

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in Ciberspazio e Diritto, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

I 'cybercriminali': rischi e limiti dei profili criminologici

Mara Mignone¹

1. Introduzione.

L'attenzione e la curiosità sollevate dal recente, sensibile aumento della criminalità informatica non riguardano solo l'evoluzione delle fattispecie di violazione, o la rapidità con cui le tecniche di attacco divengono sempre più sofisticate, quanto anche il profilo del cybercriminale. Gli addetti ai lavori, ma anche l'immaginario collettivo, si interrogano su chi e perché utilizzi le nuove tecnologie di informazione e comunicazione per delinquere.

Le riflessioni sul profilo dei soggetti attivi degli illeciti realizzati in specie in Internet, riconducono nella quasi totalità dei casi alla figura dell'*hacker*, l'utilizzo incondizionato di questo termine, ha finito in realtà per reciderne i legami con il contesto socio-culturale che l'ha originato, rendendolo un semplice sinonimo di pirata informatico o di cybercriminale. Contrariamente a quanto si possa pensare, non si tratta di una semplice questione terminologica; alla pur comprensibile generalizzazione delle definizioni utilizzate per etichettare i nuovi criminali moderni, si sta accompagnando, infatti, anche una progressiva semplificazione, contenutistica e metodologica, delle indagini soggettive che li riguardano. Negli ultimi tempi, si sono susseguiti numerosi tentativi di schematizzazione, finalizzati a sintetizzarne i tratti principali; senza contare tutti quei contributi che esplorano la cosiddetta 'psicologia *hacker*', delineando profili, definiti spesso, a torto forse più che a ragione, 'criminologici'.

Non volendo entrare nel merito dei singoli contributi, non possono però non sollevarsi alcune perplessità sulla validità, l'attendibilità ed in parte anche l'utilità, di talune di queste astrazioni. In particolare, ciò che si vuole delineare in questo scritto, è una riflessione introduttiva ai rischi ed ai limiti che questo genere di interventi possono presentare, sia come 'profili' sia in quanto definiti 'criminologici'.

2. I 'profili' del cybercriminale: l'ambigua figura dell'*hacker* tra hacktivism e hackeraggio.

Il punto di partenza per ogni altra considerazione, non può che essere il prototipo dell'*hacker* come emerge dai diversi tratteggi. In linea generale, oggi *hacker* sembra essere chiunque, per abilità quanto per fortuna, riesce a sfidare Internet e a catturare l'attenzione, specie dei *media*.

¹ TRANSCRIME, Università degli Studi di Trento, <http://www.transcrime.unitn.it>.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in Ciberspazio e Diritto, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

Fino a qualche tempo fa, molti profili descrivevano adolescenti problematici, introversi e scontrosi, privi di ogni altro stimolo ed interesse se non il proprio computer, dediti alla 'sperimentazione informatica', ma non così pericolosi. L'evoluzione criminale che ha interessato il contesto informatico ha poi spostato l'attenzione verso una tipologia soggettiva diversa; oggi l'*hacker* viene identificato per lo più con un individuo giovane (tra i 24 e i 33 anni), di sesso maschile, con un buon livello di istruzione ed un impiego, intelligente e dotato di una discreta alfabetizzazione informatica. Anche 'l'*hacker* italiano' sembra porsi in linea con quest'ultimo profilo: ha tra i 25 e i 30 anni, non ha una strumentazione informatica poi così sofisticata ma sa destreggiarsi, 'agisce' in tarda serata o di notte perché studia o lavora ed ha un livello di istruzione medio-alto.

Comuni ad entrambi i profili sono anche le motivazioni del loro agire: la volontà di sfidare i sistemi informatici per mettersi alla prova, per emulare e superare quanti hanno già ottenuto risultati gratificanti.

Se questo è l'*hacker* per così dire 'medio', come individuato dai profili, non si può non chiedersi chi si cela allora dietro alcuni schemi di frodi e truffe *online* che, al di là del danno economico che riescono a generare, sono talmente originali da evidenziare un'intelligenza criminale vivace, estrosa e non così comune. E come si spiega poi la dilatazione applicativa del termine *hacker* che oggi viene utilizzato indifferente anche per i casi, sempre più frequenti, di vandalismo informatico, caratterizzati da un intento per così dire 'distruttivo'? Facendo un passo indietro, fino al contesto che ha dato vita alla vera figura dell'*hacker*, qualche perplessità sull'attendibilità di questa figura di cybercriminale diventa ancora più legittima.

Forse la risposta a questa domanda non è riscontrabile nei profili, quanto piuttosto nella contrapposizione tra *hacktivismo* e *hackeraggio*.

Il riferimento è al MIT (*Massachusetts Institute of Technology*) ed all'*hacker* della fine degli anni cinquanta, quale 'virtuoso' dell'informatica, la cui finalità è l'innovazione tecnica, lo studio e la sperimentazione per lo sviluppo del sapere. La libertà è il tema centrale dell'attività dei primi *hacker*, da intendersi quale libertà della conoscenza e della sua circolazione; alla base vi è la finalità di rispondere tanto ad un'esigenza personale di confrontarsi con l'intelligenza artificiale, quanto alla necessità di semplificazione dell'uso della tecnologia a favore della collettività. È chiaro che, così concepita, libertà non è per nulla sinonimo di accesso incondizionato a fini di danneggiamento, blocco del sistema informatico e telematico o alterazione e distruzione dei dati. Il fenomeno *hacker*, così inteso, è un vero e proprio movimento culturale; nulla toglie, naturalmente, che il sistema di valori da cui origina la comunità *hacker* possa anche non essere condiviso, o prestarsi a critiche e condanne. Così come non è possibile stabilire se tale sistema di valori sia mai uscito realmente dai confini fisici della ricerca accademica o comunque di laboratorio. Ma non è tanto questo il punto. L'aspetto che preme evidenziare è l'essenza dell'*hacktivismo*, per indagare la psicologia *hacker* che emerge dai vari profili per così dire moderni, anche in un'ottica di confronto e

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

valutazione di tali profili. Se l'*hacktivismo*, in senso stretto, è anche rispettare delle regole, l'*hackeraggio* moderno si distingue per un'anarchia comportamentale, nel senso che non sembrano esserci regole quanto, piuttosto, solo risultati. O meglio, vi sono regole e codici a cui si attengono le comunità *hacker*, ma rispettano sempre meno l'etica e la filosofia originarie: la sfida è sempre più contro la società che non verso se stessi; la tecnologia non è uno stimolo al confronto, quanto piuttosto un potente mezzo per affermare la propria presenza e le proprie idee, per ottenere ciò che si vuole, non importa se questo voglia dire commettere un reato. Con questo non si vuole dire che non esistano più *hacker* definibili 'puri', ma sono dei particolari in una fotografia che rappresenta uno scenario diverso, in cui i protagonisti sono forse altri. Il fulcro del discorso è quindi il seguente. Stando ai profili, l'*hacker* moderno è sostanzialmente una persona come tante altre, non ha tratti o segni distintivi che lo possano individuare come 'criminale'; stando alla casistica, invece, l'*hacker* è un ribelle.

Per riuscire a sanare le contraddizioni tra la tipologia soggettiva e motivazionale dei profili e i dati che emergono dalla casistica, dovremmo concludere, quindi, che forse non lo è nei modi e nei gesti del vivere quotidiano, ma sicuramente lo è in rete. Segue uno stile di vita per così dire ordinario, se non normale, ma si ribella alle regole utilizzando le nuove tecnologie, si fa bandiera della libertà di comunicazione attraverso Internet perché proprio in Internet trova spazi e opportunità per manifestare il suo pensiero: più l'azione è plateale, e se necessario dannosa, più crede che il suo messaggio arrivi chiaro.

Conclusione che non può non dare adito a qualche legittima perplessità.

E di dubbi devono averne anche quanti propongono profili soggettivi, anche in considerazione del fatto che è più che evidente che vi è stato un passaggio generazionale tra le diverse figure di *hacker*. Ai profili si stanno infatti affiancando studi sulle 'tipologie' di *hacker*, distinte a seconda della psicologia, delle competenze informatiche e del livello di pericolosità. Ci sono i *wannabe lamer* e gli *script kiddie*, soggetti per lo più innocui perché non sufficientemente *skillati*, i *cracker* e i *cyber-warrior*, pericolose minacce alla sicurezza informatica, gli *hacker* etici (una contraddizione in termini visto che vengono considerati comunque pericolosi) e quelli cosiddetti paranoici e specializzati. Ora, non è solo la distinzione di per sé stessa che crea dubbi, quanto piuttosto, come si vedrà oltre, il percorso che è stato seguito per giungere a tale schematizzazione. Ed inoltre, senza risposta rimane la domanda su come si possano conciliare queste tipologie con il profilo sintetico dell'*hacker*.

Al di là dei dubbi irrisolti e dato quantomeno per certo che oggi si parla di *hacker* in un'accezione generale, ben lontana da quella originaria, resta da chiedersi: vi è reale corrispondenza tra l'*hacker* per così dire 'dei profili' e quello 'della rete'? e, se così non fosse, quali allora i rischi di un profilo che, nel suo delinearsi, mal si adatta al cybercriminale?

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in Ciberspazio e Diritto, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

La risposta alla prima di queste domande necessita di un breve *excursus* sulle tipologie di attacco realizzate per mezzo e nell'ambito delle infrastrutture informatiche. Si tratta di fattispecie assolutamente diversificate: potenzialmente si può dire che ogni tipologia di reato realizzabile nel mondo fisico ha il suo parallelo in rete, dove trova tecniche di commissione spesso semplificate, per ottenere risultati migliori, in tempi brevi. Senza dimenticare poi tutta quella serie di nuove violazioni che integrano i crimini informatici in senso stretto.

Se a questo si aggiunge l'analisi dei casi di attacco degli ultimi tempi, si nota come i rischi maggiori siano sempre più correlati a violazioni di particolare gravità: non più il solo *defacement* di una *home page* o lo *spamming* o la sola violazione di un domicilio informatico, ma il blocco totale dei *server* e delle attività economico-informative; basti pensare anche solo all'anno che si è appena concluso: si sono susseguiti i *denials of service* in grado di paralizzare anche i portali più organizzati (si pensi al caso Yahoo.com), i furti di dati sensibili (i numeri di carte di credito vantano il primato tra le informazioni a maggior rischio), gli atti di vandalismo informatico e le minacce di casi di cyber-terrorismo, senza dimenticare l'*information warfare* e le varie tipologie di spionaggio industriale e sabotaggio a fini di concorrenza sleale (uno per tutti, il caso Microsoft).

Sulla base di queste considerazioni, non si può che concludere che la tipologia di *hacker* 'medio', come riportata in apertura, è quantomeno improbabile, inadeguata a descrivere l'autore di violazioni complesse, che richiedono competenze e *skills* non alla portata di tutti. Se è evidente che il termine *hacker* non connota più l'*hacker* cosiddetto 'puro' dei primi anni sessanta, è oltremodo contestabile parlare oggi di *hacker* come di un qualunque pirata informatico: è la stessa fenomenologia criminale a smentirlo.

Fenomenologia che evidenzia, quindi, il semplicismo di profili che sembrano tagliati più per i *mass media* che non per la reale conoscenza scientifica della criminalità informatica. Quali, allora, i possibili rischi della disinformazione in quest'ambito?

3. I rischi della disinformazione nell'analisi soggettiva dei crimini informatici.

Il discorso si sposta inevitabilmente sul piano sociale, prima che giuridico; presentare l'*hacker* quale ogni anonimo paladino delle reti telematiche, che sfida le autorità di *law enforcement* e le leggi di ogni paese, giocando al ladro che semina sempre le guardie, rischia di innescare un gioco pericoloso. Un gioco in cui tutti vogliono essere protagonisti, da un lato, e tutti vogliono prendere e punire dall'altro, senza sapere, alla fine dei conti, di chi e di cosa si sta realmente parlando. Così come delineato, l'*hacker* può essere chiunque. Il pericolo è quello di mitizzare, innalzandole a gesta, le imprese, anche mediocri, di persone che, nella maggior parte dei casi, non sono neanche lontanamente etichettabili come *hacker*, ma ne rincorrono la notorietà e vogliono l'attenzione che questi ultimi sono in grado di sollevare; spesso si tratta di

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

persone sprovviste dei mezzi, delle abilità informatiche e soprattutto che finiscono per aderire a motivazioni per così dire eversive, pur senza percepirne la reale portata. Il fatto, poi, che l'attenzione, tanto del mondo della comunicazione quanto della comunità scientifica, sia circoscritta a questa tipologia di soggetti, rischia di lasciare sconosciuto, ed indisturbato, quello che al contrario dovrebbe essere l'ambito soggettivo di maggior interesse: i veri conoscitori della rete, ovvero gli autori degli attacchi complessi ed economicamente più dannosi.

Quanto detto finora non è slegato da possibili implicazioni di tipo giuridico. Nel momento in cui mancano normative specifiche e soprattutto è estremamente difficile l'applicazione del diritto in un contesto quale è quello di Internet, non si può negare che proprio verso il mondo giuridico, ed in particolare quello giudiziario, convergano l'attenzione e le aspettative di risposta. Risposte che devono arrivare nonostante sia le lacune legislative sia, soprattutto, le difficoltà oggettive di investigazione e la stessa impreparazione di quanti indagano. È inevitabile che colpire l'*hacker* per così dire 'medio' diventa molto più facile che individuare e condannare il criminale 'skillato', in grado di confondere le tracce e garantirsi l'anonimato e l'impunità. Si innesca così un circolo vizioso: si risponde all'esigenza di punire anche i crimini informatici, si dà alla stampa il modo di trattare anche questo genere di violazioni, si confermano i sedicenti profili criminologici stilati da più parti, si aumenta la curiosità, quasi morbosa, della collettività e si alimentano le aspirazioni dei mediocri maghi del computer. Il tutto senza incidere sulla reale fenomenologia criminale e sulla sua potenzialità dannosa.

Non va sottovalutato il rischio dei 'processi-copertina', delle cause giudiziarie in cui la pena più che la sua funzione retributiva o rieducativa per il reo, riveste il ruolo di monito alla collettività. In un'ottica di prevenzione, poi, questo genere di processi non ha alcuna efficacia, in quanto sono e rimangono episodi isolati che non contribuiscono alla funzione di prevenzione speciale e generale, attribuita dall'ordinamento alla sanzione penale. Senza dimenticare che, sempre dal punto di vista giuridico, un approccio quantomeno discutibile verso il profilo soggettivo degli autori di reati in rete, non contribuisce neppure alla dinamicità ed al buon esito dell'attività di investigazione.

Da un lato, quindi, il rischio di proporre una nuova sfida per quanti confidano nell'anonimato garantito dalla rete e nelle risapute, notevoli difficoltà di investigazione dei reati e degli abusi commessi con l'ausilio delle nuove tecnologie, dall'altro la possibilità reale di un'applicazione non obiettiva della norma penale.

Quanto detto finora, compresi i rischi che si è cercato di delineare, seppur per sommi capi, nasce da una riflessione sui contenuti dei profili criminologici. Di non minore importanza sono però le considerazioni relative alla metodologia utilizzata, o meglio al come e sulla base di quali elementi si può arrivare a stilare un profilo soggettivo, in specie se criminologico.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in Ciberspazio e Diritto, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

4. Osservazioni generali sulla metodologia dei profili criminologici.

Un primo dubbio è legato alla quantità ed alla qualità dei dati disponibili: è innegabile che, al momento, sono ridotte, e comunque frammentarie, le informazioni sulle reali dinamiche criminali che afferiscono alla diffusione delle nuove tecnologie. Per quanto vi sia una circolazione aperta di notizie sul tema, questo non vuol dire che si tratti necessariamente di elementi suscettibili di dar vita ad un profilo soggettivo attendibile, a livello contenutistico e metodologico. Vale a dire che è vero che sono oramai quotidiani i casi del ragazzino che riesce a rubare il numero di carta di credito al Bill Gates di turno, dello studente universitario che si è arricchito con i *banner* pubblicitari gestendo una quantità non indifferente di *file* musicali pirata, o ancora del giovane che, per sua stessa ammissione, è riuscito per sbaglio a sviluppare e diffondere un *virus* in grado di paralizzare i computer di mezzo mondo: ma non è questo il genere di informazioni che può dar vita ad un profilo definibile come criminologico. E forse è il caso, per onestà scientifica, di accettare il fatto che, allo stato attuale, non è possibile stilare alcuno che possa essere suscettibile di applicazione alla generalità dei casi.

Per spiegare quest'ultima affermazione è necessario un passaggio preliminare che dia conto dell'essenza, delle finalità e del metodo della criminologia.

Tratto distintivo di quest'ambito del sapere è la sua caratteristica di scienza empirica, vale a dire la sua profonda aderenza alla realtà attraverso la sua osservazione diretta; questo non significa che non si tratti anche di una scienza speculativa, quanto piuttosto che non si basa su speculazioni concettuali. La criminologia studia e analizza il contesto da indagare, valuta i dati che raccoglie, o che le vengono forniti da altre scienze, e li interpreta, tenendo sempre presente il sistema socio-valoriale da cui tali dati originano. Questo per evidenziare che la criminologia non può prescindere, al tempo stesso, dal contatto con la dimensione empirica, individuale e collettiva, come da un approccio di tipo filosofico. Per quanto riguarda la metodologia e le fonti, non esiste un metodo unico, valevole per tutti i casi, così come sono varie e diversificate le fonti. Queste ultime spaziano dalle statistiche di massa all'osservazione individuale - tipica della criminologia clinica - allo studio di gruppi-campione, alle ricerche partecipate, alle interviste - dirette o a mezzo questionario -, alle ricerche operative e sperimentali, alle indagini catamnestiche, solo per citarne alcuni. Ci sono, inoltre, gli studi predittivi, finalizzati all'individuazione dei fattori e dei parametri che permettono di tracciare le possibili linee di sviluppo di un determinato fenomeno criminale. Il tutto perché la criminologia prova ad indagare il cosiddetto numero oscuro della criminalità, vale a dire quel *quantum* di crimini che vengono commessi ma che, per diversi motivi, non emerge dalle fonti ufficiali di informazione; motivi che possono essere legati ai fatti delittuosi, alle vittime ma anche agli autori.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

Da dove nasce, quindi, un profilo criminologico? Così come inteso dalla criminologia clinica che ne è l'ambito di elezione, un profilo necessita di un rapporto diretto con l'autore, finalizzato alla comprensione delle specificità soggettive ma anche all'accertamento di tutta una serie di fattori socio-culturali e ambientali che possono avere rilevanza, più o meno diretta. Tale contatto è legato, nella maggior parte dei casi, all'*iter* processuale nel quale il reo, o presunto tale, si trova ad essere coinvolto e presuppone che a procedere sia una persona per così dire 'competente', opportunamente formata per tali tipologie di analisi. L'osservazione di più episodi individuali permette poi, in presenza di concreti elementi comuni, di stilare profili di più ampia portata, valevoli per una generalità di casi e soggetti e soprattutto suscettibili di svolgere una funzione per così dire predittiva.

Ciò considerato, i motivi dei dubbi sull'attendibilità metodologica dei profili criminologici degli *hacker* divengono intuibili.

In primo luogo, molti dei profili diffusi non provengono da criminologi o comunque da addetti ai lavori, vale a dire da persone che possano rispondere anche del metodo usato per arrivare alle loro deduzioni. Certo un *ex hacker* o un *hacker* possono essere una preziosa fonte di informazioni, ma non gli autori di un profilo criminologico; sarebbero giustificati i dubbi sull'imparzialità delle loro deduzioni, così come sulla possibilità effettiva di generalizzare quella che è comunque solo un'esperienza personale che, per quanto attendibile e importante, non può essere sufficiente per rappresentare un fenomeno di tale portata e complessità quale è la criminalità informatica.

In secondo luogo, c'è un reale problema di quantità e qualità delle fonti; i precedenti giurisprudenziali non sono ancora in grado di assolvere, specie nel contesto europeo, ad un possibile ruolo di collettori di informazioni sugli *hacker*: il numero esiguo e la rilevanza alquanto contenuta dei casi di specie trattati, la contestabilità di talune decisioni, sono solo alcuni dei limiti. Manca inoltre, ad esempio, il contatto con la criminalità informatica per così dire dei 'colletti bianchi'; che senso può avere tracciare un profilo su uno studente che gestisce un sistema commerciale basato sull'*Internet mail order*, facendolo diventare un criminale informatico, quando Internet è il mercato della pedo-pornografia, caratterizzato da un'offerta spesso gestita a livello organizzato? Allo stesso modo, qual è la funzione di un profilo soggettivo basato su questo genere di casistica, quando esiste una rete di insospettabili professionisti che dalle loro scrivanie riciclano via Internet quantità di denaro impensabili? Restando nell'ambito della criminalità economica, non si può non riparlare di tecniche di concorrenza sleale attraverso l'attacco diretto della proprietà intellettuale e del *know-how* aziendale; dietro questo genere di fattispecie ci sono persone in grado di realizzarle tecnicamente ma anche di far valere, economicamente, le proprie competenze ed il rischio che corrono. Senza considerare che la loro responsabilità va divisa con insospettabili committenti che fanno parte del mondo imprenditoriale.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in Ciberspazio e Diritto, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

Ridurre la realtà in schemi concettuali e paradigmi di riferimento è senza dubbio necessario ed utile, ma mai come per Internet è necessario evitare catalogazioni statiche che mal si adattano, anche a prima vista, ad una realtà mutevole e dall'evoluzione inarrestabile.

5. Considerazioni conclusive.

Le osservazioni che compongono questo lavoro non sono finalizzate alla condanna di ogni tentativo di individuare tratti generali di riferimento, per approfondire la conoscenza dei criminali informatici. Il fine è piuttosto quello di evidenziare come talune conclusioni siano approssimative e talvolta fuorvianti, al punto che sarebbe forse auspicabile un approccio alternativo, con meno pretese di universalità ma maggiormente aderente al dato empirico. Vale a dire che andrebbero tracciati profili, non necessariamente criminologici in senso stretto, per singole fattispecie per le quali sono disponibili elementi di conoscenza attendibili. Questo sarebbe espressione di maggiore serietà scientifica e onestà metodologica, e soprattutto sarebbe di maggiore utilità.

La proposta è quella di evitare inutili distinzioni, spesso di difficile collocazione concettuale, per guardare ai cybercriminali come divisi, essenzialmente, in due categorie: quelli che lo sono quasi per caso e quelli che, al contrario, lo sono per scelta. I primi ricomprendono quanti commettono reati quasi inconsapevolmente, talvolta perché non padroneggiano la tecnologia e non comprendono appieno le conseguenze di talune loro condotte; i secondi, invece, non solo hanno competenze informatiche approfondite ma sono mossi da finalità criminali, sempre più spesso accompagnate dal fine di lucro. È questa una distinzione che, ben lontana dal voler essere scientifica, muove da una convinzione di fondo: non è la tipologia di *attacker* a determinare la dannosità e la lesività di una condotta, così come non si possono misurare queste ultime sulla base del livello di alfabetizzazione informatica. Talvolta un attacco sferrato senza piena cognizione di causa può essere molto più dannoso di un attacco, tecnicamente più complesso, ma studiato per ottenere un certo risultato e quindi circoscritto solo ad alcune funzioni. Molto dipende, poi, anche dal contesto che viene colpito, dalla vittima, dalle circostanze spazio-temporali entro cui si colloca il fatto e da tutta una serie di altri elementi, comunque legati al caso di specie.

L'impossibilità di indagare in modo soddisfacente il profilo degli autori dei crimini informatici, quindi, dovrebbe almeno per ora far convergere risorse e attenzioni verso la conoscenza, sempre più approfondita, delle modalità di attacco e delle singole, diverse fattispecie. Maggiore attenzione dovrebbe essere riservata al perfezionamento delle tecniche di investigazione, dato che il reato informatico non è poi così diverso da una scena del crimine: per risolvere il caso è indispensabile riconoscere tempestivamente le prove, imparare ad interpretarle e a conservarle. In questo, la stessa tecnologia è di innegabile ausilio, fino al punto che proprio la

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è I cybercriminali: rischi e limiti dei profili criminologici, Mara Mignone, in Ciberspazio e Diritto, Volume I, Numero II, pp. 3-15. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

tecnologia può permettere di tracciare il percorso a contrario: dal danno, quale conseguenza dell'azione criminosa, al suo autore. È una sfida. I criminali sono sempre un passo avanti e hanno ampiamente dimostrato di saper sfruttare a proprio favore l'innovazione tecnologica; si tratta di vedere se è possibile ridurre le distanze, grazie proprio tanto ad un diverso approccio conoscitivo quanto alle nuove tecnologie. Questo anche in un'ottica di sviluppo di misure e *policy* di prevenzione e riduzione del rischio, a tutela della sicurezza.