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**

Tutti gli articoli pubblicati su questa Rivista sono distribuiti con licenza **Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License** (cc) BY-NC-ND

Editore e Direttore: **Augusto BALLONI**, presidente S.I.V., già professore ordinario di criminologia, Università di Bologna, Italia (direzione@vittimologia.it)

COMITATO EDITORIALE

Coordinatore: **Raffaella SETTE**, dottore di ricerca in criminologia, professore associato, Università di Bologna, Italia (redazione@vittimologia.it)

Elena BIANCHINI (Università di Bologna), Roberta BIOLCATI (Università di Bologna), Lorenzo Maria CORVUCCI (Foro di Bologna), Emilia FERONE (Università "G. D'Annunzio", Chieti-Pescara), Francesco FERZETTI (Università "G. D'Annunzio", Chieti-Pescara), Maria Pia GIUFFRIDA (Associazione Spondé), Giorgia MACILOTTI (Università Tolosa 1 Capitole, Francia), Andrea PITASI (Università "G. D'Annunzio, Chieti-Pescara), Sandra SICURELLA (Università di Bologna)

COMITATO SCIENTIFICO

Coordinatore: **Roberta BISI**, vice Presidente S.I.V., professore ordinario di sociologia della devianza, Università di Bologna, Italia (comitatoscientifico@vittimologia.it)

Andrea BIXIO (Università Roma "La Sapienza"), Encarna BODELON (Università Autonoma di Barcellona, Spagna), Stefano CANESTRARI (Università di Bologna), Laura CAVANA (Università di Bologna), Gyorgy CSEPELI (Institute of Advanced Studies Koszeg, Ungheria), Janina CZAPSKA (Università Jagiellonian, Cracovia, Polonia), Lucio D'ALESSANDRO (Università degli Studi Suor Orsola Benincasa, Napoli), François DIEU (Università Tolosa 1 Capitole, Francia), Maria Rosa DOMINICI (S.I.V.), John DUSSICH (California State University, Fresno), Jacques FARSEDAKIS (Università Europea, Cipro), André FOLLONI (Pontifical Catholic University of Paraná, Brasile), Ruth FREEMAN (University of Dundee, UK), Paul FRIDAY (University of North Carolina, Charlotte), Shubha GHOSH (Syracuse University College of Law, USA), Xavier LATOUR (Université Côte d'Azur), Jean-Marie LEMAIRE (Institut Liégeois de Thérapie Familiale, Belgio), André LEMAÎTRE (Università di Liegi, Belgio), Silvio LUGNANO (Università degli Studi Suor Orsola Benincasa, Napoli), Mario MAESTRI (Società Psicoanalitica Italiana, Bologna), Luis Rodriguez MANZANERA (Università Nazionale Autonoma del Messico), Gemma MAROTTA (Sapienza Università di Roma), Vincenzo MASTRONARDI (Unitelma-Sapienza, Roma), Maria Rosa MONDINI (Centro Italiano di Mediazione e Formazione alla Mediazione, Bologna), Stephan PARMENTIER (Unviersità Cattolica, Lovanio, Belgio), Tony PETERS† (Università Cattolica, Lovanio, Belgio), Monica RAITERI (Università di Macerata), Francesco SIDOTI (Università de l'Aquila), Philip STENNING (Università di Griffith, Australia), Liborio STUPPIA (Università "G. D'Annunzio, Chieti-Pescara), Emilio VIANO (American University, Washington, D.C.), Sachio YAMAGUCHI (Università Nihon Fukushi, Giappone), Simona ZAAMI (Università Roma "La Sapienza"), Christina ZARAFONITOU (Università Panteion, Atene), Vito ZINCANI (Procura della Repubblica, Modena), Vladimir ZOLOTYKH (Udmurt State University, Russia)

doi: 10.14664/rcvs/814

Studiare la cybercriminalità: alcune riflessioni metodologiche

Étudier la cybercriminalité : quelques réflexions méthodologiques

Studying cybercrime: some methodological reflections

Giorgia Macilotti[•]

Riassunto
L'articolo propone alcune riflessioni metodologiche in merito all'analisi delle forme di criminalità associate all'utilizzo di Internet e delle tecnologie digitali. Queste realtà devianti rappresentano infatti un fecondo terreno di ricerca, grazie in particolare alla relativa tracciabilità delle pratiche degli utenti e alla quantità di dati disponibili online.
Si presenteranno i principali approcci, metodi e problematiche riguardanti lo studio della cybercriminalità, focalizzandosi in particolare su alcuni esempi tratti da ricerche sulle unità di polizia specializzate nel contrasto al fenomeno in esame. Oltre agli apporti degli strumenti "tradizionali" dell'indagine sociologica, si esploreranno le interazioni con le nuove opportunità offerte dalle tecnologie digitali, così come gli effetti della relazione tra il ricercatore e l'oggetto della sua ricerca sulla costruzione e l'interpretazione dei dati.

Résumé
L'article propose quelques réflexions méthodologiques concernant l'analyse des formes de délinquance associées à l'utilisation d'Internet et des technologies numériques. En effet, ces réalités déviantes représentent un terrain de recherche fécond, grâce notamment à la relative traçabilité des pratiques des internautes et à la quantité de données disponibles en ligne.
Il s'agira de présenter les principaux approches, méthodes et problématiques concernant l'étude de la cybercriminalité, en se focalisant plus particulièrement sur certains exemples tirés d'études sur les unités de police spécialisées dans la lutte contre la cybercriminalité. Au-delà des apports des instruments « traditionnels » de la recherche sociologique, il serait également question d'explorer leurs interactions avec les nouvelles opportunités offertes par les technologies numériques, tout en considérant les effets de la situation d'enquête sur la construction et l'interprétation des données.

Abstract
The article intends to provide an overview of research methods on studying digital crimes. Indeed, these deviant realities provide a rich ground for social research, especially thanks to the traceability of digital activities and the availability of online data.
We will discuss the main approaches, methods and issues related to the study of cybercrime, focusing particularly on some examples drew from researching cybercrime law enforcement agencies. In addition to the opportunities offered by "traditional" sociological methods, the article explores their interplays with digital approaches, as well as the impacts of the researcher/researched relationship on data construction and analysis.

Key words: cybercrime; social research; methods; law enforcement.

[•] Dottore di ricerca in Criminologia e in Scienza politica, *enseignante-chercheuse contractuelle* presso l'Université Toulouse 1 Capitole (Francia), IDETCOM.

1. Introduzione.

La fine del ventesimo secolo è stata descritta come l'era di una nuova "rivoluzione"[1] legata allo sviluppo e alla diffusione di Internet e delle tecnologie dell'informazione, considerati fra i più espressivi "fondali in cui leggere il mutamento socioculturale nella tarda modernità"[2]. Se gli strumenti digitali, il cyberspazio e le forme sociocomunicative ad essi legate sono associati a cambiamenti decisivi in tutti gli ambiti della vita sociale, questi stessi effetti possono essere osservati anche per quanto riguarda l'agire criminale. Le tecnologie informatiche e telematiche, infatti, non solo hanno contribuito all'emergere di nuove condotte illecite interamente associate alla Rete, ma hanno anche fornito nuovi spazi, opportunità e strumenti di espressione alle forme di criminalità più "tradizionali". Dagli attacchi contro le infrastrutture critiche ai delitti sessuali contro i minori, passando per le frodi informatiche, gli esempi sono innumerevoli.

Si tratta di realtà criminali che hanno ampiamente investito la scena pubblica e mediatica, così come stimolato lo sviluppo di modelli analitici e interpretativi da parte di molteplici discipline scientifiche. La criminalità legata alle nuove tecnologie è stata inizialmente un ambito di studio privilegiato dell'informatica, dell'ingegneria elettronica e dei *computer security studies*, generalmente focalizzati sulla ricerca delle vulnerabilità e dei rischi riguardanti i sistemi informatici e telematici, nonché sullo sviluppo di soluzioni tecniche finalizzate all'individuazione delle minacce all'integrità dei sistemi e alla loro protezione[3]. Il problema che sollevano questi approcci non risiede tanto nei fenomeni analizzati, quanto nel modello di analisi spesso limitato "agli aspetti tecnici dei problemi di sicurezza, che sono trattati separatamente dagli effetti sociali e indipendentemente dalle interazioni costanti fra queste due dimensioni"[4]. È in questa prospettiva che si iscrivono invece gli orientamenti elaborati dalle scienze sociali che se, da un lato, intendono fornire dei contributi al fine di approfondire la natura e le caratteristiche delle realtà criminali e delle forme di vittimizzazione associate alla Rete, consentono altresì d'interrogare le ricomposizioni contemporanee delle forme di devianza e di controllo sociale, così come i processi di costruzione e di criminalizzazione dei rischi associati alle tecnologie digitali.

In quest'ottica, le forme di criminalità legate alla Rete rappresentano un terreno fecondo di ricerca, grazie in particolare alla relativa tracciabilità delle pratiche degli utenti e alla quantità di informazioni disponibili online. Tuttavia, l'esperienza empirica mostra come ci siano diversi aspetti problematici associati alle ricerche in questo ambito. Si pensi, ad esempio, alla difficoltà di misurare la prevalenza e l'incidenza[5] di questi fenomeni, che riguarda tanto le statistiche ufficiali sulla criminalità, che le inchieste di vittimizzazione e gli strumenti di *self-report*

[1] Si veda, in particolare: Castells M., *La nascita della società in rete*, Milano, Egea, 2002.

[2] Morcellini M., Pizzaleo A.G. (a cura di), *Net sociology. Interazioni tra scienze sociali e Internet*, Guerini e Associati, Milano, 2002, p. 29.

[3] Holt T. J., "Situating the problem of cybercrime in a multidisciplinary context", in Holt T. J. (a cura di), *Cybercrime through an interdisciplinary lens*, Routledge, London & New York, 2017, p. 1-15; Yar M., "Toward a cultural criminology of the Internet", in Steinmetz K. F., Nobles M. R. (a cura di), *Technocrime and criminological theory*, Routledge, New York, 2017, pp. 119-122.

[4] Dupont B, Gautrais V., "Crime 2.0 : le web dans tous ses états !", in *Champ pénal/Penal field*, Vol. VII, 2010, p. 36, disponibile alla pagina http://journals.openedition.org/champpenal/7782

[5] Nell'ambito delle statistiche sulla criminalità, generalmente si indica con "prevalenza" la percentuale di persone che hanno commesso i delitti e con "incidenza" il numero di delitti commessi. Sul punto si veda Aebi M. F., *Comment mesurer la délinquance ?*, Armand Colin, Paris, 2006, p. 37.

destinati ai possibili autori di reato[6]. Inoltre, realizzandosi in parte nel cyberspazio e in un ambiente per così dire "dematerializzato", la "cybercriminalità elimina nella maggior parte dei casi la presenza di testimoni"[7] e lascia spesso delle tracce che necessitano, per essere interpretate, di specifiche competenze che contribuiscono a lanciare una sfida anche "sul piano della effettiva gestione del *know how* tecnologico"[8].

Senza pretendere di realizzare un bilancio esaustivo, il presente articolo si propone d'interrogare i principali metodi di ricerca elaborati, in particolare dalla sociologia e dalla criminologia, per superare le difficoltà legate allo studio dell'agire criminale online, sottolineando al contempo le problematiche associate agli approcci adottati. In tal senso, dopo un breve esame della nozione di cybercriminalità, si presenteranno alcuni strumenti e strategie di rilevazione e di elaborazione delle informazioni elementari utilizzati per analizzare, tanto da un punto di vista "numerico" che "empatico"[9], le forme di criminalità associate alla Rete. L'analisi si fonda sulla più recente letteratura in materia, così come su esempi tratti da alcune nostre ricerche condotte, in particolare, con le unità di polizia specializzate nel contrasto alla cybercriminalità[10].

2. La cybercriminalità: alcune precisazioni terminologiche.

Tra i primi termini utilizzati per descrivere il fenomeno in esame si può ricordare quello di criminalità informatica (*computer crime*), nozione che designa tutte le attività illecite in cui il computer è coinvolto come strumento, simbolo o oggetto del fatto delittuoso[11]. Con la democratizzazione del Web verso la metà degli anni novanta del secolo scorso, al termine evocato si affianca quello di cybercriminalità (*cybercrime*), con cui si indicano tutti quei comportamenti illeciti la cui commissione implica l'uso delle reti telematiche o in cui "l'autore utilizza delle conoscenze particolari del cyberspazio"[12]. In questa prospettiva, se la prima nozione si riferisce principalmente alle realtà criminali in cui è presente l'utilizzo del computer, la cybercriminalità abbraccia in realtà un insieme più ampio di condotte illecite, accomunate dall'utilizzo di Internet e realizzate attraverso un qualsiasi dispositivo che consenta la connessione in Rete[13].

Proprio in virtù della diffusione massiva del Web, quest'ultimo termine si è progressivamente imposto nel dibattito pubblico e scientifico ed è stato consacrato, almeno dal punto di vista dei trattati internazionali, dalla "Convenzione sulla cybercriminalità" del Consiglio d'Europa, primo strumento multilaterale in materia firmato a

[6] Per tutti si veda Holt T. J., "Cybercrime", in Huebner B.M., Bynum T.S., *The handbook of measurement issues in criminology and criminal justice*, John Wiley & Sons, New York, 2016, p. 30.

[7] Lavoie P.-E., Fortin F., Tanguay S., "Problèmes relatifs à la définition et à la mesure de la cybercriminalité", in Fortin F., (a cura di), *Cybercriminalité. Entre inconduite et crime organisé*, Presses Internationales Polytechnique, Canada, 2013, p. 16.

[8] D'Alessandro L., "Prefazione", in in Pitasi A. (a cura di), *Webcrimes. Normalità, devianze e reati nel cyberspace*, Pitasi A. (a cura di), Guerini e Associati, Milano, 2007, p. 13.

[9] Baraldi C., "L'orientamento epistemologico della ricerca empirica", in Cipolla C. (a cura di), *Il ciclo metodologico della ricerca sociale*, FrancoAngeli, Milano, 2001, pp. 46-47.

[10] Nello specifico, un lavoro per la preparazione della tesi di dottorato in cotutela "Pedofilia e pedopornografia online: una ricerca socio-criminologica nella realtà italiana e francese" (Dipartimento di Sociologia, Università di Bologna e CERP, Université Toulouse 1 Capitole) e due indagini post-dottorali in merito alla vittimizzazione online dei minori ("Les enfants face aux écrans: pratiques, exposition au risque et victimation", IDETCOM, Université Toulouse 1 Capitole) e all'azione delle forze di polizia nell'ambito del contrasto alla cybercriminalità ("Le contrôle social au prisme des technologies de l'information et de la communication. Acteurs, pratiques et problématiques", IDETCOM, Université Toulouse 1 Capitole).

[11] Ponti G., *Compendio di criminologia*, Torino, Cortina, 1994, pp. 161 – 163.

[12] Furnell, S., *Cybercrime: vandalizing the information society*, Addison Wesley, Boston, 2002, p. 21, Wall D. S., "Cybercrimes and the Internet", in Wall D. S (a cura di), *Crime and the Internet*, Routledge, New York, pp. 1-7.

[13] Moore R., *Cybercrime. Investigating high-technology computer crime*, Elsevier/Anderson, Amsterdan/Boston, 2011, p. 4; Holt T. J, "Cybercrime", *op. cit.*, pp. 30-31.

Budapest nel 2001. Ciononostante, la nozione in esame non è esente da critiche, tanto da indurre alcune autori a parlarne nei termini di "un'impasse scientifica totale"[14] o "di una fragile base per la ricerca e la rilevazione di dati (…) che tende a rendere più complessa l'attività di prevenzione e repressione"[15]. In quest'ottica, ad esempio, le Nazioni Unite sottolineano come le difficoltà di cooperazione internazionale nell'ambito del contrasto al fenomeno in esame siano in parte legate alla natura vaga e imprecisa di questa nozione[16].

Diversi aspetti permettono di comprendere le ragioni sottese a queste affermazioni e, più in generale, alle critiche sollevate. Un primo elemento concerne la mancanza di un consenso in letteratura in merito alla definizione e alla classificazione delle realtà criminali associate alla cybercriminalità, aspetto che rinvia inoltre alla sua origine etimologica legata ai romanzi di *science-fiction* e alla sua diffusione in ambito mediatico[17]. È opportuno poi precisare che, nella maggioranza dei Paesi, non esiste una definizione legale di quest'espressione[18]. La stessa Convenzione sulla cybercriminalità, ad esempio, non precisa il significato di questo termine, ma si limita ad enumerare le forme di criminalità che dovrebbero essere comprese al suo interno. A queste considerazioni si aggiunge poi la natura vaga e imprecisa di questa nozione, che ingloba una pluralità di condotte criminali il cui unico comune denominatore è il fatto di essere realizzate "nel" o "attraverso" il cyberspazio[19]. Si tratta quindi di un termine che designa un insieme vasto ed eterogeno di condotte criminali che vanno dalla diffusione di virus informatici alla creazione di mercati di vendita di droga online, passando per le forme di bullismo in Rete. In Francia, ad esempio, si stima che siano circa 470 le infrazioni codificate legate ai sistemi d'informazione e alla cybercriminalità[20].

Si sottolinea, in tal senso, come sia più opportuno utilizzare questa nozione non tanto per descrivere un fenomeno criminale a sé stante, quanto per indicare un insieme di pratiche e condotte criminali accomunate, nella loro commissione, dal ruolo centrale svolto dalle tecnologie dell'informazione e della comunicazione[21]. La cybercriminalità è pertanto un termine di natura pragmatica e non scientifica, utilizzato per designare differenti realtà criminali caratterizzate da problematiche simili per quanto concerne la loro regolazione e il loro contrasto che, ad esempio, sono resi complessi dal supposto anonimato dei comportamenti, dal carattere immateriale delle informazioni e dalla dimensione transnazionale delle condotte.

A partire da questa prospettiva si analizzeranno quindi le fonti e gli strumenti di ricerca maggiormente mobilizzati per studiare le differenti pratiche devianti associate alla Rete.

3. Lo studio della cybercriminalità: principali strumenti di misura e di rilevazione "numerica".

Misurare la criminalità è uno dei più antichi problemi a cui gli approcci macrosociologici sullo studio del crimine hanno tentato di dare risposta, in

[14] Leman-Langlois S., "Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberspace commercial", in *Criminologie*, 2006, Vol. 39, N. 1, p. 78.
[15] Lavoie P.-E., Fortin F., Tanguay S., "Problèmes relatifs à la définition et à la mesure de la cybercriminalité", *op. cit.*, pp. 3-4.
[16] *Ibidem,* p. 10.
[17] Wall D. S., "Criminalising cyberspace: the rise of the Internet as a 'crime problem'", in Jewkes Y., Yar M. (a cura di), *Handbook of Internet crime*, Willan Publishing, Cullompton, 2009, pp. 89-90.
[18] *Ibidem*, p. 88.
[19] Yar M., *Cybercrime and* society, Sage, London, 2006, p. 5.
[20] Pereira B., "La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité", in *Revue internationale de droit économique*, Tomo XXX, N. 3, 2016, p. 388.
[21] Yar M., *Cybercrime and* society, *op. cit.*, p. 9.

particolare attraverso l'uso di fonti e lo sviluppo di strategie di rilevazione che permettano di evidenziare non solo "la diffusione dei differenti tipi di reato e la distribuzione nel tempo e nello spazio del fenomeno criminale"[22], ma anche le caratteristiche degli eventi criminosi, dei loro autori e eventualmente delle loro vittime. In tal senso, differenti tecniche sono utilizzate per tentare di stimare l'incidenza e la prevalenza dei fenomeni devianti associati alla Rete.

3.1 Le statistiche ufficiali sulla criminalità.

Fra i differenti strumenti utilizzati per misurare la criminalità, un ruolo di primo piano è tradizionalmente svolto dalle statistiche ufficiali[23], ovvero quelle statistiche prodotte a partire dai dati generati dall'attività delle forze di polizia e della giustizia penale nell'ambito della repressione dei fenomeni criminali. Si tratta infatti di una tipologia di fonti che si iscrive nella storia stessa degli studi sulla criminalità, di cui i primi esempi possono essere trovati nei lavori degli "statistici morali" del XIX secolo, Quetelet e Guerry[24].

Fermo restando le differenze fra i diversi ordinamenti giuridici nazionali, generalmente le statistiche utilizzate sono quelle "di polizia", che concernono i delitti trasmessi alla magistratura di cui le forze dell'ordine sono venute a conoscenza in seguito alle denunce ricevute o alle indagini svolte d'iniziativa, e quelle "giudiziarie", che riguardano i reati per i quali la magistratura ha iniziato l'azione penale o adottato dei provvedimenti giudiziari[25]. Se queste ultime sono state le prime ad apparire già agli inizi XIX secolo nel momento in cui la criminalità diviene oggetto del dibattito pubblico e dell'azione politica, a partire dal XX secolo sono le statistiche di "polizia" ad essere maggiormente utilizzate per lo studio della criminalità, in quanto considerate più prossime all'evento criminoso rispetto a quelle processuali o dell'amministrazione penitenziaria e, pertanto, in grado di misurarlo in maniera più precisa[26].

In questa prospettiva, uno dei primi fattori che rende estrematemene arduo lo studio della cybercriminalità è l'inadeguatezza delle fonti

[22] Bandini T. *et al*., *Criminologia. Il contributo della ricerca alla conoscenza del crimine e della reazione sociale*, Giuffré, Milano, 1991, p. 99.

[23] Si fa riferimento al carattere "ufficiale" di queste statistiche in quanto si tratta di "raccolte di dati che vengono effettuate, nella quasi totalità dei casi, dall'amministrazione pubblica", Corbetta P., *Metodologia e tecniche della ricerca sociale*, il Mulino, Bologna, 2011, p. 289.

[24] Per un approfondimento si veda Balloni A., Bisi R., Sette R., *Principi di criminologia. Le teorie*, Wolters Kluwer-Cedam, Padova, 2015, p. 181-183. Invero, l'utilizzo di fonti statistiche pubbliche si associa alla tradizione empirica della sociologia più in generale, con esempi illustri come nel caso dello studio sul suicidio di Émile Durkheim o dell'analisi dei comportamenti elettorali di André Siegfried.

[25] Saponaro A., *Vittimologia. Origini - Concetti – Tematiche*, Giuffré, Milano, 2004, pp. 151-152; Robert Ph. *et al*., *Les comptes du crime. Les délinquances en France et leurs mesures*, L'Harmattan, Paris, 1994. Nel testo si è adottata la dicitura in uso in Francia. Per quanto riguarda l'Italia, le statistiche giudiziari penali sono elaborate e pubblicate dall'ISTAT che distingue principalmente tre diverse elaborazioni: le "statistiche della delittuosità", che corrispondono all'espressione statistiche di "polizia" richiamata nel presente articolo; le "statistiche della criminalità", che riguardano i crimini che vengono iscritti nei registri dei reati delle Procure della Repubblica e che permettono in seguito di analizzare l'ammontare dei procedimenti archiviati e di quelli che proseguono l'iter processuale; le "statistiche sui condannati", che concernono le sentenze definitive depositate nel Casellario giudiziale centrale e che consentono di conoscere l'entità e le caratteristiche dei condannati e delle sentenze di condanna passate in giudicato. Sul punto si vedano i diversi rapporti dell'ISTAT sulla criminalità e la sicurezza in Italia e, in particolare, Muratore M. G. (a cura di), *Delitti, imputati e vittime dei reati. Una lettura integrata delle fonti sulla criminalità e la giustizia*, ISTAT, Roma, 2017, p. 7. Pare altresì opportuno precisare che le statistiche di "polizia" presentano differenti tipi di dati che non si limitano alla sola infrazione, ma riguardano anche l'autore presunto del reato e, in alcuni casi, la vittima, così come le misure adottate dalle forze di polizia come denunce, arresti/fermi e, in talune ipotesi, perquisizioni e sequestri.

[26] Zauberman R. *et al*., "L'acteur et la mesure. Le comptage de la délinquance entre données administratives et enquêtes", in *Revue française de sociologie*, Vol. 50, n. 1, 2009, pp. 31-32; Robert Ph. *et al*., *Les comptes du crime. Les délinquances en France et leurs mesures*, *op. cit.*, p. 11. Si veda inoltre l'analisi classica di Sellin T., "The Basis of a Crime Index", in *The Journal of Criminal Law et Criminology*, n. 22, 1931, pp. 335-356.

statistiche ufficiali che, nella maggioranza dei Paesi, non permettono di stimare con sufficiente precisione l'incidenza e la prevalenza nella popolazione delle tipologie di delitti in esame[27]. In tal senso, differenti iniziative sono state sviluppate al fine di migliorare gli strumenti di rilevazione, ma ciononostante i dati prodotti non permettono di avere una "fotografia" accurata del fenomeno. Negli Stati Uniti, ad esempio, l'*Uniform Crime reporting* (UCR) del FBI non prevede alcun indicatore per gli eventi criminosi associati alla Rete e il *National Incident-Based Reporting System* (NIBRS), sebbene abbia introdotto una categoria concernente i fatti commessi "attraverso" o "contro" il computer, consente di misurare con precisione solamente i delitti sessuali contro i minori e le varie forme di frode online[28]. In Francia, i fatti denunciati dalle forze di polizia all'autorità giudiziaria sono tradizionalmente registrati attraverso l'*état 4001*, una griglia di classificazione delle infrazioni composta da 107 *index* fra cui solo due si riferiscono, e solo in parte, alla cybercriminalità. Al fine di ottenere una misura più precisa del fenomeno, le unità della *Police* e della *Gendarmerie* hanno implementato un nuovo sistema di rilevazione basato non più su delle categorie di sintesi, ma direttamente sulle infrazioni previste dal codice penale e da altri testi normativi in materia[29]. Se dal 2015 questi nuovi strumenti hanno permesso di avere una visione statistica più precisa del fenomeno, in realtà si tratta ancora d'informazioni frammentate e che in genere si riferiscono ad alcune tipologie di delitti digitali e non all'insieme delle realtà criminali associate alla Rete[30]. Un risultato simile può essere osservato anche per quanto riguarda le statistiche "di polizia" pubblicate dall'istituto italiano di statistica (ISTAT), che forniscono dati significativi solamente per tre macro-categorie di fenomeni: la "pornografia minorile e detenzione di materiale pedopornografico", le "truffe e frodi informatiche" e i "delitti informatici"[31]. Sembra poi opportuno precisare che, al di là della mancata previsione di criteri precisi concernenti le infrazioni associate a Internet, la maggior parte dei sistemi di rilevazione non consente di discriminare il delitto commesso attraverso la Rete da quello simile nei contenuti, ma realizzato secondo modalità più "tradizionali". Un esempio in tal senso è fornito dalla categoria italiana "pornografia minorile e detenzione di materiale pedopornografico" che ingloba al suo interno tutte le infrazioni in materia a prescindere dalle modalità concrete di realizzazione del fatto (attraverso Internet, riviste, documenti cartacei, ecc.).

[27] Sul punto la letteratura sembra concorde, per tutti si veda Côté A. M., Bérubé M., Dupont B., "Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité", in *Réseaux*, Vol. 3., N. 197-198, 2016, pp. 207-208.

[28] Holt T. J, "Cybercrime", *op. cit.*, pp. 36-37.

[29] I sistemi d'informazione della *Police* (LRPPN) e della *Gendarmerie* (PULSAR) utilizzano, rispettivamente dal 2014 e dal 2012, i codici NATINF (*NATures d'INFractions*) del Ministero della Giustizia francese. I dati concernenti i fatti e le persone denunciate sono trasmessi al *Service statistique ministériel de la sécurité intérieure* (SSMSI) e sono poi elaborati dall'*Observatoire national de la délinquance et des réponses pénales* (ONDRP) che pubblica annualmente le statistiche francesi sulla criminalità.

[30] Attualmente le informazioni più precise riguardano le infrazioni ai "sistemi di trattamento automatico dei dati" (STAD), come ad esempio l'accesso abusivo a un sistema informatico; le infrazioni "ai diritti delle persone risultanti da trattamenti informatici", come ad esempio la violazione della corrispondenza elettronica; le infrazioni legate alla diffusione di "contenuti illeciti", come i casi di diffamazione a mezzo Internet; i delitti sessuali contro i minori, come nei casi di produzione e diffusione di materiale pedopornografico. Per i delitti registrati nel 2016, si veda Langlade A., "La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'Internet en 2016 : éléments de mesure et d'analyse", in ONDRP, *La note de l'ONDRP. Rapport annuel 2017*, 2017, pp. 1-4, disponibile al sito web https://inhesj.fr/ondrp/publications/la-note-de-londrp/la-cybercriminalite-et-les-infractions-liees-lutilisation

[31] http://dati.istat.it/ Si sottolinea, tuttavia, che queste considerazioni valgono per le statistiche di "polizia" (numero di delitti denunciati all'autorità giudiziaria, numero di autori denunciati all'autorità giudiziaria), mentre per le statistiche "giudiziarie" i dati disponibili riguardano un insieme più vasto di delitti associati alla Rete.

A queste diverse considerazioni si associano poi i problemi che concernono le statistiche della delittuosità più in generale, dal punto di vista tanto della loro produzione che della loro interpretazione. Questo tipo di fonti, infatti, fornisce delle informazioni solamente sui delitti ufficialmente rilevati dalle forze di polizia e trasmessi all'autorità giudiziaria, i quali costituiscono solo una parte dei crimini commessi. Si parla, in tal senso, di "numero oscuro" della criminalità per designare la differenza fra la criminalità "registrata" dalle agenzie del controllo sociale e quella "reale" corrispondente all'insieme dei delitti effettivamente perpetrati[32].

In primo luogo, le statistiche "di polizia" risentono della scelta dei singoli cittadini di denunciare o meno i reati subiti. La persona offesa dal reato, ad esempio, può decidere di non allertare le forze di polizia in quanto teme le conseguenze della denuncia in termini d'immagine o di ritorsione del criminale. In altri casi, la vittima può ritenere che l'entità del danno subito non valga il dispendio di tempo ed energia che il contatto con il sistema legale richiede, soprattutto laddove non abbia sufficiente fiducia nelle competenze e nell'efficienza dell'apparato giudiziario. In materia di tecnologie digitali, inoltre, gli individui possono non disporre delle adeguate conoscenze per comprendere e affrontare i fenomeni legati alla cybercriminalità e, in taluni casi, possono semplicemente ignorare di esserne stati vittime, come si verifica spesso per gli accessi abusivi ai sistemi informatici[33].

In secondo luogo, le statistiche sulla delittuosità dipendono dalle modalità concrete di registrazione dei reati da parte delle forze di polizia, la cui analisi mostra come questo tipo di fonti non sia il risultato di un processo neutro di raccolta dei dati, ma piuttosto una "costruzione sociale" frutto di differenti logiche[34]. Infatti, la possibilità concreta che un determinato evento criminoso, denunciato dalla vittima o conosciuto dalle istituzioni del controllo sociale, sia effettivamente registrato e portato all'attenzione dell'autorità giudiziaria dipende da molteplici fattori[35]. La rilevazione di un evento delittuoso è condizionata innanzitutto dal modo in cui lo stesso è qualificato dalle forze di polizia e da come una determinata definizione legale è applicata in concreto nelle loro procedure[36]. Ad esempio, nel corso di alcuni periodi di osservazione diretta presso delle unità di polizia specializzate nel contrasto alla cybercriminalità, si è avuto modo di analizzare le pratiche di registrazione dei delitti digitali e di esaminare le diverse modalità di qualificazione di una medesima condotta che, come sottolinea un gendarme francese, talvolta conducono a degli errori anche significativi:

"Abbiamo sviluppato un nuovo sistema per tenere traccia e far risalire i dati, ma ci sono ancora alcuni problemi, soprattutto dal punto di vista dell'inserimento dati (…) Non serve a niente fare tutte queste modifiche se poi [gli operatori, n.d.a] *mi mettono tutti i fatti come truffe online, invece di specificare come qui* [la persona indica lo schermo del computer che presenta il software di gestione] *che si tratta di un accesso abusivo ad un sistema informatico"*[37].

[32] Per una sintesi si veda Gallino L., *Dizionario di sociologia*, Utet, Torino, 2006, p. 182.

[33] Macilotti G., "La criminalità informatica e telematica fra antichi dilemmi e nuove sfide", in Balloni A., Bisi R., Sette R., *Principi di criminologia applicata. Criminalità, controllo, sicurezza*, Wolters Kluwer-Cedam, Padova, 2015, p. 275; Ghernaouti-Hélie S., *La cybercriminalité. Le visible et l'invisible*, PPUR, Lausanne, 2009, pp. 59-60.

[34] Maguire M., "Crime data and statistics", in Maguire M., Morgan R. e Reiner R (a cura di), *The Oxford Handbook of Criminology*, Oxford University Press, Oxford, 2007, pp. 249 e s.

[35] Per un'analisi approfondita si veda Matelly J.-H., Mouhanna C., *Police des chiffres et des doutes*, Michalon, Paris, 2007.

[36] Maguire M., "Crime data and statistics", *op. cit.*, p. 258.

[37] Ufficiale della *Gendarmerie nationale*, operatore specializzato nelle investigazioni sulla cybercriminalità (NTECH).

La corretta comprensione di questi eventi richiede, infatti, un bagaglio di competenze specifiche, tanto dal punto di vista giuridico che informatico, le quali non sono necessariamente possedute da tutti gli operatori di polizia. Un secondo ordine di fattori concerne poi l'evoluzione della normativa penale e un esempio in tal senso può essere tratto dal contesto italiano in cui, fino al 2012, l'adescamento online di minore non era qualificato penalmente e, pertanto, questo fenomeno era escluso dalle statistiche pubblicate dall'ISTAT. Inoltre, soprattutto in quegli ordinamenti dove sia prevista "l'opportunità" e non "l'obbligatorietà" dell'esercizio dell'azione penale, le priorità politiche e degli uffici di polizia possono condurre a privilegiare le investigazioni concernenti alcune tipologie di reato, come è attualmente il caso in Francia per l'apologia di terrorismo associata anche alla Rete[38], talvolta a detrimento di altre fattispecie che suscitano minor allarme sociale o che non rientrano fra i principali indirizzi delle politiche penali e di sicurezza[39].

Si osserva allora come innumerevoli realtà, afferenti tanto alla cybercriminalità che alla delittuosità più in generale, non appaiano nelle statistiche ufficiali annualmente pubblicate. Ciò non significa che queste fonti non siano di alcuna utilità, ma piuttosto che debbano essere interpretate per quello che effettivamente sono in grado di misurare. Le statistiche sulla criminalità, e in particolare quelle "di polizia", sono fondamentalmente il prodotto di logiche di selezione e pertanto devono essere considerate come uno strumento di analisi dell'attività di carattere repressivo svolta dalle istituzioni del controllo sociale[40], come il riflesso dell'attività dei servizi di polizia che fornisce una misura precisa solamente della criminalità da essi segnalata all'autorità giudiziaria[41].

Al fine di ovviare a queste differenti problematiche, le amministrazioni pubbliche così come gli studiosi si avvalgono di altri strumenti di rilevazione volti ad analizzare non tanto l'attività delle istituzioni penali, quanto il concreto vissuto e le percezioni della popolazione in merito alla criminalità.

3.2 Le inchieste di vittimizzazione.

Dapprima, si possono ricordare le inchieste di vittimizzazione apparse alla fine degli anni sessanta del secolo scorso[42]. Si tratta di studi condotti su

[38] Nelle statistiche francesi pubblicate dall'ONDRP si osserva, ad esempio, come questo tipo di reati commessi attraverso la Rete passi da 30 casi nel 2014 a 173 nel 2015, Langlade A., "La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'Internet en 2016 : éléments de mesure et d'analyse", *op. cit.*, pp. 3-4. In questo caso, l'aumento esponenziale dei delitti registrati nel 2015 deve essere interpreto alla luce del contesto francese caratterizzato dalla recrudescenza degli attentati terroristici, a cui sono seguite una serie di misure normative e circolari ministeriali che invitano le istituzioni penali ad essere particolarmente reattive nell'ambito del contrasto all'apologia e alla provocazione, anche online, del terrorismo. Per un esempio si veda la circolare del 12 gennaio 2015 dell'allora ministro della Giustizia Christiane Taubira, http://www.justice.gouv.fr/publication/circ_20150113_infractions_commises_suite_attentats201510002055.pdf

[39] Yar M., *Cybercrime and society*, *op. cit.*, pp. 12-13; Mucchielli L., *Violences et insécurité. Fantasmes et réalités dans le débat français*, La Découverte, Paris, 2001, p. 24; Matelly J.-H., Mouhanna C., *Police des chiffres et des doutes, op. cit.*, in particolare p. 47-48, 53-59; Jobard F., De Maillard J., *Sociologie de la police. Politiques, organisations, réformes*, Armand Colin, Paris, 2015, pp. 220-222.

[40] Kitsuse J., Cicourel A., "A note of the uses of official statistics", in *Social problems*, Vol. 11, N. 2, 1963, pp. 131-139.

[41] Dieu F., *Politiques publiques de sécurité*, L'Harmattan Paris, 1999, p. 72.

[42] Le inchieste di vittimizzazione sono state inaugurate negli Stati Uniti su impulsione della *President's Commission on Law Enforcement and the Administration of Justice* e, a partire gli anni settanta del secolo scorso, sono state implementate annualmente. In Europa, le inchieste di vittimizzazione cominciano ad essere utilizzate sporadicamente a partire dagli anni '80, in particolare nel Regno Unito, e sono poi implementate negli altri Paesi europei solamente a partire dal decennio successivo con modi e tempi differenti. In Italia, ad esempio, le prime due indagini condotte dall'istituto italiano di statistica (ISTAT) sono del 1997-1998 e del 2002. Si precisa, infine, che accanto alle indagini sulla vittimizzazione in generale, si sono nel tempo sviluppati degli studi focalizzati su alcune tematiche particolari (come ad esempio la violenza contro le donne o in ambito scolastico), così come su alcuni contesti territoriali specifici (come una regione o una città). Robert Ph.,

campioni rappresentativi della popolazione interrogati in merito alle eventuali esperienze di vittimizzazione vissute in un preciso arco temporale precedente alla somministrazione del questionario, il quale è generalmente fatto compilare durante un'intervista telefonica, per via postale/telematica o nell'ambito di un'interazione faccia a faccia. Questi strumenti di rilevazione si pongono così l'obiettivo non solo di misurare la frequenza e l'evoluzione di determinati reati indipendentemente dall'azione dalle istituzioni pubbliche e dai cambiamenti normativi, ma altresì di analizzare le caratteristiche delle vittime e i fattori di vittimizzazione[43], informazioni che possono essere utilizzate per "attuare strategie di prevenzione mirate, in relazione a specifici contesti e determinati soggetti"[44].

Nell'ambito della cybercriminalità molte inchieste pubbliche di vittimizzazione hanno progressivamente integrato delle questioni concernenti alcuni delitti associati alla Rete. L'ufficio di statistica britannico (ONS), ad esempio, ha introdotto nel *Crime Survey for England & Wales* (CSEW) alcune domande in merito alle esperienze di vittimizzazione legate alla frode informatica, agli accessi abusivi ai sistemi informatici, ai *computer virus* o all'utilizzazione abusiva di dati personali. Inoltre, per quanto riguarda le questioni concernenti le molestie e lo *stalking*, il questionario permette di specificare se i fatti dichiarati dalla vittima siano stati commessi anche attraverso l'uso delle nuove tecnologie. In Francia, l'inchiesta di vittimizzazione *Cadre de vie et sécurité* (CVS) dell'istituto nazionale di statistica (INSEE) prevede delle domande in merito alle frodi online, alle ingiurie e alle minacce realizzate anche attraverso la Rete. L'inchiesta italiana sulla "sicurezza dei cittadini" condotta dall'ISTAT presenta aspetti analoghi, con una parte del questionario dedicata alle clonazioni delle carte di credito, alle truffe legate alla Rete, al furto o all'utilizzo improprio dell'identità digitale, alla ricezione di proposte e messaggi inappropriati attraverso Internet e i *social networks*. Al di là degli studi realizzati dagli organismi pubblici, questo strumento di rilevazione è altresì utilizzato in ambito accademico, in particolare per studiare le forme di vittimizzazione associate alla cyber-violenza contro i minori[45] e alle condotte di *hacking*[46]. È grazie a questo tipo di studi, infatti, che si sono acquisite maggiori informazioni sulla vittimizzazione online dei pre-adolescenti che, generalmente, sono esclusi dal campione interrogato

Zauberman R., *Mesurer la déliquance*, Presses de Sciences-Po, Paris, 2011. Per un esempio di inchiesta di vittimizzazione a livello regionale, si veda Balloni A., Bisi R., Costantino S. (a cura di), *Legalità e comunicazione*, FrancoAngeli, Milano, 2008.

[43] Mucchielli L., "Enquêter sur la délinquance. Réflexions méthodologique et épistémologiques", in Boucher M. (a cura di), *Enquêter sur les déviances et la délinquance. Enjeux scientifiques, politiques et déontologiques*, L'Harmattan, Paris, 2015, pp. 53-58, Saponaro A., *Vittimologia. Origini - Concetti – Tematiche*, *op. cit.*, pp. 148 e s.

[44] Sicurella S., "Lo studio della vittimologia per capire il ruolo della vittima", in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. VI, N. 3, Settembre-Dicembre 2012, p. 70.

[45] Per gli Stati Uniti si vedano, ad esempio, le ricerche condotte dal *Crimes Against Children Research Center* dell'università del New Hampshire e, in particolare, i risultati degli *Youth Internet Safety Surveys* condotti nel 2000, 2005 e 2010, Jones L. M., Mitchell K. J., Finkelhor D., ''Trends in Youth Internet Victimization: findings from three Youth Internet Safety Surveys 2000–2010", in *Journal of Adolescent Health*, Vol. 50, N. 2, 2012, pp. 179–186. Per un'analisi della vittimizzazione online dei minori nel contesto europeo si veda il progetto *Eu Kids Online*, uno studio finanziato nell'ambito del programma europeo *Safer Internet* e condotto da un gruppo di ricercatori provenienti da una ventina di Paesi europei, Livingstone *et al.*, *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, London, 2011 disponibile alla pagina http://eprints.lse.ac.uk/33731/. Per un'analisi della vittimizzazione online attraverso una ricerca condotta in ambito scolastico si veda Bisi R., Ceccaroli G., Sette R., *Il tuo Web. Adolscenti e social network*, Wolters Kluwer-Cedam, Padova, 2016.

[46] Bossler A. M., Holt T. J., "On-line activities, guardianship, and malware infection: an examination of routine activities theory", in *International Journal of Cyber Criminology*, Vol. 3, N. 1, 2009, pp. 400–420.

nell'ambito delle inchieste condotte dagli istituti nazionali di statistica.

Ciononostante, diversi aspetti problematici possono essere identificati anche per quanto riguarda questi strumenti di rilevazione. In primo luogo, l'introduzione di questioni concernenti la vittimizzazione legata alla Rete non è una pratica adottata da tutti i Paesi che si avvalgono di queste tecniche di misura. Negli Stati Uniti, ad esempio, il *National Crime Victimization Survey* (NCVS) non prevede nel questionario principale alcuna domanda in merito alla cybercriminalità. Se è vero che degli studi complementari sono stati realizzati sullo *stalking* e l'utilizzo improprio di dati personali associato anche a Internet, in realtà si tratta di analisi tematiche puntuali e non costanti nel tempo[47]. Un'eccezione è rappresentata dal *National Survey of Children's Exposition to Violence* (NatSCEV) che, tuttavia, fornisce informazioni solamente in merito ai minori vittime di delitti digitali. Inoltre, anche qualora i dati siano disponibili, le comparazioni nazionali appaiono complesse in ragione della diversa metodologia e dei differenti sistemi di classificazione adottati per i fenomeni afferenti alla cybercriminalità[48].

A questi aspetti si associano poi delle considerazioni in merito ai limiti strutturali e metodologici delle inchieste di vittimizzazione[49] che divengono ancora più pregnanti in materia di delitti digitali. Questi strumenti, infatti, non possono essere utilizzati per analizzare gli eventi in cui non ci sia una vittima diretta o individuale, come ad esempio nelle ipotesi di apologia di reato e di *hate crime* online. Nella maggioranza dei casi poi s'intervistano le persone a partire da una determinata soglia di età (14, 15 o 16 anni), aspetto che pertanto esclude qualsiasi analisi sulle forme di vittimizzazione online contro i pre-adolescenti. In questo caso, di fondamentale importanza sono allora le ricerche condotte dalla comunità accademica i cui lavori, da un lato, si sono particolarmente focalizzati sulla vittimizzazione online dei minori, ma dall'altro sono puntuali e non necessariamente ripetuti nel tempo. A prescindere da chi realizzi l'inchiesta o dal campione studiato, è inoltre importante ricordare che le risposte si basano sulle percezioni degli intervistati e, in particolare, sulla loro capacità di identificare come criminale un determinato evento rispetto al quale stimarsi vittima. Nell'ambito della cybercriminalità, questi processi di identificazione e attribuzione sono resi ancora più complessi dal fatto che la persona può non essere conscia di essere stata vittima di un delitto digitale, come è spesso il caso per gli eventi afferenti all'*hacking*. Infine, questo tipo di inchieste tende spesso ad attribuire agli intervistati un *savoir-faire* tecnologico in merito alla qualificazione dell'esperienza di vittimizzazione, come ad esempio per le questioni sui virus informatici, competenza che invece non è necessariamente posseduta da tutti i soggetti studiati[50].

Pertanto, se le inchieste di vittimizzazione hanno rappresentano un indubbio contributo allo studio della cybercriminalità e delle sue vittime, i risultati ottenuti devono essere analizzati con precauzione e, al pari delle statistiche ufficiali, devono essere interpretati tenendo in considerazione il tipo di informazioni che queste indagini sono effettivamente in grado di rilevare. A tal proposito,

[47] Holt T. J., "Cybercrime", *op. cit.*, p. 37.
[48] Wall D. S., "Cybercrimes and the Internet", *op. cit.*, pp. 7-8.
[49] Robert Ph., Zauberman R., *Mesurer la déliquance, op. cit*.; Aebi M. F., *Comment mesurer la délinquance ?, op. cit*., pp. 41-43.
[50] Bossler A. M., Holt T. J., "On-line activities, guardianship, and malware infection: an examination of routine activities theory", *op. cit.*; Benbouzid B., Ventre D., "Pour une sociologie du crime en ligne. Hackers malveillants, cybervictimations, traces du web et reconfigurations du policing", in *Réseaux*, Vol. 3, N. 197-198, 2016, p. 17.

si sottolinea come questo metodo di ricerca non fornisca in realtà la misura della criminalità "reale", ma piuttosto rappresenti un'altra fonte per studiare un problema estremamente articolato a partire dal punto di vista di un attore sociale particolare: la vittima[51].

3.3 Le inchieste sulla delinquenza auto-rivelata.

Nell'ambito degli studi criminologici di fondamentale importanza sono inoltre le indagini sulla delinquenza auto-riportata o auto-rivelata, in cui "s'interrogano campioni rappresentativi di persone in merito ai comportamenti devianti o delittuosi eventualmente commessi"[52] attraverso un questionario somministrato alla presenza del ricercatore, durante un'intervista telefonica o secondo modalità di auto-compilazione, ad esempio in un ambiente specifico (le classi scolastiche) o in seguito ad invio postale o telematico. Realizzati a partire dagli anni '50 negli Stati Uniti[53], questi strumenti di rilevazione forniscono delle informazioni dettagliate su determinati comportamenti devianti e criminali, così come sulle caratteristiche sociodemografiche e gli stili di vita degli autori di reato, e ciò indipendentemente dalle informazioni tratte dalle statistiche ufficiali e dai problemi di costruzione giuridica[54]. Sebbene non consentano di avere una misura precisa della criminalità, queste inchieste hanno avuto un impatto significativo sullo sviluppo dei modelli teorici in ambito criminologico rimettendo in questione l'immagine, predominante nella seconda metà del secolo scorso, del delinquente come uomo giovane, appartenente a determinate minoranze etniche e dal basso status socio-economico[55]. Tuttavia, le indagini sulla delinquenza auto-riportata si sono rivelate degli strumenti adeguati soprattutto per analizzare le pratiche devianti dei minori e dei giovani, per condurre degli studi in alcuni contesti specifici come il carcere, per esaminare gruppi particolari come i tossicomani o per studiare le condotte associate al consumo di sostanze stupefacenti, mentre il loro uso è spesso contestato per studiare la prevalenza della criminalità nella popolazione più in generale[56]. È in questa prospettiva, ad esempio, che questo strumento di rilevazione è stato prevalentemente utilizzato nell'ambito degli studi condotti da organismi pubblici[57], sebbene le questioni sulla cybercriminalità non siano in genere affrontate.

Infatti, per avere delle informazioni più dettagliate in merito è indispensabile analizzare gli studi condotti dalla comunità accademica i cui lavori di ricerca, fondati su quest'approccio metodologico, hanno contribuito in maniera significativa alla comprensione dei fenomeni devianti legati alla Rete. È il caso, ad esempio, delle condotte di *hacking,* delle

[51] Robert Ph. *et al*., *Les comptes du crime. Les délinquances en France et leurs mesures*, *op. cit*., pp. 26-27.

[52] Mucchielli L., "Enquêter sur la délinquance. Réflexions méthodologique et épistémologiques", *op. cit.*, p. 57.

[53] Inaugurata tra gli anni '40 e '50 negli Stati Uniti, questa tecnica di ricerca comincia a diffondersi in Europa durante gli anni '60, in particolare grazie alle ricerche di West e Farrington, ma è solamente a partire dalla fine degli anni '80 che l'inchiesta sulla delinquenza auto-rivelata s'impone sul panorama scientifico, soprattutto in seguito al primo *International Self-Report Delinquency Study* condotto in undici paesi europei. Per maggiori approfondimenti si veda Aebi M. F., Jaquier V., "Les sondages de délinquance autoreportée : origines, fiabilité et validité", in *Déviance et Société*, Vol. 32, N. 2, 2008, pp. 207-211.

[54] *Ibidem*, p. 222.

[55] *Ibidem*, pp. 208-209.

[56] *Ibidem*, p. 216; Robert Ph. *et al*., *Les comptes du crime. Les délinquances en France et leurs mesures*, *op. cit*., p. 26.

[57] Per gli Stati Uniti, ad esempio, si veda il *National Longitudinal Survey of Youth* (NLSY) o il *National Youth Survey* (NYS); per il Regno Unito un esempio è il *Crime Survey for England & Wales* (CSEW) che, oltre alle domande sulle esperienze di vittimizzazione, prevede altresì una parte dedicata alle dichiarazioni concernenti il consumo di sostanze stupefacenti, acquistate anche attraverso la Rete, e dirette a tutto il campione composto da persone aventi almeno 16 anni. In Francia questo tipo di studi sono spesso realizzati nell'ambito d'indagini più vaste relative allo stato di salute della popolazione, come nel caso del "Baromètre Santé" dell'*Institut National de Prévention et d'Education pour la Santé*, ma le questioni sulla cybercriminalità non sono per il momento previste.

pratiche di pirateria digitale e delle varie forme di cyber-violenza, come lo *stalking*, il bullismo e le molestie attraverso Internet[58]. Nella maggioranza dei casi questo tipo di ricerche sono condotte con campioni composti di minori o studenti universitari e, in molte ipotesi, interrogano i partecipanti non solamente sulla loro propensione ad essere autori di determinate condotte devianti o criminali, ma altresì sulle esperienze di vittimizzazione online eventualmente vissute. Si tratta di un approccio particolarmente fecondo che ha permesso di rilevare, in particolare per i fenomeni di molestie e di bullismo online, come il fatto di essere coinvolti in una condotta associata alla cybercriminalità sia fortemente correlato al rischio di vittimizzazione, così come l'inverso[59].

Nonostante l'indubbio contributo di questi studi, differenti aspetti critici meritano di essere sottolineati. In primo luogo, si tratta di ricerche focalizzate in prevalenza su gruppi specifici di persone, come gli studenti, i cui risultati quindi non possono essere generalizzati. Inoltre, in taluni casi i risultati ottenuti non sono nemmeno generalizzabili alla specifica popolazione di riferimento a causa dell'uso di campioni di convenienza[60], vale a dire costruiti a prescindere da un qualsiasi disegno di campionamento.

A questi aspetti si associano poi delle considerazioni di natura metodologica che riguardano in realtà non solo le indagini di delinquenza auto-rivelata o di vittimizzazione, ma le inchieste campionarie più in generale. Al di là delle riflessioni di ordine epistemologico e in merito alle strategie di campionamento, la letteratura in materia ha infatti da tempo sottolineato come i termini impiegati, la formulazione e l'ordine delle domande e delle risposte di un questionario esercitino delle influenze sulle informazioni rilevate attraverso questo strumento[61]. In tal senso, uno dei presupposti alla base delle inchieste campionarie e degli sforzi di standardizzazione è che le domande abbiano un significato e soprattutto lo stesso significato per tutti gli intervistati. Tuttavia, come già notavano Bourdieu e colleghi, "supporre che la stessa questione abbia lo stesso senso per soggetti sociali separati da differenze di cultura associate alle appartenenze di classe, è ignorare che i differenti linguaggi non differiscono solamente per l'estensione del lessico o il grado di astrazione ma anche per le tematiche e le problematiche che veicolano"[62]. In questa prospettiva, si è già avuto modo di sottolineare come nell'ambito delle ricerche sulla cybercriminalità uno degli aspetti più problematici riguardi proprio la corrispondenza tra l'universo di senso del ricercatore e quello dell'intervistato, è ciò al di là delle diverse competenze linguistiche. Ad esempio, nel corso di una ricerca sulle forme di vittimizzazione e le

[58] Rogers M., Smoak N. D., Jia L., ''Self-reported deviant computer behavior: a big-5 moral choice, and manipulative exploitive behavior analysis", in *Deviant Behavior*, N. 27, 2006, p. 245–268; Higgins G. E., Marcum C. D., *Digital piracy: an integrated theoretical approach*, Carolina Academic Press, Raleigh, 2011; Reyns B. W., Henson B., Fisher B. S., ''Stalking in the twilight zone: extent of cyberstalking victimization and offending among college students'' in *Deviant Behavior*, Vol. 33, N. 1, 2012, pp. 1-25; Livingstone *et al.*, *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*, *op. cit.*

[59] Holt J. T, Bossler A. M., "An assessment of the current state of cybercrime scholarship", in *Deviant Behavior*, N. 35, 2014, p. 24; Ybarra M. *et al.*, "Examining characteristics and associated distress related to Internet harassment: findings from the Second Youth Internet Safety Survey", in *Pediatrics*, Vol. 118, N. 4, 2006, pp. 1169-1177.

[60] Holt T. J., "Cybercrime", *op. cit.*, p. 38.

[61] Per una sintesi, Grémy J.-P., "Les expériences françaises sur la formulation des questions d'enquête. Résultats d'un premier inventaire", in *Revue française de sociologie*, Vol. 4, 1987, pp. 567-599.

[62] Bourdieu P., Chamboredon J.-C., Passeron J.-C., *Le Métier de sociologue*, Mouton, Berlin/New York, 2005 (5° edizione), p. 63.

condotte devianti associate alla Rete da noi condotta in ambito scolastico[63], alla domanda "*Usi Internet?*" alcuni minori (9-10 anni) del gruppo con cui si è testato il questionario di ricerca sono rimasti perplessi in quanto non in grado di comprendere cosa si volesse indicare con il termine "Internet". Interrogati sul punto alcuni ragazzi hanno quindi chiesto "*Maestra, vuole dire Facebook, Youtube e Snap?*"[64], sottolineando così come l'universo della Rete fosse da essi percepito e definito a partire dalle pratiche e dalle applicazioni più utilizzate e non secondo i termini e le categorie impiegati dal ricercatore. Quest'esempio illustra allora come sia spesso difficile per lo studioso liberarsi dell'illusione che delle espressioni, anche di uso corrente come "Internet", siano univoche per tutta la popolazione di riferimento e ciò appare ancora più pregnante nel caso di ambiti specifici e per certi versi tecnici come quelli dei delitti digitali. Inoltre, anche la stessa scelta delle questioni da porre è intrisa di aspetti problematici, in quanto talvolta le domande possono non solo essere diversamente interpretate, ma anche non avere proprio alcun significato per gli intervistati. Nel fatto di porre la stessa domanda a tutti, sottolineava Bourdieu, è implicita l'ipotesi "che ci sia un consenso sui problemi, altrimenti detto, che ci sia un accordo sulle questioni che meritano di essere poste"[65], aspetto che in realtà non è per niente scontato. Ad esempio, sempre nel corso della ricerca in precedenza citata, alla domanda "*Nel corso degli ultimi dodici mesi, hai inviato messaggi sessuali di qualsiasi genere su Internet?*" più di uno studente delle scuole superiori non si spiegava la ragione della questione in quanto, come nota uno dei minori, "*è normale, non ci vedo alcun problema. Non capisco perché ci fa questa domanda. Io abito a * e la mia ragazza a * e quindi come facciamo? Beh…usiamo Skype, è normale!*"[66].

In questa disamina non possono poi mancare alcune considerazioni in merito all'attendibilità delle risposte e del comportamento verbale degli intervistati. Nell'ambito delle inchieste sulla delinquenza auto-riportata, infatti, uno dei principali limiti evidenziati concerne la desiderabilità sociale delle risposte, ossia la "valutazione, socialmente condivisa, che in una certa cultura viene data ad un certo atteggiamento o comportamento individuale"[67]. In questa prospettiva, "considerando che la criminalità è considerata un comportamento contrario alle norme della vita in società, [le persone, n.d.a.] possono essere particolarmente reticenti a svelare i propri delitti"[68] e, in questo modo, le risposte rilevate possono non sempre corrispondere ai reati effettivamente compiuti dagli intervistati. Vi possono essere poi delle imprecisioni legate a problemi di memoria, alla difficoltà di datare un determinato evento o di attribuirgli un carattere illecito. È il caso, ad esempio, delle condotte legate al *download* o allo *streaming* di contenuti protetti dal diritto d'autore che sono spesso considerate legali e, in tal senso, non dichiarate nel corso di questo tipo di ricerche. Questi aspetti, e in particolare la desiderabilità

[63] Si tratta di una ricerca in merito alle forme di vittimizzazione e alle condotte devianti associate alla Rete realizzata con un gruppo di 900 studenti delle scuole elementari, medie e superiori (9-17 anni) di un dipartimento del sud-ovest della Francia (*Les enfants face aux écrans*, 2013-2015). Per una sintesi dei risultati, si veda Macilotti G., "La jeunesse à l'ère du numérique : pratiques, exposition au risque et victimation. Une étude auprès de la Communauté d'Agglomération du Grand Rodez", in *Les Cahiers de la Sécurité et de la Justice*, N. 37, 2017, pp. 110-129.

[64] La domanda è stata posta da alcuni minori del gruppo con cui si è testato il questionario per la ricerca *Les enfants face aux écrans* da noi condotta. La citazione, in particolare, è di un bambino di 10 anni.

[65] Bourdieu P., *Questions de sociologie*, Minuit, Paris, 1984, p. 222.

[66] Studente di liceo, 16 anni, partecipante alla ricerca *Les enfants face aux écrans* da noi condotta.

[67] Corbetta P., *Metodologia e tecniche della ricerca sociale, op. cit.*, p. 180.

[68] Aebi M. F., *Comment mesurer la délinquance ?, op. cit.*, p. 37.

sociale, possono inoltre essere influenzati dalle modalità di somministrazione del questionario[69] e, più in generale, da diversi parametri della situazione di ricerca, come l'interazione fra l'intervistato e il ricercatore, la distanza sociale fra di essi e le loro rispettive caratteristiche (età, sesso, classe sociale, etnia, ecc.). A tal proposito, Mauger sottolinea come nell'ambito delle inchieste attraverso questionario l'analisi della situazione di ricerca sia stata spesso trascurata. Al contrario, l'autore nota come sia importante prendere in considerazione "la situazione sociale particolare che è la situazione di ricerca, le condizioni sociali della sua instaurazione, le forme del suo sviluppo e di individuare gli effetti di questa situazione particolare sui 'materiali' raccolti"[70]. La letteratura sulle indagini di delinquenza auto-rivelata mostra in tal senso come non solo "la semplice presenza del ricercatore possa limitare la menzione di comportamenti socialmente poco desiderabili o d'informazioni di natura sensibile", ma come le stesse caratteristiche dello studioso possano "interagire con il soggetto dell'intervista e produrre delle distorsioni specifiche sulle risposte fornite da quest'ultimo"[71], ad esempio attraverso la negazione di determinate condotte devianti o stigmatizzate in quanto in grado di far "perdere la faccia"[72] alla persona. I ricercatori sono spesso consapevoli di questi aspetti e, generalmente, i questionari prevedono non solo una serie di domande filtro e di verifica per testare l'attendibilità delle risposte, ma altresì delle modalità di somministrazione che garantiscano la percezione di un maggior anonimato, come nel caso dell'auto-compilazione anche attraverso l'utilizzo delle nuove tecnologie. In quest'ultimo caso, tuttavia, è opportuno precisare come proprio la relativa tracciabilità delle informazioni online possa suscitare reticenze in taluni intervistati e, come si vedrà in seguito, quest'aspetto deve essere tenuto in considerazione non solo per quanto concerne il disegno della ricerca, ma anche per quanto riguarda l'analisi delle informazioni rilevate.

Le considerazioni svolte ci permettono pertanto di sottolineare come anche per le inchieste sulla delinquenza auto-rivelata ci si confronti con misure statistiche che, da un lato, sono il risultato delle loro specifiche condizioni di produzione e, dall'altro, forniscono un'immagine della criminalità a partire da un punto di vista particolare: quello dell'autore di reato. Infatti, che si tratti di statistiche di "polizia", di inchieste di vittimizzazione o di delinquenza auto-rivelata, le misure che si ottengono dipendono dalla perspettiva di analisi adottata. Ciò non significa che non si possa ottenere alcuna informazione specifica sulla scia di un perfetto relativismo, ma riconoscere che la conoscenza di un fenomeno complesso come quello criminale non possa basarsi su un'unica misura, ma piuttosto sull'utilizzazione e se possibile sull'integrazione di differenti fonti, "terreni" e strumenti d'indagine[73].

In quest'ottica, ad esempio, la ricerca accademica ha non solo adottato degli approcci di tipo "empatico" e "numerico" per studiare gli attori e le pratiche associate alla cybercriminalità, ma ha anche progressivamente adattato i metodi "tradizionali" della ricerca sociale alle nuove opportunità offerte dalla dimensione digitale.

[69] Aebi M. F., Jaquier V., "Les sondages de délinquance autoreportée : origines, fiabilité et validité", *op. cit.*, p. 216.
[70] Mauger M., "Enquêter en milieu populaire", in *Genèses*, N. 6, 1991, p. 129.
[71] Aebi M. F., Jaquier V., "Les sondages de délinquance autoreportée : origines, fiabilité et validité", *op. cit.*, p. 215.
[72] Goffman E., *Les Rites d'interaction*, Minuit, Paris, 1974.
[73] Robert Ph. *et al.*, *Les comptes du crime. Les délinquances en France et leurs mesures, op. cit.*, p. 27.

4. Lo studio della cybercriminalità: approcci "empatici" e analisi delle tracce digitali.

L'emergenza di spazi di comunicazione e di interazione online, l'utilizzo sempre più crescente dei media sociali, il proliferare di gruppi e di comunità virtuali rappresentano un valido ausilio per la ricerca, soprattutto per raggiungere realtà sommerse e soggetti poco propensi a svelare la propria identità, così come tipologie specifiche di partecipanti che in gruppo online possono essere coinvolti talvolta più facilmente[74]. In tal senso, una delle maggiori particolarità del cyberspazio concerne la possibilità di studiare gli utenti e le loro pratiche non solo avvalendosi delle potenzialità della comunicazione digitale, ma altresì sfruttando le informazioni e le tracce lasciate online. Quest'ultima nozione, infatti, è al centro di numerose applicazioni e riflessioni che riguardano tanto le discipline informatiche quanto le scienze sociali. Secondo queste ultime, in particolare, la definizione di traccia digitale rinvia a due approcci complementari che si fondano sulle proprietà ad essa riconosciute. Una prima prospettiva analizza questa nozione come interazione fra l'uomo e la macchina e, in tal senso, è vista come il risultato dei segni lasciati dalle attività umane nel cyberspazio. Un secondo approccio privilegia invece il concetto di evento e, in quest'ottica, il termine in esame designa una sequenza di avvenimenti ordinati associati alla Rete[75]. A prescindere dall'ottica adottata, le tracce digitali utilizzate a fini di ricerca possono essere di tipo esplicito, vale a dire risultanti dell'agire intenzionale dell'utente attraverso la produzione di scritti e altri tipi di documenti (come ad esempio immagini, video, *tweets*, ecc.), o possono essere di natura implicita, aspetto che si riferisce ai segni che il soggetto più o meno inconsapevolmente lascia online navigando sugli spazi virtuali e utilizzando le applicazioni e i servizi digitali (ad esempio i file di log, i *cookies*, gli indirizzi IP, ecc.)[76].

È in questa prospettiva, pertanto, che si sottolinea come il cyberspazio possa essere al contempo considerato uno "strumento", un "luogo" e un "oggetto" della ricerca sociale [77]. Gli studi sulla cybercriminalità possono allora realizzarsi "attraverso" la dimensione digitale, intesa come mezzo per intervistare ad esempio un gruppo di *hackers*, per somministrare loro dei questionari o per implementare nuove modalità di raccolta delle informazioni concernenti la diffusione di virus informatici. Le ricerche possono essere condotte "nel" cyberspazio, visto come nuovo "campo" dove analizzare, per esempio, le pratiche, le norme e i valori che caratterizzano le comunità dedite alla pirateria digitale. Infine, la dimensione virtuale può essere considerata come "oggetto" stesso della ricerca sociale, ad esempio qualora si vogliano analizzarne gli effetti dal punto di vista della strutturazione online dei mercati di stupefacenti. Gli studi sulla cybercriminalità si sono ampiamente avvalsi di tutte queste potenzialità e declinazioni della Rete, integrando in taluni casi differenti fonti e approcci.

4.1 Intervistare gli attori della cybercriminalità.

L'intervista qualitativa è generalmente considerata come una delle tecniche privilegiate per accedere alla prospettiva dei soggetti studiati, per analizzare il senso che donano alle loro pratiche, per coglierne le

[74] Fedeli L., *La ricerca scientifica al tempo dei social media*, FrancoAngeli, Milano, 2017, pp. 53-54.

[75] Serres A., "Problématiques de la trace à l'heure du numérique", in *Sens-Dessous*, Vol. 1, N. 10, 2012, p. 89.

[76] Ertzscheid O., Gallezot G., Simonnot B., "A la recherche de la 'mémoire' du web : sédiments, traces et temporalités des documents en ligne", in Barats C. (a cura di), *Manuel d'analyse du web*, Armand Colin, Paris, 2013, p. 55.

[77] Sul punto si veda Barats C. (a cura di), *Manuel d'analyse du web*, *op.cit.*

categorie mentali e le interpretazioni secondo un approccio comprensivo della realtà sociale[78].

Nell'ambito degli studi sulla cybercriminalità la realizzazione di interviste qualitative caratterizzate dalla compresenza di ricercatore e intervistato ha permesso, ad esempio, di ottenere le prime informazioni in merito alle condotte associate alla pedopornografia e alle motivazioni sottese all'agire degli autori, di approfondire le tecniche di neutralizzazione e di razionalizzazione impiegate nel campo del *file sharing* e della pirateria digitale, così come di analizzare le costruzioni ideologiche, le motivazioni e le traiettorie biografiche degli informatici appartenenti ad alcune comunità di *hackers*[79]. Tuttavia, è opportuno precisare come non sia così semplice trovare degli autori di reati digitali disposti a farsi intervistare alla presenza del ricercatore e, in maniera più generale, a partecipare ad una ricerca accademica. Questi ultimi, infatti, spesso temono di vedere svelata la propria identità e, eventualmente, di essere identificati dalle forze di polizia. Inoltre, lo stesso processo di selezione degli autori da intervistare presenta differenti aspetti problematici associati anche ai differenti stratagemmi di natura umana e tecnica adottati dagli utenti per proteggere l'anonimato e le condotte illecite realizzate. Una delle conseguenze principali è che gli studi possano allora focalizzarsi su soggetti che non sono rappresentativi o informativi del gruppo di autori che in realtà si desidera analizzare. Esemplificative, in tal senso, sono le ricerche condotte sugli *hackers* attraverso interviste qualitative e questionari somministrati alla presenza del ricercatore in occasione dei principali eventi del settore. In questi casi, infatti, molti degli intervistati "sono dei professionisti della sicurezza che non sono rappresentativi dei *black hat hackers*"[80], vale a dire degli esperti informatici che utilizzano le loro competenze tecniche per commettere delle infrazioni secondo degli intenti malevoli. Diverse strategie sono state quindi adottate per cercare di superare queste criticità, alcune delle quali meritano di essere approfondite.

In primo luogo, gli studiosi possono avvalersi delle informazioni presenti online e di alcuni servizi informatici per individuare i possibili intervistati, contattarli e realizzare l'intervista secondo delle modalità che garantiscano un maggior anonimato. A partire generalmente dall'osservazione degli spazi in Rete specializzati sulla tematica oggetto della ricerca o frequentati dal gruppo di attori che s'intende studiare, i ricercatori possono utilizzare degli strumenti di comunicazione asincrona, come mail e forum, o di discussione in tempo reale, come messaggeria istantanea e comunicazioni via webcam, per presentare il lavoro di ricerca e realizzare eventualmente l'intervista. Quest'approccio, ad esempio, si è rivelato particolarmente proficuo per evidenziare il carattere comunitario dell'ambiente dell'*hacking* e per studiare le caratteristiche delle subculture associate, così come per approfondire le pratiche di pirateria digitale o esaminare l'utilizzo e gli effetti delle nuove tecnologie per quanto

[78] Corbetta P., *Metodologia e tecniche della ricerca sociale, op. cit*., pp. 406-435.

[79] Quayle E., Taylor M., ''Child pornography and the Internet: perpetuating a cycle of abuse", in *Deviant Behavior*, Vol. 23, N. 2, 2002, p. 331-361; Moore R., "Digital file sharing: an examination of neutralization and rationalization techniques employed by digital file shares", in Jaishankar K. (a cura di), *Cyber Criminology. Exploring Internet crimes and criminal behavior*, CRC Press, New York, 2011, p. 209-225; Auray N., Kaminsky D., "Les trajectoires de professionnalisation des hackers : la double vie des professionnels de la sécurité", in *Annales des Télécommunications*, Vol. 62, N. 11-12, 2007, pp. 1313-1327.

[80] Décary-Hétu D., Dupont B., Fortin F., "Policing the hackers by hacking them: studying online deviants in IRC chat rooms", Masys A. J. (a cura di), *Networks and Network Analysis for Defence and Security*, Springer, New York, 2014, p. 65.

concerne l'organizzazione online della prostituzione[81]. La letteratura sottolinea in tal senso come la realizzazione di interviste attraverso l'uso delle nuove tecnologie presenti diversi vantaggi[82]. Al di là del fatto di rendere più semplice la scelta del momento dell'intervista e la trascrizione dell'interazione, quest'approccio sembra avere degli effetti positivi per quanto concerne il tasso di partecipazione dei soggetti alla ricerca e la raccolta di commenti più attendibili. L'interazione mediata dallo schermo e dalla dimensione digitale consentirebbe, infatti, di ridurre le preoccupazioni degli intervistati in merito al fatto di "perdere la faccia" e di mantenere una determinata presentazione di sé durante l'interazione.

Ciononostante, anche l'intervista associata all'uso delle nuove tecnologie non è esente da aspetti problematici. Ad esempio, soprattutto qualora non ci sia alcun contatto visivo fra ricercatore e intervistato, lo studioso non ha la possibilità di analizzare la comunicazione non verbale tipica dell'interazione in presenza, così come non può essere certo della reale identità della persona. A questi differenti aspetti si associano poi delle considerazioni in merito all'attendibilità delle risposte e del comportamento verbale degli intervistati, che presentano molti punti in comune con quanto già evidenziato per le inchieste sulla delinquenza auto-rivelata. Inoltre, a seconda del tipo di devianza online analizzata, l'accesso agli intervistati può rivelarsi particolarmente difficile e, anche qualora il ricercatore identifichi le persone da studiare, convincerle a discutere di aspetti concernenti le loro attività illecite e la loro vita richiede notevoli sforzi, nonché differenti strategie finalizzate a guadagnarne la fiducia. Si tratta, infatti, di soggetti che proprio per la natura illegale delle condotte agite sono particolarmente cauti nelle interazioni online, soprattutto per paura di essere identificati o di confrontarsi non con un ricercatore ma con un operatore di polizia. Ad esempio, in uno studio condotto su alcune comunità virtuali dedicate alla discussione sulla coltivazione di cannabis, Potter racconta come i membri consigliassero di non svolgere l'intervista online, ma piuttosto di rendere disponibili le questioni all'interno del gruppo lasciando poi ai partecipanti la scelta di stamparle e di spedire le risposte attraverso la posta ordinaria, ovviamente da un ufficio lontano dalla città di residenza. In questi casi, sottolinea l'autore, una strategia che consente di vincere, almeno in parte, la diffidenza dei soggetti di studio è di realizzare le interviste nell'ambito di un approccio etnografico fondato su periodi di osservazione partecipante online e offline[83]. A prescindere dalla realizzazione di ricerche in immersione, è tuttavia opportuno precisare come l'interazione con gli autori di determinati reati possa presentare aspetti problematici per la sicurezza stessa del ricercatore, come raccontano Holt e Copes a proposito di un intervistato che inviò un virus informatico a uno dei

[81] Taylor P.A., *Hackers: Crime in the digital sublime*, Routledge, New York, 1999; Holt T. J, Copes H., "Transferring subcultural knowledge online: practices and beliefs of persistent digital pirates", in *Deviant Behavior*, Vol. 31, N. 7, 2010, pp. 625-654; Finn M. A., Stalans L J., "How targeted enforcement shapes marketing decisions of pimps: evidence of displacement and innovation", in *Victims and Offenders*, Vol. 11, N.4, 2016, pp. 578-599.

[82] Holt T. J., "Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data", in *Journal of Criminal Justice Education*, Vol. 21, N. 4, 2010, pp. 471-472; Kivitz J., "Online interviewing and the research relationship", in Hine C. (a cura di), *Virtual methods: issues in social research on the Internet*, Berg, Oxford, 2005, pp. 35-50.

[83] Potter G. R., "Real gates to virtual fields: integrating online and offline ethnography in studying cannabis cultivation and reflections on the applicability of this approach in criminological ethnography more generally", in *Methodological Innovations*, Vol. 10, N. 1, 2017, pp. 1-11.

due studiosi in quanto non soddisfatto delle questioni poste[84].

Un'altra possibilità è allora quella di intervistare non direttamente la popolazione oggetto dello studio, ma degli osservatori privilegiati, ossia dei soggetti che grazie ad esempio alla loro professione hanno una conoscenza diretta e una visione approfondita dell'ambito di analisi[85]. In tal senso, si possono ricordare gli operatori delle forze di polizia e, in particolare, le unità specializzate nel contrasto alla cybercriminalità create nel corso degli ultimi decenni al fine di adattare l'azione di contrasto alle nuove sfide offerte dalla Rete. Questo tipo di approccio, ad esempio, si è rivelato particolarmente utile per studiare i fenomeni di abuso sessuale su minori e, in particolare, per analizzare le pratiche, le caratteristiche e gli autori di condotte legate alla pornografia minorile[86]. Inoltre, le ricerche realizzate "attraverso" gli operatori del controllo sociale, soprattutto se condotte nell'ambito di periodi di osservazione diretta, possono consentire al ricercatore di avere accesso a dei contenuti non disponibili liberamente online, come nel caso delle conversazioni fra gruppi di *hackers* realizzate in spazi riservati, dei contenuti pedopornografici detenuti nei supporti digitali degli indagati o delle interazioni nell'ambito di processi di adescamento online di minore[87].

Tuttavia, anche in queste ipotesi, differenti aspetti devono essere considerati al fine di analizzare in maniera riflessiva i risultati associati a questa tecnica di ricerca. Dapprima, è opportuno ricordare che le dichiarazioni rilasciate nel corso delle interviste riflettono non necessariamente un'immagine precisa dei delitti digitali, ma piuttosto la rappresentazione che degli stessi si fanno gli operatori di polizia anche rispetto al tipo di indagini da essi svolto. Inoltre, come in ogni interazione sociale, l'attore può più o meno coscientemente tentare di dare una "buona immagine" di sé e fornire delle risposte che non gli facciano "perdere la faccia". In una ricerca da noi condotta, ad esempio, un operatore di polizia interrogato in merito agli indagati per reati di pedopornografia invece di fornirci una risposta a partire della sua esperienza personale e lavorativa, ci presenta la definizione e le caratteristiche del concetto di pedofilia secondo la disciplina psichiatrica mostrandoci, al contempo, un documento da lui stesso redatto per l'intervista:

"Vede? Mi sono preparato, ho preso direttamente dal DSM [manuale diagnostico e statistico dei disturbi mentali, n.d.a] *per essere sicuro"*[88].

Lungi dall'essere un caso isolato, questo tipo di risposte è esemplificativo dell'attitudine di alcuni intervistati a rispondere sul proprio lavoro o in merito a un determinato fenomeno presentando una sorta di "teoria della pratica", basata su quello che si dovrebbe fare o su quello che il soggetto pensa si attenda il ricercatore[89]. Su un piano per certi versi

[84] Holt T. J, Copes H., "Transferring subcultural knowledge online: practices and beliefs of persistent digital pirates", *op. cit.*

[85] Corbetta P., *Metodologia e tecniche della ricerca sociale*, *op. cit.*, pp. 420-421.

[86] Per tutti si veda Wolak J., Finkelhor D., Mitchell K. J., "Child pornography possessors: trends in offender and case characteristics", in *Sexual abuse: A Journal of Research and Treatment*, Vol. 23, N. 1, 2011, pp. 22-42. In questo caso, ad esempio, la ricerca ha previsto in un primo momento la somministrazione di un questionario a un campione di operatori di polizia e, in seguito, la realizzazione di interviste telefoniche con alcuni componenti il campione.

[87] Décary-Hétu D., Dupont B., Fortin F., "Policing the hackers by hacking them: studying online deviants in IRC chat rooms", *op. cit.*; Fortin F., Corriveau P., *Who is Bob_34? Investigating child cyberpornography*, UBC Press, Vancouver-Toronto, 2015; Macilotti G., "La pedopornografia e l'adescamento online di minori", in Balloni A., Bisi R., Sette R., *Principi di criminologia applicata. Criminalità, controllo, sicurezza*, Wolters Kluwer-Cedam, Padova, 2015, pp. 279-315.

[88] Agente italiano, Polizia Postale e delle Comunicazioni.

[89] Mucchielli L., "Enquêter sur la délinquance. Réflexions méthodologique et épistémologiques", *op. cit.*, pp. 60-61.

simile, un agente dei servizi di *intelligence* francese ci fa notare:

"Anche se non me l'ha chiesto direttamente, ho capito cosa voleva sapere sull'investigazione nel cyber, ma non ho voluto dirglielo. Insomma…lo sa anche lei, il mio lavoro si fonda sul segreto e sul controllo di cosa dico e come lo dico"[90].

L'intervista, infatti, è una situazione socialmente definita in cui lo studioso non detiene il primato dell'osservazione, essendo stesso oggetto di analisi e di anticipazione da parte degli intervistati.

A prescindere che sia svolta con un autore di reato, una vittima o un operatore del controllo sociale, questa tecnica di ricerca non può pertanto essere considerata come un mero passaggio di informazioni fra i soggetti, ma piuttosto come una relazione sociale da cui emergono delle informazioni che non possono essere astratte dai loro contesti di produzione[91]. Come già sottolineato per le inchieste di vittimizzazione e di delinquenza auto-rivelata, il tipo e l'oggetto di ricerca, le attribuzioni di senso, le posture di "prestigio" e di razionalizzazione degli intervistati, la dissimmetria nell'interazione legata alla distanza sociale fra i partecipanti, le loro rispettive rappresentazioni sono tutti elementi significativi sul piano del processo di co-produzione dell'informazione. Gli strumenti dell'indagine sociologica sono infatti delle "tecniche di sociabilità socialmente qualificate"[92] e, in questa prospettiva, l'esame degli esiti di un'intervista domanda di adottare un approccio riflessivo fondato sull'analisi della situazione di ricerca intesa come incontro fra "un'offerta di parola" e "una disposizione a parlare"[93]. Quest'ultima, infatti, anche se si distingue dalla maggior parte degli scambi dell'esistenza ordinaria, resta in definitiva "una relazione sociale che esercita degli effetti (…) sui risultati ottenuti" che è pertanto necessario conoscere, controllare e analizzare[94].

Infine, come sottolinea Mucchielli, il ricercatore che si limiti ad adottare solamente la tecnica dell'intervista si confronta a due rischi maggiori. In primo luogo, di ridurre la conoscenza del fenomeno al solo punto di vista presentato dagli intervistati che, come si è visto, risente di tutta una serie di parametri afferenti anche alle caratteristiche di questa particolare relazione sociale. Il secondo rischio può riguardare l'incapacità di analizzare la dimensione situazionale, micro-interattiva e emozionale dei comportamenti devianti, rendendo così difficile restituire le pratiche in una dimensione comprensiva. Per studiare la cybercriminalità così come altri fatti sociali, il consiglio è allora di associare l'intervista all'uso di altre fonti e alla realizzazione, ad esempio, di periodi di osservazione diretta o indiretta sfruttando le opportunità offerte dalla Rete[95].

4.2 Lo studio della cybercriminalità attraverso l'osservazione partecipante in Rete.

Gli approcci fondati sulle tecniche di osservazione partecipante sono da tempo utilizzati nell'ambito dello studio del crimine, in particolare per cogliere

[90] Ufficiale "contro-ingerenza cyber", appartenente ad un servizio di informazione militare francese.

[91] Furlotti R., "L'intervista come relazione significativa", in Cipolla C. (a cura di), *Il ciclo metodologico della ricerca sociale*, *op. cit.*, pp. 170-171; Mauger G., "Sociologie de la situation d'enquête. Une clé d'intelligibilité de l'espace des styles de vie déviants des jeunes des classes populaires", in Boucher M. (a cura di), *Enquêter sur les déviances et la délinquance. Enjeux scientifiques, politiques et déontologiques*, *op. cit.*, pp. 133-135.

[92] Bourdieu P., Chamboredon J.-C., Passeron J.-C., *Le Métier de sociologue*, *op. cit.*, p. 62.

[93] Mauger M., "Enquêter en milieu populaire", *op. cit.*

[94] Bourdieu P., "Comprendre", in Bourdieu P. (a cura di), *La misère du monde*, Seuil, Paris, 1993, pp. 903-939.

[95] Mucchielli L., "Enquêter sur la délinquance. Réflexions méthodologique et épistémologiques", *op. cit.*, pp. 62-63; Holt T. J., "Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data", *op. cit.*; Beaud S., Weber F., *Guide de l'enquête de terrain*, La Découverte, Paris, 2003.

in chiave interpretativa la perspettiva dei soggetti devianti e proporre così un'altra immagine della criminalità rispetto a quella fornita dalle statistiche ufficiali o dalle analisi quantitative di tradizione positivista[96]. In questa prospettiva, il cyberspazio può essere visto come un nuovo "campo" in cui immergersi per analizzare "dal di dentro" un determinato contesto sociale e in cui interagire con i soggetti studiati al fine di descriverne le azioni e di comprenderne le motivazioni[97]. Sebbene meno numerose rispetto gli studi in precedenza citati, alcune ricerche sulla cybercriminalità si sono avvalse non solo delle potenzialità della Rete in termini di comunicazione e interazione, ma anche delle tracce online per studiare gli autori e le pratiche a partire da periodi di osservazione diretta che, soprattutto per gruppi devianti caratterizzati da un forte aspetto comunitario, sono sovente connotati da strategie d'immersione prolungata del ricercatore.

Nell'ambito dello studio dei gruppi di *hackers*, di pirati digitali e di attivisti politici in Rete, ad esempio, gli approcci di tipo etnografico e della *digital ethnography*[98] fondati sull'osservazione partecipante in Rete hanno permesso di analizzare, in una prospettiva comprensiva e interpretativa, le pratiche dei partecipanti, le dinamiche sociali in seno alle comunità, le norme, i valori, le credenze e le giustificazioni prodotti nel corso dei processi di interazione e socializzazione all'interno dei differenti spazi digitali[99]. Esemplificativo, in tal senso, è lo studio etnografico condotto da Gabriella Coleman sugli "hacktivisti" di *Anonymous* nel quale l'autrice ricostruisce la genesi del collettivo, le diverse pratiche e forme d'implicazione dei membri, mostrando come "una rete di *trolls* [sia] diventata una forza essenzialmente consacrata al bene comune"[100]. Oltre all'analisi della subcultura associata agli *Anons*, all'esame delle forme e dei contenuti delle interazioni fra i membri, la ricerca mette in evidenza come il collettivo non presenti in realtà un orientamento e un programma politico chiaro, così come costituisca un fenomeno complesso alla frontiera fra un gruppo deviante, un collettivo militante e una comunità di difensori della libertà di espressione.

Come evidenzia la letteratura, tuttavia, la realizzazione di uno studio fondato sull'approccio etnografico o sulla conduzione di periodi di osservazione partecipante presenta degli aspetti più o meno problematici di ordine metodologico, etico e pratico che devono essere analizzati anche alla luce delle peculiarità della dimensione digitale[101]. In primo luogo, l'immersione prolungata online al fine di partecipare, studiare e comprendere i processi umani e sociali interroga ad esempio i concetti di "partecipazione", "immedesimazione" e "ambiente naturale". Lungi da focalizzarsi su uno spazio definito, l'osservazione in Rete infatti concerne una gamma differenziata di luoghi di ricerca, si caratterizza per la dissolvenza della demarcazione fra spazi fisici e virtuali, si accompagna a delle interazioni sincrone e asincrone, in presenza o mediate dallo "schermo", in cui "'l'ambiente

[96] Si veda, ad esempio, Becker H., *Outsiders. Études de sociologie de la déviance*, Métaillié, Paris, 1985.

[97] Si fa riferimento alla definizione della tecnica dell'osservazione partecipante proposta da Corbetta P., *Metodologia e tecniche della ricerca sociale*, *op. cit.*, pp. 367-368.

[98] Murthy D., "Digital ethnography: an examination of the use of new technologies for social research" in *Sociology*, Vol. 42, N. 5, 2008, pp. 837-855.

[99] Ad esempio, Rehn A., "The politics of contraband: the honor economies of the Warez scene", in *The Journal of Socio-Economics*, V. 33, N. 3, 2004, pp. 359-37. Per una rassegna, Holt T. J., "Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data", *op. cit.*

[100] Coleman G., *Anonymous. Hacker, activiste, faussaire, mouchard, lanceur d'alerte*, Lux, Montréal, 2016, p. 62.

[101] Beaud S., Weber F., *Guide de l'enquête de terrain*, *op. cit.*; Hine C. (a cura di), *Virtual methods: issues in social research on the Internet*, *op. cit*.

naturale' si compone di frammenti non sempre integrati in un unico spazio-temporale"[102]. Questi aspetti si traducono allora in un'immersione prolungata e un investimento anche temporale notevole, tanto per la preparazione del lavoro sul "campo", che per la conduzione dell'osservazione e l'analisi dei materiali raccolti. Inoltre, come per tutte le strategie di ricerca fondate sull'osservazione partecipante, il ricercatore deve essere in grado di identificare il gruppo da studiare, deve ottenerne l'accesso e guadagnare la fiducia dei membri così da poter instaurare un rapporto di interazione personale finalizzato ad analizzarne e comprenderne le azioni, le motivazioni e i valori. Nell'ambito degli studi sulla cybercriminalità, questi differenti aspetti appaiano particolarmente complessi proprio per la necessità degli attori di celare le attività illecite realizzate[103]. Dalla creazione di gruppi ad accesso condizionato, alla predisposizione di regole specifiche per la partecipazione, passando per l'utilizzazione di sistemi di anonimizzazione che consentano di non indicizzare gli spazi online sul *Clear Web*[104], gli autori di reati digitali adottano differenti strategie per dissimulare le loro condotte e la loro presenza in Rete. In questa prospettiva e a seconda del gruppo o del fenomeno che si intende studiare, la preparazione del lavoro sul "campo" dovrà molto probabilmente fondarsi su un'analisi dettagliata di differenti spazi digitali, sull'incrocio di una pluralità di fonti, sullo studio delle pratiche e dei linguaggi propri allo specifico gruppo deviante al fine di "mapparne" la presenza online e di identificare quegli informatori privilegiati che, ad esempio, possono introdurre il ricercatore alla comprensione del contesto sociale oggetto di ricerca e facilitare l'accesso alla comunità virtuale, così come i contatti e le interazioni con i suoi membri. Inoltre, il successo di questo tipo di strategie d'indagine varia in funzione del fenomeno deviante studiato. Determinati gruppi, come ad esempio quelli legati al mondo dell'*hacking*, hanno una presenza digitale relativamente semplice da identificare e si caratterizzano generalmente per una logica e un'etica fondate sulla condivisione, sullo scambio e sulla libertà di espressione che possono allora facilitare i contatti e le interazioni con gli studiosi. La ricerca diviene invece estremamente più complessa qualora l'oggetto di studio, ad esempio, concerna le comunità virtuali dedite alla vendita o allo scambio di beni e contenuti illeciti, come nel caso degli stupefacenti o della pedopornografia, in cui i forti interessi sottesi anche di tipo finanziario non solo li rendono estremamente impermeabili a "interventi" esterni, ma possono porre dei problemi dal punto di vista dell'etica e della sicurezza stessa del ricercatore.

Inoltre, anche qualora siano ottenuti l'accesso al gruppo e la disponibilità dei membri, la realizzazione effettiva dell'osservazione pone una serie di interrogativi riguardanti, ad esempio, il livello di immersione e di interazione nel contesto studiato, i cambiamenti indotti dalla presenza del

[102] Fedeli L., *La ricerca scientifica al tempo dei social media*, *op. cit*., p. 116.

[103] Décary-Hétu D., "Online crime monitoring", in Rossy Q. *et al.* (a cura di), *The Routledge international handbook of forensic intelligence and criminology*, Routledge, London/New York, 2018, pp. 238-240.

[104] Con l'espressione *Clear Web* si designa la parte del cyberspazio accessibile a tutti e indicizzata dai motori di ricerca, come ad esempio i siti web dei principali quotidiani. Il termine *Deep Web*, invece, indica generalmente gli spazi e i contenuti della Rete che non sono direttamente accessibili e che non sono indicizzati dai motori di ricerca. Di per sé, quindi, questa parte del cyberspazio non è necessariamente illegale, ma semplicemente presenta dei contenuti non accessibili pubblicamente: banche dati universitarie, registri dell'amministrazione pubblica, spazi di stoccaggio online di documenti, etc. Infine, il *Dark Web* designa quella parte del cyberspazio che non solo non è indicizzata dai motori di ricerca, ma che è accessibile solo utilizzando dei *softwares* appositi di criptazione e anonimizzazione (come ad esempio TOR). Sebbene non sia di per sé illegale, questa parte della Rete, proprio per il grado di protezione e anonimato che potenzialmente garantisce, si caratterizza per la maggior presenza di attività e contenuti illeciti.

ricercatore, così come il grado di validità delle dichiarazioni e dei comportamenti dei soggetti esaminati[105]. In altre parole, si tratta ancora una volta di adottare un approccio riflessivo che consideri le caratteristiche e gli effetti della situazione di ricerca nell'analisi dei differenti materiali raccolti e costruiti nel corso dell'indagine. Infine, appare importante sottolineare alcune considerazioni in merito ai processi di immedesimazione e di partecipazione nell'ambito di gruppi associati alla delinquenza online. Infatti, differenti aspetti problematici sono associati in particolare alla dialettica fra coinvolgimento e distacco[106], alla necessità di trovare e conservare quell'equilibrio fra partecipazione e distanza che consenta di raggiungere la comprensione della situazione sociale senza precludere l'analisi riflessiva e il rispetto dell'etica della ricerca[107]. Al di là della capacità di comprendere il punto di vista degli osservati senza limitare lo studio alle sole interpretazioni che gli attori danno delle situazioni, l'accettazione in determinate comunità online può essere subordinata all'investimento attivo del ricercatore non solo nelle discussioni, condotta tipica e di per sé non problematica dell'osservazione partecipante, ma soprattutto nello scambio di documenti che, invece, pone differenti problemi di ordine etico e legale. In Francia, ad esempio, il solo fatto di consultare abitualmente un servizio di comunicazione online che presenti dei contenuti pedopornografici è sanzionato penalmente (art. 227-23 c.p.) e, in tal senso, il ricercatore che studi questi fenomeni non solo dovrà prestare particolare attenzione agli ambienti virtuali esaminati, ma molto probabilmente sarà impossibilitato a condurre delle ricerche fondate sull'osservazione partecipante nell'ambito dei gruppi dediti allo scambio di queste rappresentazioni.

4.3 Lo studio della cybercriminalità attraverso l'osservazione e l'analisi delle tracce digitali.

Consci delle difficoltà legate allo studio di determinati delitti digitali, così come in ragione di approcci epistemologici e teorici rispetto ai quali l'osservazione partecipante può non essere sempre appropriata, gli studiosi hanno sviluppato differenti tecniche di ricerca basate, in particolare, sullo studio delle tracce digitali. Grazie infatti alle informazioni e agli elementi in essa presenti, la dimensione digitale permette l'osservazione, sia essa diretta o indiretta, di svariate pratiche e condotte associate alla cybercriminalità[108]. Si tratta, in altre parole, di analizzare il comportamento deviante anche a partire dalle tracce digitali intese come nuova categoria della presenza online[109]. A tal proposito, si sottolinea come l'emergere di forme sociocomunicative associate anche al web sociale, di nuove pratiche produttive e discorsive, di culture e forme di socialità legate al cyberspazio apra la sociologia, così come le scienze sociali, "alla possibilità di confrontarsi con metodi capaci di trattare grandi quantità di dati prodotti dagli utenti della Rete anche secondo percorsi qualitativi"[110]. Il cyberspazio fornisce infatti una pluralità di "fonti" e

[105] Per una rassegna, Holt T. J., "Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data", *op. cit.*

[106] Elias N., *Engagement et distanciation. Contributions à la sociologie de la connaissance*, Fayard, Paris, 1993.

[107] Fedeli L., *La ricerca scientifica al tempo dei social media, op. cit.*, pp. 115-116.

[108] Benbouzid B., Ventre D., "Pour une sociologie du crime en ligne. Hackers malveillants, cybervictimations, traces du web et reconfigurations du policing", *op. cit.*, p. 19.

[109] Serres A., "Problématiques de la trace à l'heure du numérique", *op. cit.*, p. 89; Ertzscheid O., Gallezot G., Simonnot B., "A la recherche de la 'mémoire' du web : sédiments, traces et temporalités des documents en ligne", *op. cit.*, p. 53-57.

[110] Boccia Altieri G., "La sociologia italiana su informatica e nuovi media", in Cipolla C. (a cura di), *L'identità sociale della sociologia in Italia*, FrancoAngeli, Milano, 2012, pp. 270-271.

"luoghi" attraverso cui analizzare differenti aspetti associati alla cybercriminalità, secondo degli approcci tanto di natura empatica che numerica[111].

Si possono dapprima ricordare i *forums* e i *newsgroups* che si presentano come degli spazi online dove discutere di un determinato tema, interagire con altri utenti e condividere contenuti in maniera asincrona. Questi ambienti digitali possono essere aperti e liberamente visibili sulla Rete, così come possono essere soggetti ad un'iscrizione ed eventualmente all'accettazione del nuovo membro da parte degli amministratori o degli altri partecipanti. Indipendentemente dal grado di "trasparenza", il vantaggio di questi spazi è di tener traccia delle attività realizzate online consentendo così un'eventuale analisi da parte del ricercatore. Un altro campo di ricerca sono le *chat rooms* (in particolare IRC) e i servizi di messaggeria istantanea che sono simili ai precedenti per quanto concerne le attività realizzabili, ma che presentano la differenza di fondarsi sulla comunicazione in tempo reale le cui tracce, tuttavia, possono non essere conservate sulle piattaforme o essere accessibili solo ai membri della conversazione. Grazie al livello di interazione e di prossimità relazionale, questi differenti ambienti possono caratterizzarsi inoltre per un forte aspetto comunitario. Si possono poi citare i siti web che, sebbene non consentano necessariamente l'interazione fra gli utenti, rappresentano una fonte significativa di informazioni, materiali e rimandi verso altri spazi che condividono gli stessi interessi. Fra questi, ad esempio, si possono menzionare i *blogs* dove i soggetti autorizzati possono "postare" contenuti e organizzare discussioni in maniera asincrona su differenti tematiche. In questa disamina non possono poi mancare i differenti *social networks* che, soprattutto qualora gli utenti scelgano di adottare un profilo pubblico, consentono di raccogliere informazioni significative in merito alle pratiche dei soggetti, così come di analizzare i contenuti e la costruzione dei dibattiti su determinati temi utili ai fini della ricerca. Infine, gli studi più recenti sulla cybercriminalità si focalizzano sui "criptomercati" illeciti, termine con cui si designano gli spazi online di vendita e acquisto di beni illegali generalmente accessibili attraverso dei programmi e dei *networks* che permettono la criptazione delle interazioni (ad esempio Tor, I2P e Freenet). Questi ambienti virtuali, infatti, rappresentano un punto di osservazione privilegiato per studiare la strutturazione e l'organizzazione dei traffici illeciti in Rete, nonché per analizzare le pratiche devianti realizzate nel *Dark Web*.

Senza pretendere di realizzare una disamina esaustiva, si può evidenziare come numerose ricerche si siano avvalse delle informazioni tratte da questi ambienti virtuali per studiare, ad esempio, la pirateria digitale, i furti d'identità online, le pratiche di *hacking*, i criptomercati illegali e la cosiddetta "pedofilia online"[112]. Esemplificativo in tal senso è lo studio di Corriveau che, a partire dalla raccolta e dall'analisi qualitativa delle conversazioni presenti in alcuni *newsgroups* a sfondo pedofilo, mostra non solo come si strutturino e si caratterizzino gli scambi di rappresentazioni pedopornografiche, ma soprattutto come le interazioni in questi spazi e il sentimento d'appartenenza ad un gruppo consentano ai collezionisti di questi contenuti di ridurre gli eventuali sensi di colpa e di sviluppare norme, razionalizzazioni e giustificazioni alle loro credenze

[111] Holt T. J., "Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data", *op. cit.*; Décary-Hétu D., "Online crime monitoring", *op. cit.*

[112] Per una rassegna, Holt T. J., "Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data", *op. cit.*; Décary-Hétu D., "Online crime monitoring", *op. cit.*

e condotte devianti[113]. Un altro esempio può essere tratto da una ricerca condotta da Dupont e colleghi su alcuni gruppi di *hackers* a partire dalla raccolta e dall'analisi dei *files* di log e dei messaggi postati in diverse *chats* di tipo IRC[114]. L'esame numerico delle tracce digitali associato a tecniche di geolocalizzazione e all'analisi delle reti sociali mostra, ad esempio, come questi utenti tendano effettivamente a strutturarsi in comunità virtuali di natura transnazionale le quali, tuttavia, non sono omogene tanto dal punto di vista del profilo degli attori, che per quanto concerne le attività e i sistemi utilizzati per proteggere le interazioni nell'ambito di questi spazi virtuali. Infine, gli studi più recenti sulla cybercriminalità fanno ricorso anche a strategie automatizzate di raccolta delle tracce digitali implicite e esplicite per analizzare, in particolare, la strutturazione e le caratteristiche dei criptomercati illeciti[115]. Quest'approccio, ad esempio, è stato utilizzato da Aldridge e Décary-Hétu per studiare il traffico di stupefacenti associato a *Silk Road*, una delle più conosciute piattaforme di vendita di beni illeciti basata sulla rete TOR e chiusa dall'FBI nel 2013. Contrariamente all'immagine presentata dai media, gli autori mostrano in particolare come molti degli acquirenti di questo "criptomercato" non siano in realtà singoli consumatori di droga, ma piuttosto spacciatori che acquistano quantità anche significative di prodotto per poi rivenderlo attraverso altri canali[116].

Tuttavia, l'abbondanza di tracce e di spazi online associati ai fenomeni di cybercriminalità non deve condurre a sottostimare tutta una serie di criticità che, invece, devono essere integrate nel disegno della ricerca. Dapprima, come già sottolineato per la tecnica dell'osservazione partecipante, identificare gli ambienti e le informazioni digitali da utilizzare nell'ambito della ricerca può rivelarsi particolarmente complesso e variare sensibilmente a seconda del tipo di realtà deviante oggetto di studio. Inoltre, il ricorso a strategie automatizzate di raccolta delle tracce digitali richiede specifiche competenze tecniche di tipo informatico e, se il ricercatore non le possiede, le alternative sono di ricorre a programmi commerciali o alla collaborazione con esperti tecnici i cui costi, tuttavia, non sempre possono essere sostenuti nell'ambito di un lavoro accademico[117]. Da non dimenticare poi che nel cyberspazio non solo le interazioni possono realizzarsi in maniera anonima, ma i contenuti eventualmente "postati" sono il risultato di processi di costruzione e selezione attraverso cui l'utente definisce e struttura la propria presenza online[118]. In quest'ottica, lo studioso è allora sovente confrontato ad informazioni che sollevano numerose questioni per quanto concerne

[113] Corriveau P., "Les groupes de nouvelles à caractère pédopornographique : une sous-culture de la déviance", in *Déviance et Société*, Vol. 34, N. 3, 2010, pp. 381-400.

[114] In questo caso, la strategia di ricerca integra l'analisi quantitativa delle tracce di tipo esplicito, come i messaggi postati, e di tipo implicito, come gli indirizzi IP e la cronologia delle connessioni, per tentare di proporre un ritratto dei "pirati" informatici attivi in questo tipo di spazi virtuali, Décary-Hétu D., Dupont B., Fortin F., "Policing the hackers by hacking them: studying online deviants in IRC chat rooms", *op. cit.*

[115] Il riferimento è in particolare alle ricerche che si avvalgono di specifici *softwares*, come i *web crawlers*, che consentono di "scaricare" una pagina web procedendo al contempo a indicizzare tutti gli *hyperlinks* in essa presenti. Questo tipo di programmi procede poi all'analisi di ogni spazio collegato al fine di ricercare altri contenuti da "scaricare" e altri *links* da seguire, consentendo così di raccogliere in maniera quasi automatica tutte le tracce digitali, sia implicite che esplicite, presenti in un determinato sito web, Décary-Hétu D., Aldridge J., "Sifting through the Net: monitoring of online offenders by researchers", in *The European Review of Organised Crime*, Vol. 2, N. 2, 2015, pp. 125-126.

[116] Aldridge J., Décary-Hétu D., "Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets", *in International Journal of Drug Policy*, Vol. 35, 2016, pp. 7–15.

[117] Décary-Hétu D., "Online crime monitoring", *op. cit.*, pp. 241-242.

[118] Cardon D., "Le design de la visibilité. Un essai de cartographie du web 2.0", in *Réseaux*, Vol. 6, n. 152, 2008, pp. 97-98.

la loro autenticità e validità, soprattutto qualora l'analisi non possa avvalersi di altre fonti e strumenti di rilevazione. Questi aspetti, in realtà, invitano a interrogare lo statuto stesso della traccia digitale che, contrariamente a quella "analogica" (ad esempio, l'impronta di una scarpa), è il frutto di una costruzione che si opera a differenti livelli[119]. In primo luogo, il modo in cui i contenuti e le informazioni sono presentati e strutturati dipende dal dispositivo tecnico e dalle scelte operate in termini di apparenza, forma e registrazione. Esemplificativa in tal senso è la piattaforma Twitter, dove non solo le informazioni che l'utente decide di "postare" sono limitate a un certo numero di caratteri e al rispetto di una determinata presentazione, ma in cui il tipo di traccia implicita che può essere eventualmente analizzato dipende dalle scelte operate dal sistema in termini di registrazione dei metadati. Inoltre, come già evidenziato, i contenuti resi disponibili dagli utenti sono il risultato di differenti strategie e, in generale, forniscono delle informazioni in merito a quello che l'utente ha fatto o deciso di fare online e non necessariamente rispetto a quello che voleva fare o ha fatto in altri contesti. Infine, il tipo di tracce utilizzate per la ricerca dipende dagli approcci e dai criteri di selezione adottati nell'ambito della rilevazione delle informazioni, aspetti che rinviano alle considerazioni già evidenziate a proposito delle inchieste di tipo "numerico".

Parafrasando le riflessioni di Martin a proposito del dato statistico[120], si possono allora sottolineare almeno tre aspetti fondamentali dell'analisi delle tracce digitali. Dapprima, emerge come queste ultime non abbiano un forte valore informativo se non si conoscono le loro modalità di costruzione, dal punto di vista del supporto informatico, dell'utente e del disegno della ricerca. Inoltre, un solo tipo di tracce non permette di descrivere, misurare e analizzare l'evoluzione di un fenomeno sociale e, in particolare, non permette di situare gli usi digitali nel contesto più largo delle pratiche sociali degli individui. Infine, questi contenuti non parlano da soli, ma assumono significato attraverso gli approcci teorici e le interpretazioni dello studioso. La traccia digitale, infatti, non è "un'evidenza empirica che si consegna alla nostra percezione senza sbavature, in modo tale da poter essere utilizzata così com'è", ma un'informazione elementare che "va sempre 'interpretata', alla luce di costrutti ed ipotesi teoriche"[121].

5. Riflessioni conclusive.

Lo studio delle realtà devianti associate alla Rete invita a confrontarsi con fenomeni criminali d'indubbia attualità, ma anche di difficile analisi. In tal senso, alcuni degli strumenti e delle fonti "tradizionali" della ricerca sociale mostrano tutti i loro limiti di fronte ad una criminalità che, almeno in parte, presenta una natura immateriale e una dimensione transnazionale. Inoltre, si è visto come le strategie e i metodi d'indagine, anche associati alle nuove tecnologie, debbano accompagnarsi ad un'analisi riflessiva delle condizioni di rilevazione e di costruzione dell'informazione che tenga conto degli effetti della situazione di ricerca sui materiali raccolti.

[119] Ertzscheid O., Gallezot G., Simonnot B., "A la recherche de la 'mémoire' du web : sédiments, traces et temporalités des documents en ligne", *op. cit.*, pp. 56-57.

[120] Martin O., "Les statistiques parlent d'elles-mêmes ? Regards sur la construction sociale des statistiques", in Collectif, *La pensée confisquée*, La Découverte, Paris, 1997, pp. 173-191 citato in Mucchielli L., "Enquêter sur la délinquance. Réflexions méthodologique et épistémologiques", *op. cit.*, p. 47.

[121] Il riferimento è alla differenza fra "dato" e "informazione elementare", Cremonini F., "Il ciclo metodologico dell'informazione scientifica", *op. cit.*, p. 68.

Nel corso dell'articolo si è cercato poi di sottolineare come nessun approccio possa pretendere l'esaustività soprattutto rispetto a fenomeni che, per la natura stessa di Internet, presentano un carattere globale, distribuito e reticolare. In questa prospettiva, si è evidenziato allora come le strategie di ricerca possano permettere di ottenere un'immagine più accurata della cybercriminalità soprattutto qualora integrino differenti fonti e metodi d'indagine, avvalendosi anche delle potenzialità della Rete per quanto concerne, ad esempio, la disponibilità e la tracciabilità delle informazioni e delle pratiche. Le opzioni di ricerca associate al cyberspazio costituiscono tuttavia un ecosistema complesso, che necessita di essere interrogato non solo in merito all'affidabilità e all'autenticità delle informazioni in esso presenti, ma anche per quanto concerne le modalità di visibilità e di registrazione dei contenuti, che rinviano alle scelte operate dai differenti dispositivi tecnici e dai diversi spazi online.

L'analisi delle tracce digitali assume in questo contesto un significato particolare, non solo perché si associa ai più recenti approcci della ricerca, ma soprattutto perché pone una serie di interrogativi che dovrebbero essere affrontati non solo dalle discipline scientifiche, ma in maniera più generale dalle istanze pubbliche e politiche. Da un lato, infatti, la rilevazione e l'analisi di questo tipo di contenuti solleva necessariamente delle questioni di carattere etico concernenti l'identità dei soggetti studiati e la protezione della loro privacy, aspetti che dovrebbero pertanto essere integrati nel disegno stesso della ricerca in modo tale da identificare le migliori strategie da adottare per assicurare il rispetto della vita privata, così come per ottenere il consenso degli individui relativo al trattamento delle informazioni e al coinvolgimento nell'indagine. Dall'altro, la rilevazione e l'analisi delle informazioni e delle tracce digitali pone degli interrogativi di natura sociopolitica, in particolare per quanto riguarda i crescenti processi di digitalizzazione della "vita" dei cittadini i cui risultati possono essere strumentalizzati anche per fini commerciali e politici. La questione della protezione dei dati personali è pertanto centrale e domanda l'adozione da parte delle istituzioni pubbliche di misure specifiche volte ad assicurare il rispetto della vita e dell'identità digitale dei cittadini, seguendo ad esempio le linee guida identificate dal recente regolamento generale sulla protezione dei dati personali adottato dall'Unione Europea (RGPD).

Bibliografia.

- Aebi M. F., *Comment mesurer la délinquance ?*, Armand Colin, Paris, 2006.
- Aebi M. F., Jaquier V., "Les sondages de délinquance autoreportée : origines, fiabilité et validité", in *Déviance et Société*, Vol. 32, N. 2, 2008, pp. 205-227.
- Aldridge J., Décary-Hétu D., "Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets", in *International Journal of Drug Policy*, Vol. 35, 2016, pp. 7-15.
- Auray N., Kaminsky D., "Les trajectoires de professionnalisation des hackers : la double vie des professionnels de la sécurité", in *Annales des Télécommunications*, Vol. 62, N. 11-12, 2007, pp. 1313-1327.
- Balloni A., Bisi R., Costantino S. (a cura di), *Legalità e comunicazione*, FrancoAngeli, Milano, 2008.
- Balloni A., Bisi R., Sette R., *Vittime e vittimologia: percorsi di ricerca*, Minerva, Bologna, 2012.
- Balloni A., Bisi R., Sette R., *Principi di criminologia. Le teorie*, Wolters Kluwer-Cedam, Padova, 2015.
- Bandini T. et al., *Criminologia. Il contributo della ricerca alla conoscenza del crimine e della reazione sociale*, Giuffré, Milano, 1991.
- Baraldi C., "L'orientamento epistemologico della ricerca empirica", in Cipolla C. (a cura di), *Il ciclo metodologico della ricerca sociale*, FrancoAngeli, Milano, 2001, pp. 29-62.

- Beaud S., Weber F., *Guide de l'enquête de terrain*, La Découverte, Paris, 2003.
- Becker H., *Outsiders. Études de sociologie de la déviance*, Métaillié, Paris, 1985.
- Benbouzid B., Ventre D., "Pour une sociologie du crime en ligne. Hackers malveillants, cybervictimations, traces du web et reconfigurations du policing", in *Réseaux*, Vol. 3, N. 197-198, 2016, pp. 9-30.
- Bisi R., Faccioli P. (a cura di), *Con gli occhi della vittima*, FrancoAngeli, Milano, 1996.
- Bisi R., Ceccaroli G., Sette R., *Il tuo Web. Adolscenti e social network*, Wolters Kluwer-Cedam, Padova, 2016.
- Boccia Altieri G., "La sociologia italiana su informatica e nuovi media", in Cipolla C. (a cura di), *L'identità sociale della sociologia in Italia*, FrancoAngeli, Milano, 2012, pp. 265-272.
- Boccia Altieri G., "La sociologia italiana su informatica e nuovi media", in Cipolla C. (a cura di), *L'identità sociale della sociologia in Italia*, FrancoAngeli, Milano, 2012, pp. 265-272.
- Bossler A. M., Holt T. J., "On-line activities, guardianship, and malware infection: an examination of routine activities theory", in *International Journal of Cyber Criminology*, Vol. 3, N. 1, 2009, pp. 400-420.
- Bourdieu P., *Questions de sociologie*, Minuit, Paris, 1984.
- Bourdieu P. (a cura di), *La misère du monde*, Seuil, Paris, 1993.
- Bourdieu P., Chamboredon J.-C., Passeron J.-C., *Le Métier de sociologue*, Mouton, Berlin/New York, 2005 (5° edizione).
- Cardon D., "Le design de la visibilité. Un essai de cartographie du web 2.0", in *Réseaux*, Vol. 6, n. 152, 2008, pp. 93-137.
- Castells M., *La nascita della società in rete*, Milano, Egea, 2002.
- Coleman G., *Anonymous. Hacker, activiste, faussaire, mouchard, lanceur d'alerte*, Lux, Montréal, 2016.
- Corbetta P., *Metodologia e tecniche della ricerca sociale*, il Mulino, Bologna, 2011.
- Corriveau P., "Les groupes de nouvelles à caractère pédopornographique : une sous-culture de la déviance", in *Déviance et Société*, Vol. 34, N. 3, 2010, pp. 381-400.
- Coîté A. M., Bérubé M., Dupont B., "Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité", in *Réseaux*, Vol. 3., N. 197-198, 2016, pp. 203-224.
- D'Alessandro L., "Prefazione", in Pitasi A. (a cura di), *Webcrimes. Normalità, devianze e reati nel cyberspace*, Pitasi A. (a cura di), Guerini e Associati, Milano, 2007, pp. 11-14.
- Décary-Hétu D., "Online crime monitoring", in Rossy Q. *et al.* (a cura di), *The Routledge international handbook of forensic intelligence and criminology*, Routledge, London/New York, 2018, pp. 238-248.
- Décary-Hétu D., Aldridge J., "Sifting through the Net: monitoring of online offenders by researchers", in *The European Review of Organised Crime*, Vol. 2, N. 2, 2015, pp. 122-141.
- Décary-Hétu D., Dupont B., Fortin F., "Policing the hackers by hacking them: studying online deviants in IRC chat rooms", Masys A. J. (a cura di), *Networks and Network Analysis for Defence and Security*, Springer, New York, 2014, pp. 63-82.
- Dieu F., *Politiques publiques de sécurité*, L'Harmattan Paris, 1999.
- Dupont B, Gautrais V., "Crime 2.0 : le web dans tous ses états !", in *Champ pénal/Penal field* [rivista online], Vol. VII, 2010, p. 36, disponibile alla pagina http://journals.openedition.org/champpenal/7782
- Elias N., *Engagement et distanciation. Contributions à la sociologie de la connaissance*, Fayard, Paris, 1993.
- Ertzscheid O., Gallezot G., Simonnot B., "A la recherche de la 'mémoire' du web : sédiments, traces et temporalités des documents en ligne", in Barats C. (a cura di), *Manuel d'analyse du web*, Armand Colin, Paris, 2013, pp. 53-68.
- Fedeli L., *La ricerca scientifica al tempo dei social media*, FrancoAngeli, Milano, 2017.
- Finn M. A., Stalans L J., "How targeted enforcement shapes marketing decisions of pimps: evidence of displacement and innovation", in *Victims and Offenders*, Vol. 11, N.4, 2016, pp. 578-599.
- Fortin F., Corriveau P., *Who is Bob_34? Investigating child cyberpornography*, UBC Press, Vancouver-Toronto, 2015.
- Furnell, S., *Cybercrime: vandalizing the information society*, Addison Wesley, Boston, 2002.
- Gallino L., *Dizionario di sociologia*, Utet, Torino, 2006.
- Ghernaouti-Hélie S., *La cybercriminalité. Le visible et l'invisible*, PPUR, Lausanne, 2009.
- Goffman E., *Les rites d'interaction*, Minuit, Paris, 1974.
- Grémy J.-P., "Les expériences françaises sur la formulation des questions d'enquête. Résultats

d'un premier inventaire", in *Revue française de sociologie*, Vol. 4, 1987, pp. 567-599.
- Higgins G. E., Marcum C. D., Digital *piracy: an integrated theoretical approach*, Carolina Academic Press, Raleigh, 2011.
- Hine C. (a cura di), *Virtual methods: issues in social research on the Internet*, Berg, Oxford, 2005.
- Holt J. T, Bossler A. M., "An assessment of the current state of cybercrime scholarship", in *Deviant Behavior*, N. 35, 2014, pp. 20-40.
- Holt T. J, Copes H., "Transferring subcultural knowledge online: practices and beliefs of persistent digital pirates", in *Deviant Behavior*, Vol. 31, N. 7, 2010, pp. 625-654.
- Holt T. J., "Cybercrime", in Huebner B.M., Bynum T.S., *The handbook of measurement issues in criminology and criminal justice*, John Wiley & Sons, New York, 2016, pp. 29-48.
- Holt T. J., "Exploring strategies for qualitative criminological and criminal justice inquiry using on-line data", in *Journal of Criminal Justice Education*, Vol. 21, N. 4, 2010, pp. 466-487.
- Holt T. J., "Situating the problem of cybercrime in a multidisciplinary context", in Holt T. J. (a cura di), *Cybercrime through an interdisciplinary lens*, Routledge, London & New York, 2017, pp. 1-15.
- Jobard F., De Maillard J., *Sociologie de la police. Politiques, organisations, réformes*, Armand Colin, Paris, 2015.
- Jones L. M., Mitchell K. J., Finkelhor D., "Trends in Youth Internet Victimization: findings from three Youth Internet Safety Surveys 2000–2010", in *Journal of Adolescent Health*, Vol. 50, N. 2, 2012, pp. 179–186.
- Kitsuse J., Cicourel A., "A note of the uses of official statistics", in *Social problems*, Vol. 11, N. 2, 1963, pp. 131-139.
- Kivitz J., "Online interviewing and the research relationship", in Hine C. (a cura di), *Virtual methods: issues in social research on the Internet*, Berg, Oxford, 2005, pp. 35-50.
- Langlade A., "La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'Internet en 2016 : éléments de mesure et d'analyse", in ONDRP, *La note de l'ONDRP. Rapport annuel 2017*, 2017, disponibile al sito web https://inhesj.fr/ondrp/publications/la-note-de-londrp/la-cybercriminalite-et-les-infractions-liees-lutilisation
- Lavoie P.-E., Fortin F., Tanguay S., "Problèmes relatifs à la définition et à la mesure de la cybercriminalité", in Fortin F., (a cura di), *Cybercriminalité. Entre inconduite et crime organisé*, Presses Internationales Polytechnique, Montrèal, 2013, p 3-20.
- Leman-Langlois S., "Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberspace commercial", in *Criminologie*, Vol. 39, N. 1, 2006 pp. 63-81.
- Livingstone et al., *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, London, 2011 disponibile alla pagina http://eprints.lse.ac.uk/33731/
- Macilotti G., "La jeunesse à l'ère du numérique : pratiques, exposition au risque et victimation. Une étude auprès de la Communauté d'Agglomération du Grand Rodez", in *Les Cahiers de la Sécurité et de la Justice*, N. 37, 2017, pp. 110-129.
- Macilotti G., "La criminalità informatica e telematica fra antichi dilemmi e nuove sfide", in Balloni A., Bisi R., Sette R., *Principi di criminologia applicata. Criminalità, controllo, sicurezza*, Wolters Kluwer-Cedam, Padova, 2015, pp. 251-277.
- Macilotti G., "La pedopornografia e l'adescamento online di minori", in Balloni A., Bisi R., Sette R., *Principi di criminologia applicata. Criminalità, controllo, sicurezza*, Wolters Kluwer-Cedam, Padova, 2015, pp. 279-315.
- Maguire M., "Crime data and statistics", in Maguire M., Morgan R. e Reiner R (a cura di), *The Oxford Handbook of Criminology*, Oxford University Press, Oxford, 2007, pp. 241-301.
- Martin O., "Les statistiques parlent d'elles-mêmes ? Regards sur la construction sociale des statistiques", in Collectif, *La pensée confisquée*, La Découverte, Paris, 1997, pp. 173-191.
- Matelly J.-H., Mouhanna C., *Police des chiffres et des doutes*, Michalon, Paris, 2007.
- Mauger G., "Sociologie de la situation d'enquête. Une clé d'intelligibilité de l'espace des styles de vie déviants des jeunes des classes populaires", in Boucher M. (a cura di), *Enquêter sur les déviances et la délinquance. Enjeux scientifiques, politiques et déontologiques*, L'Harmattan, Paris, 2015, pp. 133-139.
- Mauger M., "Enquêter en milieu populaire", in *Geneses*, N. 6, 1991, pp. 125-143.
- Moore R., "Digital file sharing: an examination of neutralization and rationalization techniques employed by digital file shares", in Jaishankar K. (a cura di), *Cyber Criminology. Exploring Internet crimes and criminal behavior*, CRC Press, New York, 2011, pp. 209-225.

- Moore R., *Cybercrime. Investigating high-technology computer crime*, Elsevier/Anderson, Amsterdan/Boston, 2011.
- Morcellini M., Pizzaleo A.G. (a cura di), *Net sociology. Interazioni tra scienze sociali e Internet*, Guerini e Associati, Milano, 2002.
- Mucchielli L., "Enquêter sur la délinquance. Réflexions méthodologique et épistémologiques", in Boucher M. (a cura di), *Enquêter sur les déviances et la délinquance. Enjeux scientifiques, politiques et déontologiques*, L'Harmattan, Paris, 2015, pp. 45-73.
- Mucchielli L., *Violences et insécurité. Fantasmes et réalités dans le débat français*, La Découverte, Paris, 2001.
- Muratore M. G. (a cura di), *Delitti, imputati e vittime dei reati. Una lettura integrata delle fonti sulla criminalità e la giustizia*, ISTAT, Roma, 2017.
- Murthy D., "Digital ethnography: an examination of the use of new technologies for social research" in *Sociology*, Vol. 42, N. 5, 2008, pp. 837-855.
- Pereira B., "La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité", in *Revue internationale de droit économique*, Tomo XXX, n. 3, 2016, pp. 387-409.
- Ponti G., *Compendio di criminologia*, Torino, Cortina, 1994.
- Potter G. R., "Real gates to virtual fields: integrating online and offline ethnography in studying cannabis cultivation and reflections on the applicability of this approach in criminological ethnography more generally", in *Methodological Innovations*, Vol. 10, N. 1, 2017, pp. 1-11.
- Quayle E., Taylor M., "Child pornography and the Internet: perpetuating a cycle of abuse", in *Deviant Behavior*, Vol. 23, N. 2, 2002, pp. 331-361.
- Rehn A., "The politics of contraband: the honor economies of the Warez scene", in *The Journal of Socio-Economics*, V. 33, N. 3, 2004, pp. 359-374.
- Reyns B. W., Henson B., Fisher B. S., "Stalking in the twilight zone: extent of cyberstalking victimization and offending among college students" in *Deviant Behavior*, Vol. 33, N. 1, 2012, pp. 1-25.
- Robert Ph. et al., *Les comptes du crime. Les délinquances en France et leurs mesures*, L'Harmattan, Paris, 1994.
- Robert Ph., Zauberman R., *Mesurer la déliquance*, Presses de Sciences-Po, Paris, 2011.
- Rogers M., Smoak N. D., Jia L., "Self-reported deviant computer behavior: a big-5 moral choice, and manipulative exploitive behavior analysis", in *Deviant Behavior*, N. 27, 2006, pp. 245–268.
- Saponaro A., *Vittimologia. Origini - Concetti – Tematiche*, Giuffré, Milano, 2004.
- Sellin T., "The Basis of a Crime Index", in *The Journal of Criminal Law et Criminology*, n. 22, 1931, pp. 335-356.
- Serres A., "Problématiques de la trace à l'heure du numérique", in *Sens-Dessous*, Vol. 1, N. 10, 2012, pp. 84-94.
- Sette R., *Criminalità informatica. Analisi del fenomeno tra teoria, percezione e comunicazione sociale*, Clueb, Bologna, 2000.
- Sette R., *Cases on technologies for teaching criminology and victimology: methodologies and practices*, Hershey, New York, 2010.
- Sicurella S., "Lo studio della vittimologia per capire il ruolo della vittima", in *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. VI, N. 3, Settembre-Dicembre 2012, pp. 62-75.
- Taylor P.A., *Hackers: Crime in the digital sublime*, Routledge, New York, 1999.
- Wall D. S., "Criminalising cyberspace: the rise of the Internet as a 'crime problem'", in Jewkes Y., Yar M. (a cura di), *Handbook of Internet crime*, Willan Publishing, Cullompton, 2009, pp. 88-103.
- Wall D. S., "Cybercrimes and the Internet", in Wall D. S (a cura di), *Crime and the Internet*, Routledge, New York, pp. 1-7.
- Wolak J., Finkelhor D., Mitchell K. J., "Child pornography possessors: trends in offender and case characteristics", in *Sexual abuse: A Journal of Research and Treatment*, Vol. 23, N. 1, 2011, pp. 22-42.
- Yar M., "Toward a cultural criminology of the Internet", in Steinmetz K. F., Nobles M. R. (a cura di), *Technocrime and criminological theory,* Routledge, New York, 2017, pp. 116-132.
- Yar M., *Cybercrime and* society, Sage, London, 2006.
- Ybarra M. et al., "Examining characteristics and associated distress related to Internet harassment: findings from the Second Youth Internet Safety Survey", in *Pediatrics*, Vol. 118, N. 4, 2006, pp. 1169-1177.
- Ybarra M. L., Mitchell K. J., Wolak J., Finkhelor D., "Examining characteristics and associated distress related to Internet harassment: findings from the Second Youth Internet Safety

Survey", in *Pediatrics*, Vol. 118, N. 4, 2006, pp. 1169-1177.
- Zauberman R. et al., "L'acteur et la mesure. Le comptage de la délinquance entre données administratives et enquêtes", in *Revue française de sociologie*, Vol. 50, n. 1, 2009, pp. 31-62.

Siti web consultati.

- Crime Survey for England & Wales (CSEW): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice
- INSEE: https://www.insee.fr/fr/metadonnees/source/s1278
- ISTAT: https://www.istat.it/it/archivio/164581
- National Crime Victimization Survey (NCVS): https://www.bjs.gov/index.cfm?ty=dcdetail&iid=245
- National Longitudinal Survey of Youth (NLSY): https://www.bls.gov/nls/
- National Youth Survey (NYS): https://www.icpsr.umich.edu/icpsrweb/ICPSR/series/88