata in modo lungimirante da Ferri, per cui la concentrazione di individui nella zona fungerà da deterrente alla commissione di atti criminali.

Jacobs incentiva gli amministratori politici a coinvolgere i cittadini nei processi decisionali che hanno ricadute sul quartiere di riferimento e dunque sulle abitudini quotidiane, sui modi di vivere, sugli usi dei luoghi. In tal senso la Jacobs ha anticipato quei processi di consultazione dei cittadini oggi previsti a livello europeo per tutte quelle decisioni che possono in qualche modo incidere sulla qualità della vita urbana.

Nel 1971, dopo aver studiato la letteratura prodotta sulla relazione tra spazio urbano e criminalità, Ray Jeffery conia la locuzione *Crime Prevention Through Environmental Design*, (da ora CPTED) per introdurre la prevenzione situazionale.

Lo studioso muove dall'assunto per cui alla scelta di delinquere da parte del soggetto contribuiscano fattori ambientali, personali e psicologici. L'ambiente che circonda il soggetto «plays a critical role in behavior, including criminal behavior» (Jeffery 1977, p. 41) poiché stimola nel cervello lo sviluppo di sensazioni piacevoli o dolorose (Jeffery, Zahm, 1993).

Jeffery rinforza gli accorgimenti proposti dagli altri autori allorché propone di: incrementare la sorveglianza naturale degli accessi utilizzando recinzioni ed illuminazione pubblica; estendere la territorialità, quale senso di appartenenza ai luoghi dei residenti; rendere i confini degli spazi visibili utilizzando recinti, siepi, pavimentazione stradale, muretti come già sottolineato da Newman; progettare *toilette* e lavanderie comuni all'entrata del condominio o in aree con elevato passaggio pedonale per incrementare il controllo informale; costruire aree ricreative che favoriscano lo sviluppo di relazioni intergenerazionali; ampie finestre, come sostenuto dalla Jacobs, anche per i negozi così da poter controllare lo spazio antistante (Task Force, 1995).

Infine, Wilson e Kelling con la teoria delle finestre rotte sottolineano ancora una volta l'importanza di misure alternative alle sanzioni penali per prevenire la criminalità, insistendo sul mantenere le comunità intatte, senza finestre rotte per inviare un chiaro segnale di interesse, cura ed attenzione verso il quartiere al potenziale criminale, che sarà così scoraggiato dal porre in essere l'azione illecita proprio in quel luogo (Wilson, Kelling, 1982).

Secondo gli studiosi i cittadini percepiscono inciviltà e crimine come estremi dello stesso *continuum*, per cui il disordine può crescere esponenzialmente fino

a tramutarsi in criminalità, rendendo un quartiere invivibile.

Il disordine può esprimersi fisicamente con edifici abbandonati o in cattivo stato, graffiti non autorizzati, arredo urbano degradato o socialmente attraverso spaccio di sostanze stupefacenti, prostituzione, presenza di vagabondi, conflitti culturali.

Risulta dunque fondamentale l'intervento dei cittadini che dovranno prendersi cura degli spazi comuni, attuare il controllo di vicinato e se necessario organizzare ronde di pattugliamento appiedato.

Ritorna ancora una similitudine con il mondo medico, come anticipato da Ferri, «just as physicians now recognize the importance of fostering health rather than simply treating illness, so the police -- and the rest of us -- ought to recognize the importance of maintaining, intact, communities without broken windows» (Wilson, Kelling, 1982, p. 38).

6. Applicazioni pratiche

Negli anni '30 del '900 Shaw e McKay fermamente convinti che si potesse ridurre la delinquenza, soprattutto quella giovanile, incrementando il controllo sociale avviarono il *Chicago Area Project* (da ora Cap).

Il progetto si basa sulla collaborazione tra attori sociali formali e informali presenti sul territorio quali amministratori politici, associazioni di volontariato, istituzioni scolastiche.

All'interno di ogni quartiere occorre individuare *leader* significativi che siano in grado di osservare le criticità e mappare le risorse per risolvere le problematiche locali grazie alla collaborazione tra giovani e adulti.

Negli anni si sono susseguiti diversi progetti specifici per: incrementare la relazione genitori-figli così da prevenire la delinquenza giovanile includendo ragazzi problematici ed ex detenuti; promuovere l'integrazione fra comunità coinvolgendo afroamericani ed ispanici; in collaborazione con la Corte di Giustizia sono stati coinvolti giovani con precedenti penali nello svolgimento di attività regolari così da evitare il contatto con altri criminali[11] e ridurre il tasso di recidiva; incentivare la partecipazione ad attività sportive e di prevenzione sanitaria anche grazie all'aiuto di *tutor* scolastici ed universitari; cercare di eliminare gli ostacoli che rendono difficile l'accesso ai mezzi legittimi[12] per l'indipendenza economica ai soggetti con basso reddito; imparare a gestire il denaro in modo consapevole; informare i giovani sui rischi derivanti dall'utilizzo di sostanze stupefacenti, dell'alcol e del tabacco, della sessualità non protetta, educando a risolvere le conflittualità senza ricorrere alla violenza o cadere in preda alla rabbia (Cap).

Gli studi di Jeffery portarono la Law Enforcement Assistance Administration a sviluppare 3 progetti basati sui principi della CPTED. Nel primo caso si è cercato di incrementare la sorveglianza naturale e ridurre la dispersione scolastica per prevenire la criminalità scolastica (Crime Prevention Through Environmental Design: The School Demonstration in Broward County, Florida 1980).

Il secondo progetto ha applicato alcuni elementi della prevenzione situazionale lavorando sull'illuminazione pubblica e l'arredo urbano per

[11] Si può qui notare un parallelismo con la teoria dell'associazione differenziale proposta da Sutherland, si veda a tal proposito Sutherland *et al*. *Principles of Criminology: Eleventh Edition,* General Hall, New York, 1992

[12] Sul rapporto mete / mezzi si veda Merton, R. K. *Anomie, anomia and social interactions: Contexts of deviant behavior*, in M.B. Clinard (a cura di) Anomie and deviant behavior, Free Press, New York, pp. 213-242, 1964

migliorare il controllo sociale informale (Crime Prevention Through Environmental Design: The Commercial Demonstration in Portland, Oregon, 1980).

Nell'ultima esperienza sono state introdotte modifiche alla viabilità stradale e sono stati creati gruppi anti-crimine per pattugliare le vie del quartiere ed instaurare relazioni collaborative con gli operatori delle forze dell'ordine (Reducing Residential Crime and Fear: The Hartford Neighborhood Crime Prevention Program, 1979).

Negli anni '70 nascono i gruppi *Guardian Angels*, composti da volontari che organizzano ronde di controllo appiedato del territorio locale. Il nucleo iniziale guidato da Curtis Sliwa era composto da 13 volontari che cercavano di scardinare la percezione di insicurezza frequentando la metropolitana, fungendo con la loro presenza da deterrente per i potenziali criminali.

Oggi i volontari organizzano corsi di autodifesa, aiutano i giovani a proseguire gli studi formandoli sugli effetti negativi dell'assunzione di alcol e droghe, su come gestire i conflitti in modo ottimale sostenendoli nel riconoscere i propri talenti ed incentivandoli a prendersi cura della comunità (Guardian Angels, Safety Patrol).

La riflessione sull'importanza dei fattori sociali e sulla relativa prevenzione sociale inaugurata da Ferri ed approfondita negli anni successivi dagli ecologi di Chicago e dagli esponenti del *design* urbano si è concretizzata attraverso gli esempi progettuali sopra evidenziati fino ad arrivare ai giorni nostri attraverso l'attuazione di tecniche di sicurezza urbana contemporanea quali: il *community policing*, che rivede il rapporto agenti del controllo sociale formale-cittadini nell'ottica di una collaborazione proficua basata su rapporti di fiducia reciproca; il *neighborhood watch*, in cui i cittadini attraverso un controllo appiedato del territorio incrementano il senso di territorialità ed appartenenza; le *social street*, che cercano di riscoprire la socialità spesso andata perduta nei grandi agglomerati urbani attraverso attività comuni da svolgere lungo la via di residenza, resi visibili attraverso i *social network*.

In Gran Bretagna i principi del *community policing* sono parte integrante dell'organizzazione delle squadre di polizia londinese in sezioni specifiche (residenziale, commerciale, stradale) il cui obiettivo primario è prevenire e ridurre la criminalità attraverso un approccio integrato con il territorio e i cittadini (City of London Police).

Anche la Spagna si è contraddistinta avviando un programma di progressivo avvicinamento delle forze di polizia ai cittadini, a partire dal 2014 sono stati infatti istituiti canali preferenziali per rendere più agevole ed immediata la comunicazione. Diversi sono i progetti ideati per migliorare la prevenzione sociale, tra i quali si sottolineano le campagne di sensibilizzazione per la sicurezza dei minori e degli anziani incentrati su: diritti/doveri; rischi correlati all'uso di alcol e sostanze stupefacenti; meccanismi di difesa per evitare maltrattamenti o frodi (Cuerpo Nacional de Policìa).

Un'ulteriore iniziativa denominata *polìcia de barrio* porta gli agenti di polizia a frequentare quotidianamente il quartiere presso il quale prestano servizio, con lo scopo di offrire un servizio vicino al cittadino, aumentando il senso di soddisfazione e tranquillità dei residenti, fungendo da deterrente alla commissione di crimini, offrendo informazioni utili ed aiuto immediato in caso di necessità (La Funciòn Preventiva de la Policìa: La Policìa de Barrio 2010).

Il controllo di vicinato in Europa si è affermato in Francia grazie alla *Participation Citoyenne* il cui obiettivo principale è incrementare il senso di appartenenza e territorialità dei cittadini, i quali

rispettando diritti e libertà individuali possono vigilare sul quartiere ed informare tempestivamente le forze dell'ordine qualora si rendesse necessario un loro intervento (Participation Citoyenne: Devenir Actuer de sa Sécurité 2011).

Nell'ambito dell'iniziativa *Voisins Vigilants et Solidaires* diffusasi in Francia e Belgio, i cittadini utilizzano i *social network* per creare legami di vicinato, organizzare riunioni ed eventi di quartiere o informare sulla presenza di soggetti sospetti (Voisins Vigilants et Solidaires 2018).

In Gran Bretagna è nata un'organizzazione nazionale del controllo di vicinato con l'obiettivo di creare comunità coese che possano così incidere sulla percezione di sicurezza attraverso la realizzazione di diversi programmi i cui obiettivi principali sono: accettare e rispettare le diversità; includere e rendere partecipi alle attività locali i soggetti emarginati; suggerire i comportamenti da attuare sul *web* per evitare di essere vittime di reati informatici (Neighbourhood Watch).

Il *Neighborhood Watch* è giunto anche in Italia, dove sotto la guida dell'Associazione Controllo di Vicinato i gruppi di volontari organizzano un controllo appiedato del territorio per fungere da deterrente contro la commissione di atti vandalici (Associazione Controllo del Vicinato).

Le strade sociali godono di una buona diffusione in tutto il mondo, basandosi sull'utilizzo dei *social network,* cercano di veicolare i principi della socialità e del mutuo-aiuto mettendo in contatto residenti e professionisti dello stesso quartiere. Organizzare eventi culturali da svolgere lungo le vie della zona di riferimento risulta essere una buona occasione per creare legami di vicinato andando a scardinare l'anonimato che spesso dilaga in città, con ricadute positive in termini di socialità, territorialità, cura del quartiere stesso, andando così ad impattare sulla percezione di insicurezza (Social Street: dal Virtuale al Reale al Virtuoso).

Queste esperienze mostrano l'attenzione oggi riservata alle variabili sociali, nel tentativo di riscrivere il rapporto di forza tra repressione e prevenzione prestando attenzione al ruolo attivo che i cittadini possono ricoprire nella lotta all'insicurezza che dilaga in città.

Una delle frontiere più recenti è rappresentata dai progetti basati sulla rigenerazione urbana come occasione per rivedere gli assetti architettonici e sociali di un luogo attraverso una ristrutturazione di spazi, usi, legami, significati ad essi associati.

Il concetto di rigenerazione urbana si è evoluto nel corso del tempo, inizialmente il termine veniva associato, soprattutto negli Stati Uniti degli anni '60, alla demolizione di interi quartieri per sostituirli con nuovi edifici residenziali, il cui scopo ultimo era aumentare l'appetibilità economica della zona, attraendo ingenti capitali e nuovi investitori. Questo processo comportava l'allontanamento dei residenti originali e la loro sostituzione con soggetti di status socio-economico più alto[13], in grado di fronteggiare il nuovo costo del suolo (Vicari Haddock, Moulaert, 2009).

È nel corso del decennio successivo che in Europa si inizia a ragionare in termini di rigenerazione urbana per rispondere alla crisi derivante dalla commistione di recessione economica e cambiamenti industriali. In questo dibattito si inserisce anche la Commissione Europea che dagli anni '90 propone programmi e documenti di pianificazione territoriale[14].

[13] Si verifica il fenomeno della *gentrification*, Glass, R. *London: Aspects of Change*, Centre For Urban Studies, London, 1964

[14] Si vedano a titolo esemplificativo *Green Paper on the Urban Environment* 1990; *European Spatial Development Perspective* 1999.

Il fermento intellettuale sulla possibilità di rigenerare la città andando ad incidere sulla «qualità della vita urbana e [sulle] relazioni sociali che definiscono la città in quanto entità fisica e sociale coesa» (Vicari Haddock, Moulaert, 2009, p. 7) ha portato molti autori a caldeggiare l'utilizzo di un approccio multidimensionale e multisettoriale che vada ad integrare gli elementi fondamentali di vitalità di un territorio, ovvero diversi aspetti afferenti la sfera: sociale, economica e culturale.

Non basterebbe dunque concentrarsi esclusivamente sulla rigenerazione fisica intervenendo sui vuoti urbani (periferie, ex aree industriali ormai dimesse) cercando di attrarre risorse economiche esterne ed incentivando la partecipazione delle risorse interne.

Non gioverebbe neanche la sola attenzione alla rigenerazione economica incentrata da un lato sulle reti ferroviaria ed aeromobile, dall'altro sui centri di ricerca per incentivare l'ammodernamento tecnologico.

Alla stessa stregua non bisognerebbe basarsi esclusivamente sull'approccio che predilige il solo aspetto culturale, che si concentra «sulla promozione della produzione e del consumo culturale» (Vicari Haddock, Moulaert, 2009, p. 29). Rientrano in questa categoria interventi di rigenerazione di un'area realizzando «un nuovo museo in un edificio industriale dismesso (ad esempio la New Tate Gallery di Londra e il Baltic/Sage, museo auditorio di Newcastle) o la costruzione *ex novo* di un tempio per la cultura (come l'Opera House di Sidney o lo stesso museo Guggennheim di Bilbao) o di una struttura per il tempo libero (ad esempio il nuovo Acquario di Genova)» (Vicari Haddock, Moulaert, 2009, p. 32). L'approccio culturale può essere sostenuto anche attirando produttori di cultura ed accostandoli alle comunità artistiche locali.

Ancora una volta torna alla mente la riflessione di Ferri sull'importanza dell'ambiente sociale e delle condizioni di vita in cui il soggetto versa come fattori sui quali lavorare per ridurre la criminalità.

Si pone, dunque, in luce l'importanza di realizzare iniziative integrate che riescano ad incrementare l'inclusione sociale coinvolgendo cittadini ed istituzioni qui intese in senso ampio dalle amministrazioni locali, al complesso di norme sociali e culturali che possono incidere sulle scelte dei soggetti.

Parlare di integrazione nell'ambito delle politiche di rigenerazione urbana vuol dire considerare i diversi settori che afferiscono la vita dei soggetti e coinvolgere attivamente i destinatari finali dei progetti stessi.

L'Unione Europea a partire dalla seconda metà degli anni '80 ha sostenuto lo sviluppo di programmi integrati che coinvolgessero, appunto, i cittadini dal momento che la partecipazione locale aiuterebbe i soggetti a: comprendere le dinamiche che portano all'esclusione sociale e dunque la possibilità di intervenire per prevenirla; creare un clima cooperativo basato su legami fiduciari; individuare risorse territoriali utili; innovare le politiche (Vicari Haddock, Moulaert, 2009).

Ancora una volta emergono temi familiari, alcuni di essi già trattati nei paragrafi precedenti, dall'importanza del tessuto locale, allo sviluppo di relazioni umane come fattori del cambiamento sociale e del controllo informale.

Cercando di ancorare ulteriormente la riflessione teorica alla realtà si possono osservare le varie iniziative realizzate in tutta Europa nell'ambito del progetto Urbact che dal 2002 si pone l'obiettivo di guidare il cambiamento «by enabling the

cooperation and idea exchange amongst cities within thematic networks, by building the skills of local stakeholders in the design and implementation of integrated and participatory policies, and by sharing knowledge and good city practices» (Urbact).

I cittadini rappresentano una risorsa per affrontare sfide globali e cogliere importanti opportunità di crescita e confronto con altre realtà europee, Urbact promuove l'integrazione di azioni verticali ed orizzontali così da coinvolgere tutte le componenti della società.

Sul nostro territorio nazionale sono coinvolte 33 città nella realizzazione di diversi progetti relativi ad una o più aree afferenti i *core principles* di Urbact. Tra i vari progetti si ricordano: Rumourless Cities con l'obiettivo di prevenire la criminalità rafforzando la coesione sociale; Com.Unity.Lab per incrementare lo sviluppo locale; UrbInclusion per combattere la povertà in aeree urbane prive di risorse; UrbSecuirty per pianificare città più sicure; ActiveCitizens per promuovere la partecipazione in piccole e medie città (Urbact).

Come già accennato sopra, l'Unione Europea è da anni attiva nell'ambito della riduzione della criminalità urbana, spronando le amministrazioni nazionali ad implementare programmi multisettoriali che coinvolgano attivamente professionisti del settore, operatori delle forze dell'ordine e cittadini. È questo lo spirito che ha portato alla realizzazione della norma UNI CEN/TR 14383-2:2010 il cui obiettivo principale è diffondere una metodologia condivisa nell'ambito della sicurezza urbana prestando attenzione alla pianificazione urbanistica.

In tal senso vengono individuati i fattori che rendono un luogo insicuro: caratteristiche della zona legate al degrado sociale; elementi di degrado fisico; mancanza di sorveglianza e visibilità. Occorre inoltre mappare le risorse presenti sul territorio che possano essere coinvolte nella riduzione dei tassi di criminalità e percezione di insicurezza quali: amministratori e legislatori; professionisti della sicurezza; gruppi di quartiere; esperti della progettazione urbana; imprenditori; operatori delle forze dell'ordine; aziende che forniscono servizi di sicurezza; cittadini (Norma UNI CEN/TR 14383-2:2010).

La norma propone, inoltre, diverse strategie d'azione suddivise in 3 direttrici principali: progettazione urbanistica; *urban design*; gestione degli interventi (Norma UNI CEN/TR 14383-2:2010).

Alcuni paesi europei come Francia e Regno Unito hanno inserito la norma all'interno della legislazione nazionale, impegnandosi così ad applicarla operativamente.

In conclusione, sembra opportuno citare l'esperienza del Forum Europeo per la Sicurezza Urbana (FESU), fondato nel 1987, il quale raggruppa circa 250 città[15] su tutto il territorio europeo con l'obiettivo di promuovere lo scambio di esperienze tra autorità locali e regionali combinando tre elementi principali: prevenzione, sanzioni e coesione sociale attraverso *policies* co-costruite (European Forum for Urban Security).

7. Conclusione

Gli spunti di riflessione emersi sono molteplici ed estremamente attuali, mentre sulle prime esperienze possono già essere rintracciati studi specifici, le nuove sfide sono rappresentate proprio dai processi co-partecipati, durante i quali, attraverso l'aiuto di specialisti della facilitazione, gli amministratori e i

[15] Per una trattazione del contesto nazionale, si faccia riferimento al Forum Italiano per la Sicurezza Urbana, consultabile al seguente link https://www.fisu.it

tecnici dialogano con i cittadini. Sarebbe interessante indagare tanto i rapporti instauratisi tra i soggetti coinvolti per capire l'impatto in termini di percezione di (in)sicurezza e fruibilità dei luoghi, quanto le relazioni tra le città parte del *network* Urbact/FESU in un'ottica comparativa.

Si è tentato di mostrare, seppur brevemente, la lungimiranza del pensiero di Ferri individuando un parallelismo tra i suggerimenti da questi presentati e la loro evoluzione nel filone del *design* urbano, con l'intento di sottolineare l'importanza e l'attualità della prevenzione sociale del crimine.

Dalle prime esperienze di sicurezza urbana partecipata, passando per le tecniche contemporanee cui si è solo accennato, giungendo ai progetti europei si è voluta mostrare la crescente importanza riservata ai fattori sociali che possono manifestarsi come elementi incentivanti o disincentivanti dell'azione criminosa.

Dai suggerimenti architettonici da tenere a mente durante le fasi di progettazione della città, alle possibili forme della rigenerazione urbana il ruolo fondamentale della cittadinanza attiva e partecipe sembra oggi essere imprescindibile.

Se nella lotta alla criminalità le pene mantengono ancora oggi loro funzione originaria, all'anonimato che dilaga e rende insicuri nel frequentare i luoghi e nel rapportarsi all'*alter* sconosciuto occorre sempre più contrapporre nuove forme di socialità e di partecipazione attiva.

Il breve *excursus* proposto ha cercato di porre in luce alcuni aspetti del pensiero di Enrico Ferri ritenuti innovati per il contesto sociale ed intellettuale nel quale si trovò ad operare e che negli anni successivi vennero ripresi ed ampliati da studiosi con *background* differenti.

Si è dunque presentata un'occasione per riflettere sullo spirito dei sostitutivi penali e sulla prevenzione sociale che muta e si adatta alle sfide globali che le città contemporanee e i loro abitanti si trovano ad affrontare giorno per giorno.

Per concludere con le parole del Ferri «non nego che le pene siano gli argini del delitto […] [tuttavia] varrà meglio a difendere l'ordine sociale il rincorrere ai sostitutivi penali, fondati alla loro volta sulle leggi naturali della psicologia e della sociologia, e come tali ben più efficaci degli arsenali punitivi» (Ferri, 1880, p. 60).

Bibliografia

1. Angel S., *Discouraging Crime Through City Planning*, Centre for Planning and Development Research of California, Berkeley, 1968.
2. Balloni A., Bisi R., Sette R., *Criminologia e psicopatologia forens,* Wolters Kluwer, Milano, 2019.
3. Barbero Avanzini B., *Devianza e controllo sociale.* Franco Angeli Editore, Milano, 2002.
4. Beccaria C., *Dei delitti e delle pene.* Didot, Parigi, 1780.
5. Beccaria C., Bonesana, *Dei delitti e delle pene e ricerche intorno alla natura dello stile*, Giovanni Silvestri, Milano, 1834.
6. Bisi R., *Enrico Ferri e gli studi sulla criminalità,* Franco Angeli Editore, Milano, 2004.
7. *Crime Prevention Through Environmental Design: The Commercial Demonstration in Portland, Oregon,* National Institute of Law Enforcement and Criminal Justice, 1980.
8. *Crime Prevention Through Environmental Design: The School Demonstration in Broward County, Florida,* National Institute of Law Enforcement and Criminal Justice,1980.
9. *Design Out Crime: Crime Prevention Through environmental Design Guidelines.* Los Angeles Task Force, Los Angeles, 1995.
10. Durkheim E., *Breviario di sociologia,* Newton Compton Editori, Roma, 1981.
11. Ferri E., *Dei sotitutivi penali*, Tipografia Roux e Favale, Torino, 1880.
    - *Lavoro e celle dei condannati*, Libreria Nuova, Roma, 1886.
    - *Difese penali*, Vol. III., Utet, Torino, 1925.

- *Studi sulla criminalità*, Utet, Torino, 1926.
- *Sociologia criminale*, Utet, Torino, 1929.

12. Geason S., Wilson P.R., *Designing Out Crime: Crime Prevention Through Environmental Design*, Australian Institute of Criminology, Canberra, 1989.
13. Giovenale D.G., *Satire*, Vol. II., Re Zefirino, Padova, 1846.
14. «Il programma di lavoro della Commissione per la revisione della legislazione penale», *La stampa*, 10 ottobre 1919.
15. Jacobs J., *The Death and Life of Great American Cities*, Random House, New York, 1961.
16. Jeffery C.R., *Crime Prevention Through Environmental Design*, Sage Publications, Beverly Hills, 1977.
17. Jeffery C.R., Zahm D.L., *Crime Prevention Through Environmental Design, Opportunity Theory, and Rational Choice Models.*: Transaction Publisher, New Brunswick, 1993.
18. Lombroso C., *Le Figaro,* Parigi, 30 Juillet, 1906.
19. Lusa V., Pecora B., *Dissertazioni criminologiche nell'Italia pre e post unitaria: aspetti teorici e pratici e la loro valenza nel processo penale,* Key editore, Frosinone, 2015.
20. Newman O., *Defensible Space People and Design in the Violent City,* Architectural Press, Londra, 1973a.
    - *Design Guidelines for Creating Defensible Space.* National Istitute of Law Enforcment and Criminal Justice, Washington D.C., 1973b.
    - *Creating Defensible Space*, U.S Department of Housing and Urban Development-Office of Policy Development and Research, Washington D.C., 1996.
21. Norma UNI CEN/TR 14383-2:2010.
22. Park R.E., Burgess E.W., Mckenzie, R., *The City: Suggestions for Investigation of Human Behavior in the Urban Environment,* The University of Chicago Press, Chicago, 1925.
23. *Participation Citoyenne: Devenir Actuer de sa Sécurité,* Gendarmerie Nationale: Ministère de l'Interieur, 28 Agosto 2011.
24. *Reducing Residential Crime and Fear: The Hartford Neighborhood Crime Prevention Program,* National Institue of Law Enforcement and Criminal Justice, 1979.
25. Shaw C.R., Mckay H.D., *Social factors in juvenile delinquency.* National Commission on Law Observance and Enforcement Report n. 13, U.S. Government Printing, Washington D.C., 1931
26. Vicari Haddock S., Moulaert F., *Rigenerare la città: partiche di innovaione sociale nelle città europee.* Il Mulino, Bologna, 2009.
27. Williams F.P., McShane M.D., *Devianza e Criminalità*, Il Mulino, Bologna, 2002.
28. Wilson J.Q., Kelling G.L., 1982. «Broken Windows: The Police and Neighborhood Safety» *The Atlantic* 249 (3), p. 29-38.
29. Zorbaugh H.W., «The Natural Areas of the City», *The American Sociological Society,* p. 188-197, 1926.
    - *The Gold Coast and the Slum: A Sociological Study of Chicago's Near North Side.* The University of Chicago Press, Chicago, 1929.

Sitografia

1. *Associazione Controllo del Vicinato.* Disponibile al sito Internet: https://www.acdvevents.it
2. Cap. *Chicago Area Project: Strengthening neighborhoods, Helping young people.* Disponibile al sito Internet: http://www.chicagoareaproject.org
3. *City of London Police.* Disponibile al sito Internet: https://www.cityoflondon.police.uk/a/your-area/city-of-london/city-of-london/community-policing/
4. *Cuerpo Nacional de Policìa* Disponibile al sito Internet: https://www.policia.es/_es/colabora_participacion.php
5. *European Forum for Urban Security.* Disponibile al sito Internet: https://efus.eu
6. *Guardian Angels: Safety Patrol.* Disponibile al sito Internet: http://guardianangels.org
7. *La Funciòn Preventiva de la Policìa: La Policìa de Barrio.* Disponibile al sito Internet: https://www.seguridadpublica.es/2010/12/la-funcion-preventiva-de-la-policia-la-policia-de-barrio-su-necesidad-y-funciones-relaciones-de-la-policia-con-el-ciudadano-normas-basicas-de-actuacion/

8. *Neighbourhood Watch*. Disponibile al sito Internet: https://www.ourwatch.org.uk/about-us/
9. *Social Street: dal Virtuale al Reale al Virtuoso*. Disponibile al sito Internet: http://www.socialstreet.it
10. *Urbact*. Disponibile al sito https://urbact.eu/
11. *Voisins Vigilants et Solidaires*. Disponibile al sito Internet: https://www.voisinsvigilants.org/voisin