RASSEGNA ITALIANA DI CRIMINOLOGIA

ANNO VI N.3 2012

Nuove prospettive di ricerca in materia di atti persecutori: il fenomeno del cyberstalking

New research perspectives about stalking: the phenomenon of cyberstalking

Laura De Fazio • Chiara Sgarbi

Parole chiave: atti persecutori • molestie • cyberspazio • cyberstalking • Internet

Riassunto

Le molestie telematiche rappresentano un fenomeno frequente e degno di interesse scientifico e sociale, strettamente correlato al costante ed esponenziale progredire della tecnologia.

Queste tipologie di condotte sono definite dalla letteratura cyberstalking, intendendo con questo termine, pur in assenza di una definizione univoca, l'utilizzo di internet, email o di altri dispositivi elettronici per molestare un'altra persona. Si tratta di una problematica rilevante, destinata a diventare sempre più complessa e pericolosa con l'aumento inarrestabile dell'utilizzo di Internet e delle tecnologie informatiche da parte di fasce sempre più ampie di popolazione. Un più facile e veloce accesso al cyberspazio comporta anche un maggior rischio di utilizzo erroneo o di abusi del mezzo, al fine di aggredire o intromettersi nella vita di altre persone, approfittando dell'anonimato e dell'assenza dei limiti presenti in un contesto reale.

Sul piano della prevalenza, seppur numericamente limitati, gli studi empirici esistenti dimostrano una non trascurabile incidenza del fenomeno e una prevalente mancanza di consapevolezza da parte della popolazione generale. Il Report pubblicato dall'Attorney General statunitense nel 1999, stimava la presenza nel paese di circa 475.000 vittime di cyberstalking all'anno, mentre la Polizia riferiva la presenza nel 20% dei casi di molestie rilevati di forme di abuso via Internet e mezzi tecnologici in genere

In un'ottica, quindi, di prevenzione e di intervento sembra indispensabile approfondire e implementare la ricerca sul fenomeno, tenuto conto del fatto che raramente queste molestie restano limitate al mondo virtuale, essendo in grado di produrre effetti reali talvolta analoghi se non più gravi rispetto a quelli dello stalking offline.

Keywords: stalking • harassment • cybespace • cyberstalking • Internet

Abstract

Electronic stalking is a frequent phenomenon worthy of scientific and social interest, closely related to the constant and exponential progress of technology.

These types of conducts are defined by literature as cyberstalking, and even if it has no one universally agreed upon definition, it is considered as the use of the internet, email, or other electronic devices to stalk another person. Today, it seems to be a serious problem that will become more complex and dangerous as more people take advantage of the Internet and other telecommunications technologies. An easier and faster access to cyberspace also means a greater risk of incorrect use or misuse of the medium, in order to attack or intrude into the lives of others, taking advantage of anonymity and of the absence of limitations present in a real context.

Even if empirical works on cyberstalking are still few, the existing data gives evidence of its quantitative importance and of a lack of awareness. The Report published by the US Attorney General in 1999, estimated the presence in the country of about 475.000 victims of cyberstalking each year, while police reported the presence in 20% of cases of reported harassment forms of abuse through Internet and technological means in general.

In a perspective of prevention and intervention, investigating and implementing the existing research on the phenomenon seem essential, taking into account that such harassment are rarely limited to the virtual world, being able to produce effects often similar if not more severe than those produced by offline stalking.

Per corrispondenza: Laura De Fazio, Dipartimento di medicina legale e criminologia, L.go del Pozzo 71, 41100, Modena, Tel. 059/4224880 - e-mail • *defazio.laura@unimore.it*

LAURA DE FAZIO, Professore Associato di Criminologia, Università degli Studi di Modena e Reggio Emilia
CHIARA SGARBI, Dottore di Ricerca Europeo in Scienze Giuridiche, Assegnista di ricerca, Università degli Studi di Modena e Reggio Emilia

Nuove prospettive di ricerca in materia di atti persecutori: il fenomeno del cyberstalking

1. Introduzione

Internet e la tecnologia in generale rappresentano oggi un eliminabile aspetto del vivere sociale, in grado di modificare e permeare in maniera totale la nostra quotidianità (McFarlane & Bocij, 2003).

La c.d. "rivoluzione delle comunicazioni", informatica e digitale (Spitzberg & Hoobler, 2002; Bocij, 2004), già in atto sul finire del ventesimo secolo, ha condotto alla nascita di nuovi strumenti per la comunicazione ed allo sviluppo e miglioramento di quelli già esistenti. Il crescente utilizzo del computer e dei mezzi informatici, unitamente alla inarrestabile espansione del web, ha rivoluzionato non soltanto le modalità di comunicazione ma anche le dinamiche di interazione interpersonale (Phillips & Spitzberg, 2010), consentendo in modo rapido ed illimitato di entrare in contatto con altre persone e di accedere ad una vasta gamma di informazioni (MacKenzie, Mullen, Pathè & Purcell, 2003).

Se l'apporto positivo e democratico delle nuove tecnologie è innegabile, tuttavia gli effetti negativi o addirittura pericolosi legati all'espansione degli strumenti informatici sono inevitabili e connaturati all'essenza stessa del mondo telematico: Internet ha, infatti, aperto le porte ad opportunità criminali precedentemente sconosciute, in grado di trascendere i limiti e i confini fisici dell'agire umano, espressione di un "lato oscuro" della tecnologia (Merschman, 2001; Pittaro, 2007).

L'economicità, la facilità d'accesso e l'anonimato trasformano il cyberspazio in un polo d'attrazione per l'agire deviante (Merschman, 2001), fino a produrre nuove fattispecie di reato o modalità alternative di espressione di condotte illecite preesistenti (Basu & Jones, 2007). Da sempre il crimine professionale accede ai nuovi mezzi di comunicazione ed interazione a disposizione al fine di migliorare e rendere maggiormente efficaci le proprie azioni tradizionali (Lessig, 1999; Di Luciano, 2007). Allo stesso tempo, la rivoluzione tecnologica in atto ha favorito anche l'emergere e il successivo riconoscimento sociale ed istituzionale di nuovi e peculiari reati, tali proprio perché commessi all'interno e per mezzo della rete. Si tratta di un ampio numero di illeciti riconducibili alla generale categoria dei "cyber crimes" o "computer crimes", ossia un insieme di condotte di molteplice natura poste in essere attraverso l'ausilio, o meglio, l'abuso del mezzo informatico. A titolo esemplificativo ma non esaustivo, trattandosi di tipologie di reato in esponenziale aumento, sotto tale etichetta possono ricondursi (Carducci, 2011): l'accesso illegale ai sistemi informatici attraverso atti di pirateria (es. hacking), lo spionaggio e il sabotaggio dei sistemi informatici (es. netstrike), il terrorismo online (cyberterrorismo), il riciclaggio di proventi illeciti (cyberlaundering), le frodi e le truffe online (es. spamming, phishing, clonazione carte di credito), la riproduzione abusiva di programmi informatici o di opere intellettuali, la prostituzione e la pedopornografia online (cyberpedofilia), il gioco d'azzardo online (online gambling), per finire con le forme di molestie e disturbo telematico quali il cyber bullismo, il cyberharassment e, soprattutto, il cyberstalking.

L'espansione del web e del cyberspazio ha infatti sicuramente contribuito ad ampliare gli strumenti a disposizione dello stalker al fine di sviluppare la campagna persecutoria, con un potenziale incremento delle possibilità di intrusione interpersonale attuabili attraverso i mezzi tecnologici (Basu & Jones, 2007, De Fazio & Sgarbi, 2009[a]). Rispetto a questa categoria di autori di reato, Internet è divenuto lo strumento ideale per intimidire, minacciare e molestare (D'Ovidio & Doyle, 2003; Pittaro, 2007), facilitando, attraverso l'anonimato e in assenza delle restrizioni e dei limiti imposti dalle barriere fisiche, il perpetrarsi di condotte abusive.

Il cyberstalking, definibile, come "l'utilizzo di internet, della posta elettronica o di altri dispositivi di comunicazione elettronica per molestare un'altra persona attraverso una condotta minacciosa e ripetuta" (Reno, 1999), dopo aver suscitato inizialmente l'interesse quasi esclusivo dei media americani ha successivamente acquisito il ruolo di tematica di rilevanza scientifica e sociale. Il Report presentato dall'Attorney General nel 1999 al vicepresidente USA rappresenta il primo documento ufficiale in grado di riportare i dati concreti sulla diffusione del fenomeno e sulla necessità di interventi legislativi diretti a combatterlo e a limitarne le conseguenze (Di Luciano, 2007), in una prospettiva federale oltre che statale.

Da semplice modalità di espressione di attività persecutorie, a seguito della continua ed esponenziale espansione dei media informatici, il cyberstalking ha quindi finito per trasformarsi in un'autonoma fattispecie comportamentale (Basu & Jones, 2008), non rappresentando più semplicemente una replica nel mondo virtuale dello stalking reale e assumendo un proprio carattere alimentato da un ambiente in cui l'anonimato e la pseudonymity, ossia la possibilità di crearsi un'identità virtuale, sono la norma.

In un contesto di inarrestabile diffusione dello stalking elettronico, a fronte del riconoscimento della sua pericolosità, si sono susseguite anche le risposte legislative, giungendo all'emanazione di vere e proprie autonome regolamentazioni in materia (es. Florida, North Carolina) o prevedendo esplicitamente riferimenti alle modalità telematiche di molestia all'interno di leggi generali sullo stalking o sull'harassment (es. Regno Unito).

Nel nostro paese, l'interesse per questo tipo di condotte appare sicuramente limitato e molto recente (De Fazio 2009, 2011), diretta conseguenza dell'altrettanto recentemente acquisita consapevolezza mediatica, scientifica ed istituzionale della diffusione del fenomeno dello stalking, tale da condurre nel 2009 all'introduzione nel codice penale italiano dell'articolo 612bis in materia di atti persecutori (De Fazio, Merafina & Sgarbi, 2009[b]).

Questo lavoro si propone quindi di colmare parzialmente questa lacuna, dovuta all'esiguità numerica dei contributi scientifici sul tema, offrendo un quadro generale sulla letteratura esistente, soffermandosi sui diversi aspetti qualificanti le molestie telematiche al fine di descrivere in maniera sintetica ed efficace un fenomeno talvolta complicato e di incerta definizione e riconoscibilità.

2. Cos'è il cyberstalking? Definizione e natura del fenomeno

Le molestie telematiche rappresentano un fenomeno assai frequente e degno di interesse scientifico e sociale, strettamente correlato al costante ed esponenziale progredire della tecnologia. In questo contesto, dobbiamo infatti riconoscere che lo sviluppo delle cosiddette nuove tecnologie di comunicazione ha offerto allo stalker nuovi ed infiniti strumenti per porre in essere le condotte persecutorie.

Le peculiarità delle "computer mediated communication" (CMC) e della rete rendono sicuramente più efficace e semplice raggiungere l'obbiettivo delle molestie, a fronte della riconosciuta illimitata fantasia dell'autore in grado di individuare e scoprire sempre nuovi strumenti di azione.

Tuttavia, come accade per lo stalking in generale, queste tipologie di condotte pongono una serie di problematiche dal punto di vista definitorio, trattandosi di fenomeni costituiti da una pluralità di comportamenti intrusivi e ripetuti, destinati a modificarsi con il costante ed inarrestabile evolversi del mondo della tecnologia (Bocij, 2004).

Il concetto di cyberstalking risulta essere tuttora incerto e dibattuto, in assenza di una definizione univoca ed universalmente accolta (Reno, 1999; McFarlane & Bocij, 2003; Pittaro, 2007), e a fronte di due prevalenti posizioni all'interno del contesto scientifico, distinguendo tra chi ritiene semplicemente si tratti di una variazione o di un'estensione dello stalking offline (Jenson, 1996; Lee, 1998; Petherick, 2007; Pittaro, 2007; Clough, 2010), e chi invece lo considera un fenomeno nuovo, autonomo e separato da quello tradizionale, ancorché ad esso collegato (Westrup, 1998; Fisher, Cullen & Turner, 2000; Bocij 2002, 2003, 2004; Bocij & McFarlane, 2002; D'Ovidio & Doyle, 2003; Petrocelli, 2005; Chick, 2008; Moore, 2011).

Un primo tentativo ufficiale di definizione, richiamata da molti autori impegnati nello studio di queste tematiche (Spitzberg & Hoobler, 2002; D'Ovidio & Doyle, 2003; Wykes, 2007; Pittaro, 2007), è reperibile all'interno del Report on Cyberstalking, redatto dall'Attorney General Janet Reno (1999) su richiesta dell'allora Vicepresidente USA Al Gore. All'interno di questo documento, diretto a riferire sulla diffusione e sulle strategie di intervento, il fenomeno è definito, utilizzando quale riferimento principale gli elementi individuanti il concetto di stalking, come "l'utilizzo di Internet, della posta elettronica o di altri dispositivi di comunicazione elettronica[1] per molestare un'altra persona attraverso una condotta minacciosa e ripetuta" (Reno, 1999; Di Luciano, 2007).

Prendendo spunto da questa prima indicazione, seguendo in ordine cronologico le due prevalenti posizioni interpretative, molteplici sono le definizioni reperibili nella letteratura esistente.

Come già accennato, un primo gruppo di autori considera il cyberstalking come l'espressione nel cyberspace o come un'altra fase di un più generico pattern comportamentale di stalking (Jenson, 1996; Finn & Banach, 2000; Ogilvie, 2000; Aggarwal, Burmester, Henry, Kermes & Mulholland, 2005; Burgess & Baker, 2002; Wykes, 2007), cui spesso è legato o a cui frequentemente si accompagna (Lee, 1998), o come uno, anche se il più nuovo, "dell'infinito numero di metodi che uno stalker può utilizzare per terrorizzare la sua vittima" (Merschman, 2001). Fondamentalmente si tratterebbe, quindi, di una modalità high-tech di esecuzione delle condotte persecutorie, al fine di raggiungere gli stessi obbiettivi normalmente perseguiti dal molestatore nel mondo reale (Meloy, 1998; Adam, 2002; Petherick, 2007; Mcgrath & Casey, 2002; Clough, 2010; Haron & Yusof, 2010).

Tavani e Grodzinsky (2002), nel valutare gli aspetti etici dello stalking online, ritengono che tali condotte non rappresentino né un computer crime e né un nuovo reato, ma piuttosto un computer-related crime, intendendo per tali le ipotesi in cui l'autore di reato utilizzi nuovi strumenti d'azione forniti dalla espansione ed evoluzione delle tecnologie informatiche.

Sheridan e Grant (2007), a loro volta, attraverso uno studio sulla cyber-vittimizzazione, confermano la totale sovrapponibilità delle due tipologie di molestie, online e offline, descrivendo il cyberstalking non come un'entità autonoma con caratteristiche proprie ma come "un'arma aggiuntiva nell'artiglieria dello stalker", una tecnica di persecuzione più invasiva, ritenendo pertanto del tutto inutile tentare di definire queste condotte in modo preciso e universale.

Considerando i limitati contributi sul tema reperibili nel nostro paese, Di Luciano (2007), prendendo spunto dalla definizione contenuta nel Report del 1999, ritiene che lo stalking elettronico sia una semplice espressione cyber delle molestie offline, all'interno della cui categoria di condotte andrebbe ricompreso, con la semplice differenza che in questi casi il mezzo informatico si interpone tra l'autore del crimine e la vittima o rappresenta lo strumento principale per eseguire un'azione criminale. Anche MacKenzie et al. (2003), all'interno del volume a cura di Galeazzi, Curci e Secchi sulle molestie assillanti, hanno definito lo "stalking telematico" come una forma di comunicazione indesiderata, la cui diffusione è stata favorita dalle conquiste della tecnologia informatica che contribuirebbero a facilitare lo stalking e a trasferire successivamente le molestie dalla realtà virtuale a quella fisica.

Secondo questa parte della letteratura, quindi, la valutazione e la gestione delle condotte e dei fenomeni riconducibili al concetto di cyberstalking risulterebbero indissolubilmente connesse alle problematiche e alle strategie di intervento sviluppatesi in relazione alle più tradizionali forme di stalking, face to face o prossimico, dal quale non si differenzierebbe in termini né di obbiettivi e né di effetti e conseguenze.

1 Il Codice Penale dello stato della California, sezione 646.9(h), riconosce quali dispositivi di comunicazione elettronica, pur non limitandosi ad essi: telefoni, cellulari, computer, strumenti per la video registrazione, fax e cercapersone. Analoga è la previsione presente nel Codice degli Stati Uniti (Titolo 18, sezione 12 e 1250).

Chi invece appartiene alla seconda categoria di autori, ritiene le precedenti interpretazioni alquanto semplicistiche e difficilmente adattabili alla reale natura delle molestie telematiche.

In particolare Bocij (2002, 2003, 2004), a sostegno del riconoscimento di una autonoma fattispecie comportamentale o di reato, riferisce due principali motivi: da un lato il cyberstalking rappresenta il risultato della maggiore diffusione di nuovi strumenti tecnologici in grado di offrire nuove opportunità illecite; dall'altro la tendenza dei comportamenti associati al cyberstalking a presentare differenze rispetto a quelli associati allo stalking "convenzionale".

L'autore (2002, 2004), ritenendo tutte le precedenti insoddisfacenti e talvolta errate, fornisce una definizione formale e maggiormente comprensiva di cyberstalking, inteso come: "un insieme di comportamenti nei quali una persona, un gruppo di persone o un'organizzazione utilizzano le information and communications technology (ICT) per molestare un'altra persona, o un altro gruppo di persone o un'altra organizzazione. Questi comportamenti potrebbero includere, in modo esemplificativo e non esaustivo, l'invio di minacce o di false accuse, il danneggiamento di dati o di attrezzature, furti d'identità o di dati, il controllare altri computer, l'adescamento di minori per scopi sessuali e via dicendo. Con il termine molestie (harassment) si intendono quelle condotte a fronte delle quali una persona ragionevole riterrebbe di causare ad un'altra persona un ragionevole stress emotivo".

Analoga è la descrizione di queste condotte rinvenibile in altri contributi accademici (D'Ovidio & Doyle, 2003; Hitchcock, 2003; Finn, 2004; Southworth, Finn, Dawson, Fraser & Tucker, 2007; Chik, 2008; Moore, 2011), dove con il termine cyberstalking viene inteso l'uso ripetuto di internet, delle mail o di altri mezzi di comunicazione elettronica (digital elctronic communication), al fine di minacciare, spaventare o molestare un individuo o un gruppo di individui. Si tratterebbe quindi di una forma di molestia online posta in essere attraverso una serie di condotte non volute ed intrusive (Westrup, 1998; Joseph, 2003), priva di alcuno scopo legittimo, in grado di causare alla vittima un sostanziale stress emotivo.

Diversi autori (Bocij & McFarlane, 2002; Philips & Morrissey, 2004), analizzando tali modalità di abuso, utilizzano in maniera interscambiabile i termini cyberstalking o cyberharassment, intesi quali forme di molestie in forza delle quali le vittime possono sentirsi disturbate, stressate o, addirittura, temere per la propria vita, attuate attraverso comportamenti molesti che vanno dal continuo contatto indesiderato alla minaccia di violenza o, ancora, al tentativo di controllare i comportamenti o lo stile di vita di una persona. Anche Jaishankar e Sankary (2006) offrono una definizione generale di cyber molestie, limitando tuttavia l'azione del cyberstalker al mondo virtuale, escludendo il rischio di una minaccia fisica e diretta per la vittima, trattandosi di un inseguimento esclusivamente online diretto ad ottenere informazioni o a minacciare e intimidire.

A fronte di queste definizioni, sembrerebbe più corretto, invece, considerare il cyberharassment come un elemento del cyberstalking, ossia di una complessa forma di inseguimento virtuale posto in essere lungo un arco di tempo, per il tramite di uno o più mezzi di comunicazione elettronica, causando nella vittima un ragionevole timore (Mccall, 2004).

Basu e Jones (2007), in mancanza di una definizione universalmente accolta, seguono la tripartizione dei cyber crime offerta da Wall (2005), distinguendo tre differenti ipotesi: cyberstalking come semplice variante online dello stalking tradizionale; cyberstalking come "crimine ibrido", risultato di nuove modalità di espressione di condotte criminali preesistenti offerte dalla trasformazione tecnologica; cyberstalking come vero e proprio nuovo cyber reato prodotto diretto dell'uso di internet e perpetrabile solo nel cyberspace. Analizzando approfonditamente il fenomeno, gli autori giungono ad escludere la prima e la seconda ipotesi, sottolineando come il cyberstalking presenterebbe importanti differenze qualitative rispetto allo stalking ordinario, sostanziandosi attraverso un'ampia serie di comportamenti e producendo specifici effetti non associabili alle forme persecutorie offline (Basu & Jones, 2007).

Per concludere, generalmente accolta e frequentemente citata è la definizione offerta da una risorsa online costituita a garanzia della sicurezza di Internet. Il sito web CyberAngels (2000), infatti, fornisce un'autonoma definizione di cyberstalking, elencando una serie di fattori identificativi delle attività persecutorie online. L'individuazione di un'ipotesi di cyberstalking sarebbe quindi subordinata alla presenza di alcune o tutte le seguenti caratteristiche: dolo, premeditazione, ripetizione, angoscia, ossessione, vendetta, assenza di uno scopo legittimo, persistenza nonostante le richieste di smettere da parte della vittima cui si rivolgono individualmente le condotte, molestie e minacce (Spitzberg & Hoobler, 2002). Tale definizione, tuttavia, pur riguardando direttamente la specifica fattispecie in oggetto, riconoscendo esattamente gli elementi costitutivi e l'importante ruolo rivestito dalle moderne tecnologie, presenta indubbiamente alcune incoerenze che ne compromettono la validità, come ad esempio il fatto che la vittima debba chiedere al molestatore di smettere, in genere sconsigliato o non sempre possibile, o l'idea che queste condotte si indirizzino solo nei confronti di singole persone, mentre in realtà in molti casi oggetto di molestie online sono gruppi di persone.

Considerato l'approccio descrittivo di questa rassegna, resta innegabile, soprattutto in relazione alla formulazione di specifiche normative in materia oltre che per l'implementazione della ricerca, l'esigenza di giungere ad una definizione il più possibile precisa e coerente del fenomeno, pur avendo presente le difficoltà insite nella natura della fenomenologia in oggetto e l'estrema differenziazione delle posizioni scientifiche esistenti.

3. Diffusione e incidenza del cyberstalking

Nonostante i media negli ultimi anni si siano più volte occupati del "lato oscuro" di Internet, la ricerca sul cyberstalking risulta ancora limitata, soprattutto relativamente allo studio della sua diffusione e prevalenza all'interno della popolazione generale.

Al di là della corposa aneddotica a disposizione, infatti, tali fenomeni appaiono di difficile rilevazione, sia per una ancora limitata consapevolezza delle vittime che per l'elevato livello di anonimato che caratterizza queste tipologie di condotte (Basu & Jones, 2007; Pittaro, 2007).

Tuttavia, l'evolversi incessante della tecnologia e il mol-

tiplicarsi degli episodi di molestie telematiche con il passare degli anni conducono a considerare il cyberstalking una problematica sociale reale, destinata a crescere in maniera esponenziale con la ormai inarrestabile diffusione dei media informatici (Reno, 1999; Spitzberg & Hoobler, 2002; Jaishankar e Sankary, 2006; Pittaro, 2007).

I dati a disposizione, oltre che da studi epidemiologici riguardanti specificamente il cyberstalking o lo stalking offline (Ellison, 2001; Alexy, Burgess, Baker & Smoyak, 2005; Pittaro; 2007), provengono spesso da statistiche fornite dagli stessi Internet Service Provider (ISP), dalle Forze dell'ordine o dalle organizzazioni online a sostegno delle vittime.

La prima fonte ufficiale in grado di fornire dati nazionali sull'estensione e la pericolosità del fenomeno è rappresentata dal rapporto(Reno, 1999) stilato dall'Attorney General degli Stati Uniti d'America nel 1999, in risposta ad una specifica richiesta proveniente dal Vice Presidente Al Gore. Sulla base dei dati rilevabili dagli studi sullo stalking in generale, stimando che, al tempo, negli Stati Uniti vi fossero più di 80 milioni di adulti e 10 milioni di bambini con accesso ad Internet, si ipotizzava, in maniera speculativa, la presenza nel paese di circa 475.000 vittime di stalking telematico all'anno (Bocij, 2004; Glancy, Newman, Potash & Tennison, 2007; Pittaro, 2007;). Accanto a queste stime, il Report citava anche i dati forniti dalle Forze di polizia e dalle agenzie di pubblica sicurezza[2], secondo le quali in un 20% dei casi di molestie rilevati si sarebbero riscontrate anche forme di abuso attuate attraverso Internet e i mezzi tecnologici in genere (Merschman, 2001; Spitzberg & Hoobler, 2002; Joseph, 2003; Bocij, 2004).

Questi dati appaiono confermati dallo studio epidemiologico condotto nel 2006 dal Bureau of Justice Statistics (BJS) del Dipartimento di Giustizia americano (Baum, Catalano & Rand, 2009), ad integrazione del National Violence Against Women Survey (Tjaden & Thoennes, 1998). Gli autori, analizzando la prevalenza dello stalking e delle molestie in un campione di popolazione generale[3], ricercano espressamente la presenza di condotte moleste online, riferendo approssimativamente 1 caso di cyberstalking ogni 4 vittime. Rispetto alle singole condotte: l'83% riferiva molestie via e-mail, il 35% via sms, il 46% e il 10% rispettivamente denunciava l'utilizzo da parte dello stalker di una videocamera nascosta e di un GPS per monitorare e sorvegliare.

Da un punto di vista non governativo, altre statistiche vengono fornite dalle organizzazioni internazionali a sostegno delle vittime di cyberstalking, come ad esempio l'associazione no-profit americana Working to Halt Online Abuse (WHOA) (2011) che, sulla base delle richieste di aiuto ricevute da tutto il mondo, riferisce dai 50 ai 75 casi alla settimana. Anche CyberAngels (2003), a sua volta, offre dati interessanti sulla diffusione delle molestie telematiche, ricevendo già nel 2000 più di 400 richieste di aiuto all'anno e stimando, sulla base della popolazione degli Stati Uniti, l'esistenza di 63mila cyberstalker e 474mila vittime (Aftab, 2001; Spitzberg & Hoobler, 2002; Bocij, 2004).

2 Tra queste: FBI, Los Angeles District Attorney's Office; Sex Crimes Unit of Manhattan District Attorney's Office; Stalking and Threat Assessment Unit and Computer Investigation and Technology Unit of the New York City Police Department.

3 N=65270 adulti (> 18 anni).

Al di là delle statistiche ufficiali, denunciata la carenza di studi sul tema fino alla fine degli anni 90, diversi autori hanno dedicato la propria attività scientifica ad indagare questi profili fenomenologici pericolosi e numericamente in aumento.

Prendendo avvio dalla letteratura sullo stalking in generale, pochissimi sono i riferimenti espliciti al cyberstalking (Glancy, Newman, Potash & Tennison, 2007). Mullen et al. (1999) rilevano l'utilizzo di email da parte di 2 dei 145 stalker oggetto della loro indagine, così come analogamente Kamphuis ed Emmelkamp (2001) riportano un 2% di vittime (N=235) perseguitate attraverso Internet, mentre Fisher et al. (2002) individuano in un campione di studentesse di College (N=581) vittime di stalking un 24.7% di casi di molestie effettuate via mail.

I primi studi ad occuparsi in maniera esplicita del potenziale pericolo dell'utilizzo delle tecnologie informatiche si sono concentrati su specifiche categorie di vittime, coinvolgendo prevalentemente popolazioni giovanili o studenti di college ed università. In un'indagine telefonica riguardante 1500 giovani tra i 10 e i 17 anni, utenti di Internet (Finkelhor, Mitchell & Wolak, 2000), diretta a rilevare il rischio di vittimizzazione on line, il 6% del campione aveva subito nell'ultimo anno molestie online, un quarto delle quali in grado di generare timore o angoscia. Quasi un terzo, invece, dei 235 studenti di scienze della comunicazione coinvolti nella ricerca di Spitzberg e Hoobler (2002) sul cyber-obessional pursuit (COP) aveva riferito qualche forma di molestia posta in essere attraverso il computer o altri mezzi elettronici, con un 18% di messaggi di tipo sessuale e un 3% di minacce.

Burgess e Baker (2002), a loro volta, hanno condotto uno studio su 656 studenti universitari, riportando un 11% di soggetti molestati, per la maggior parte di sesso femminile (61%), con una presenza di e-mail indesiderate, spesso di tipo sessuale, nella metà dei casi e solo una ridotta percentuale di minacce di violenza fisica. Analogamente Finn (2004), in un campione di 339 studenti, ha individuato una percentuale compresa tra il 10 e il 15% di soggetti che avevano ripetutamente ricevuto e-mail e comunicazioni via Messenger (Instant Messages) contenenti insulti, minacce e molestie, e nel 59% dei casi riferimenti sessuali e pornografici. Alexy et al. (2005), successivamente, somministrando un questionario a 756 studenti di due diverse università (una pubblica e l'altra statale), hanno rilevato un 3.7% di casi di cyberstalking, corrispondente al 31.5% delle vittime di stalking presenti nel campione, con una prevalenza di autori ex-partner o compagni di corso.

Più di recente, un rapporto edito da Purcell e colleghi (2009) ci offre nuove informazioni sulla prevalenza delle molestie elettroniche o telematiche, attraverso l'analisi di una serie di autori di reato (N=906) minori di 18 anni sottoposti ad Intervention Orders. Tra questi, un 15% aveva inviato sms indesiderati mentre l'11% era stato accusato di cyberstalking, comprendendo nella fattispecie le molestie effettuate attraverso e-mail ed istant-messaging e la pubblicazione di informazioni dannose per le vittime su siti internet.

Altri autori hanno invece ampliato il raggio d'azione, superando i confini degli ambienti universitari o studenteschi, a fronte dell'inarrestabile espansione delle nuove tecnologie e delle innumerevoli ed innovative modalità di azione offerte agli autori di atti persecutori.

Bocij (2003), al fine di fornire dati precisi e attendibili sulla frequenza e la prevalenza del cyberstalking, attraverso il meccanismo del c.d. "snowballing"[4], ossia delle e-mail a catena, ha reclutato un campione di 169 soggetti utenti di Internet, principalmente residenti nel Regno Unito e negli Stati Uniti, cui è stato somministrato un questionario online. Ai partecipanti veniva quindi chiesto di indicare se fossero mai stati oggetto di una o più delle 11 condotte online elencate nel questionario, ottenendo una risposta affermativa da oltre un terzo del campione (34%), con livelli anche elevati di ansia. Ricorrendo, invece, ad una definizione più rigida, i casi di vero e proprio cyberstalking risultavano ridursi ad un 21.9%, dato questo sicuramente non trascurabile e superiore alle stime provenienti dai precedenti studi condotti.

Uno studio di Sheridan e Grant (2007), condotto mediante un questionario completato da 1051 vittime di molestie assillanti auto-definitesi tali, ha cercato di indagare aspetti inerenti la vittimizzazione da stalking non precedentemente affrontati. Nell'elenco delle condotte prevalenti erano stati ricompresi anche l'aver ricevuto e-mail indesiderate e l'aver subito molestie tramite Internet. Quasi la metà delle vittime (il 47.5%) era stata molestata via Internet, mentre il 40% aveva ricevuto e-mail indesiderate. Tuttavia, riconducendo al concetto di cyberstalking solo i casi in cui lo stalking era iniziato e proseguito solamente online per almeno quattro settimane, solo il 7% del campione era risultato essere effettivamente vittima di molestie telematiche.

Nel 2007, ancora, Rosay et al. hanno coordinato un progetto di ricerca diretto ad esaminare per la prima volta le caratteristiche del fenomeno dello stalking in Alaska, sopperendo così ad un vuoto di conoscenza lamentato da più parti. Il campione (N=215) analizzato era costituito dagli episodi di molestie assillanti denunciati alle Forze di Polizia (Alaska State Troopers) dal 1994 al 2005, includendo le informazioni provenienti dai rapporti e dalle denunce, tenendo conto anche dei dati forniti dalle vittime e dai testimoni. Nell'indagare le condotte prevalenti, gli autori hanno distinto tra i diversi contesti di espressione delle molestie, attribuendo al cyberspace un ruolo non trascurabile nell'azione dello stalker, con un 27% di denunce per casi avvenuti prevalentemente online.

Spitzberg e Cupach (2007), infine, attraverso una meta analisi hanno rilevato e comparato i dati relativi alla presenza di molestie elettroniche all'interno di studi sullo stalking e sull'ORI (obsessive relational intrusion), giungendo ad individuare la presenza di comportamenti cyber abusivi mediamente nel 14% dei casi. Tuttavia, gli autori stessi ritenevano vi fossero serie e fondate ragioni di ritenere che questa percentuale sarebbe via via aumentata con l'incremento inarrestabile dell'utilizzo dei nuovi media a livello globale.

Pur in presenza di una letteratura in espansione, è quindi evidente come i dati esistenti risultino sicuramente sottostimati essendo ancora pochi i casi individuati e denunciati (Pittaro, 2007). Le differenze esistenti tra i vari studi epidemiologici, dovute sia alla metodologia e ai campioni indagati che alla definizione di cyberstalking utilizzata, rendono inoltre i risultati a disposizione contrastanti e pertanto non comparabili o generalizzabili (Spitzberg & Phillips, 2010).

I dati esistenti sull'estensione, la natura e gli effetti del fenomeno, in conclusione, non possono essere considerati comprensivi, il che rende particolarmente difficoltoso intervenire efficacemente predisponendo misure preventive e di tutela delle vittime. Auspicabile è quindi un incremento delle analisi sia quantitative che qualitative così da incrementare la comprensione del fenomeno e l'adeguata gestione dello stesso (Southworth, Finn, Dawson, Fraser & Tucker, 2008).

4. Condotte prevalenti: caratteristiche e classificazioni

Internet e le nuove tecnologie in generale forniscono agli stalker un numero esponenziale di nuove modalità d'azione per molestare le proprie vittime (Glancy, Newman, Potash & Tennison, 2007; Spitzberg & cupach, 2007; Basu & Jones, 2007; Fraser, Olsen, Lee, Southworth & Tucker, 2010; Clough, 2010).

Da un punto di vista descrittivo, in tale concetto rientrano uno spettro molto ampio e indefinibile di condotte, individuabili solo in maniera esemplificativa e non esaustiva (Reno, 1999; MacKenzie, Mullen, Pathé & Purcell, 2003; Sheridan & Grant, 2007; Pittaro, 2007), unite tra loro dall'elemento soggettivo, ossia dalla coscienza e volontà di disturbare o spaventare la vittima.

In maniera sintetica, lo stalking elettronico include tutte le forme di molestia effettuate attraverso: e-mail, mms, sms, instant messaging (es. spamming, mail bombing, invio di messaggi eccessivamente affettuosi, pornografici/osceni, sessualmente molesti o minacciosi ecc.); chat room, siti web o social network (es. Facebook, twitter, myspace, netlog, ecc.); pubblicazione online di immagini, video o informazioni negative/false su altre persone; furto dell'identità online (es. cybersmearing, flaming, ecc.); raccolta di informazioni private senza autorizzazione; ordine di merci e servizi in nome di altre persone; utilizzo di GPS ed altri strumenti elettronici per sorvegliare la vittima; invio di virus o trojan horses; utilizzo di spyware e così via tutte le opportunità che la nuova tecnologia può offrire (Finn & Banach, 2000; Ogilvie, 2000; McFarlane & Bocij, 2003; Bocij, 2004; Glancy, Newman, Potash & Tennison, 2007; Sheridan & Grant, 2007; Bergonzi Perrone, 2010). Internet è anche una fonte importante per la ricerca di informazioni sulle vittime per facilitare lo stalking offline: indirizzo, numero di telefono e altri dati personali possono aiutare a trasferire le molestie dal virtuale alla realtà fisica, poiché, di solito, questo comportamento non si verifica isolato, ma insieme ad altre forme tradizionali di molestie (Finn & Banach, 2000; Spitzberg & Hoobler, 2002; Sheridan & Grant, 2007).

Osservando i dati statistici a nostra disposizione, all'interno di questa molteplicità di espressioni cibernetiche delle forme persecutorie, è possibile individuare alcune condotte prevalenti rispetto alle altre (Phillips & Spitzberg, 2010). Sicuramente nella maggior parte dei casi lo strumento più utilizzato e attraverso cui più frequentemente ha inizio il

4 Il meccanismo in questione consiste nel contattare un gruppo di utenti e chiedere loro di prendere parte all'attività di ricerca completando un questionario. Ad ogni individuo viene, quindi, chiesto di contattare altre persone e di chiedere loro di partecipare alla ricerca. Il ciclo si ripete fino a quando non viene raggiunto un termine, in questo caso un termine temporale, fissato in una data.

cyberstalking è l'email con percentuali che vanno dall'11% (Morrison, 2008) al 40% (Bocij, 2003; Sheridan & Grant, 2007), fino addirittura ad un 82.6% rilevato dallo studio epidemiologico del BJS (Baum, Catalano & Rand, 2009). A seguire troviamo altre modalità di contatto e comunicazione, dirette ad inviare messaggi molesti o minacciosi, come le chat room e l'instant messaging, rispettivamente presenti nel 48 e 39% (Bocij, 2003), o azioni dirette a distruggere la reputazione della vittima (12%) (Spitzberg & Hoobler, 2002), come la pubblicazione di false informazioni su message board e newsgroup (24%) (Bocij, 2003), la diffusione di informazioni personali (17%) (Spitzberg & Hoobler, 2002) spesso rubate dagli stessi computer delle vittime (17%) (Bocij, 2003), o la creazione di siti web diffamatori (8.8%) (Baum, Catalano & Rand, 2009). Nel 24% dei casi analizzati da Bocij (2003), inoltre, il cyberstalker avrebbe incoraggiato terzi a molestare, minacciare o insultare la vittima, definendo questa ipotesi third party cyberstalking.

Con percentuali comprese tra il 18 e il 31% Spitzberg & Hoobler (2002) riportano invece l'invio di messaggi pornografici o osceni (18%) o sessualmente molesti (19%), oppure messaggi imploranti (25%) o eccessivamente affettuosi (31%) (Spitzberg & Cupach, 2007). Gli stessi autori riferiscono un 20% di autori di molestie cyber che assumono una falsa identità o fingono di essere qualcun altro (Spitzberg & Hoobler, 2002).

Riferendosi ancora alle modalità più diffuse, non trascurabili sembrano anche i numeri relativi alle azioni dirette a monitorare o danneggiare il sistema informatico della vittima (Bocij, 2003), attraverso l'invio di virus o l'utilizzo di software dannosi (41%) o inserendo Trojan Horse nel computer della stessa (27%), o rivolte a sorvegliare e spiare l'oggetto della persecuzione mediante strumentazioni elettroniche (Baum, Catalano & Rand, 2009), come accade nel caso di utilizzo di video camere (40.3%), dispositivi di ascolto (35.8%) e Gps (9.7%).

Come per lo stalking offline, anche rispetto alle espressioni di abuso online, diversi sono stati i tentativi di classificazione delle molteplici condotte che integrano questo fenomeno assai complesso.

Meloy (1998), studiando le forme di molestie poste in essere attraverso Internet, individua due principali obiettivi di tali azioni: ottenere informazioni private sulla vittima al fine di favorire il successivo stalking offline e comunicare, in tempo reale o meno, con la vittima per minacciarla, implicitamente o esplicitamente, o spaventarla. Diversi autori (Adam, 2002; McFarlane & Bocij, 2003; Bocij, 2004), tuttavia, criticano questa posizione, ritenendola non in grado di comprendere le reali potenzialità di Internet e quindi di ricomprendere il c.d. third party stalking così come altre attività associate al cyberstalking, quali ad esempio il furto di dati personali o il monitoraggio della vittima.

Ogilvie (2000) definisce tre principali categorie di condotte espressione del cyberstalking: e-mail stalking, inteso quale comunicazione diretta per il tramite della posta elettronica; Internet stalking, quale forma di comunicazione globale per mezzo di Internet; computer stalking, ossia controllo non autorizzato del computer di un'altra persona. Sinteticamente, l'e-mail stalking comprende innanzitutto l'invio ripetuto e teso a contattare o intimorire la vittima di e-mail oscene o minacciose, ma anche contenenti virus o, ancora, l'invio di un elevata quantità di junk mail (spamming). La seconda categoria coinvolge una dimensione pubblica piuttosto che privata delle molestie online, facilmente estensibili al mondo fisico e per questo più pericolose, conseguenza di un utilizzo maggiormente comprensivo di Internet da parte degli stalker, al fine di calunniare o mettere in pericolo le proprie vittime. Infine, nel caso del computer stalking sarebbe esclusa qualsiasi azione nel mondo reale, in quanto lo stalker utilizzerebbe unicamente Internet e i sistemi operativi (es. Windows) per introdursi nel sistema informatico della vittima, connettendosi al suo computer, al fine di controllarla, sorvegliarla e comunicare con lei.

Ellison (2001) distingue tra molestie online dirette ed indirette. Le prime consisterebbero nell'invio di e-mail sgradite, abusive, minacciose, intimidatorie o oscene, ma potrebbero anche configurarsi come hacking o come un sabotaggio elettronico, ossia come spamming o invio di virus informatici. Tra le forme indirette rientrerebbero, invece, l' assunzione da parte dello stalker dell'identità della vittima al fine di inviare e-mail abusive o spam fraudolenti in nome della stessa, la diffusione di maldicenze o informazioni private sulla vittima su vari forum o newsgroup o, ancora, l'iscrizione delle vittime, senza il loro permesso, ad una serie consistente di mailing list o di servizi online indesiderati. Di Luciano (2007), analogamente, segue la stessa classificazione, mentre Finn (2004) definisce le due sopracitate categorie rispettivamente e-mail stalking e Internet stalking.

Bocij (2003, 2004), a sua volta, ci offre un'altra classificazione degli atti persecutori telematici, sviluppata sulla base di quattro macro categorie, successivamente ampliata fino a dieci. Nel 2003 l'autore concentra la sua attenzione su quattro principali gruppi di attività: produzione di minacce, danneggiamento della reputazione della vittima, danneggiamento di dati o attrezzature, accesso ad informazioni riservate e monitoraggio del computer. Tali categorie nel 2004 sono diventate dieci, a seguito di una maggiore specificazione dei comportamenti associati o costitutivi del cyberstalking, aggiungendo alle precedenti: l'invio di e-mail o messaggi abusivi o offensivi, spacciarsi per la vittima, incoraggiare terze persone a molestare la vittima, ordinare merci o servizi per conto della vittima, tentativi di incontrare personalmente la vittima ed aggressioni fisiche.

Più di recente, la letteratura (Clough, 2010) ha ritenuto il cyberstalking riconducibile alle seguenti categorie, sovrapponibili e combinabili ai tradizionali comportamenti di stalking in real space: comunicare, pubblicare informazioni, colpire e danneggiare il computer e sorvegliare. Rispetto all'ultima categoria possono poi individuarsi due diverse modalità attraverso cui spiare e monitorare il destinatario delle molestie, a seconda che vengano raccolte informazioni personali sulla vittima o persone ad essa legate oppure vengano osservati e controllati direttamente le attività e i movimenti della vittima. La maggior parte delle condotte qui individuate sono ordinarie forme di molestie, che però in un contesto cyber vengono poste in essere grazie all'aiuto e alla maggior efficienza dei media elettronici.

Analogamente, Fraser (2010) riconduce a tre gruppi le tattiche e gli strumenti informatici che lo stalker utilizza impropriamente per monitorare e molestare le proprie vittime: i contatti ripetuti attraverso mezzi tecnologici (es. email, sms, IM), la sorveglianza e il monitoraggio (es. Gps, video camere) e lo stalking mediante Internet. In quest'ul-

tima categoria, l'autore comprende il furto e la pubblicazione di informazioni personali e l'adozione da parte del molestatore della personalità della vittima, principalmente al fine di compromettere la reputazione della stessa.

A prescindere dai diversi tentativi di tipizzazione descritti, ciò che va sottolineato è la totale impossibilità di individuare ed elencare in maniera definitiva e completa gli infiniti comportamenti in senso lato riconducibili al complesso concetto di cyberstalking. A fianco di condotte innovative, non configurabili al di fuori di contesti online, esistono anche forme di molestie offline che subiscono trasformazioni in forza delle nuove possibilità a disposizione dello stalker per agire facilmente ed efficacemente in un contesto apparentemente privo di confini e di limiti.

5. Chi è il cyberstalker?

Le persone hanno gli stessi desideri, le stesse emozioni e la stessa capacità di esprimere un comportamento deviante nel mondo reale come in quello virtuale, ma la miscela di realtà e fantasia che viene immessa nella rete può alimentare le ossessioni e le motivazioni dello stalker creando nuove situazioni di rischio di stalking (Lloyd-Goldstein, 1998).

Secondo la definizione contenuta nel Report firmato da Janet Reno (1999), il cyberstalker è un molestatore informatico, che usa la posta elettronica o qualsiasi altro mezzo digitale per molestare ripetutamente e perseguitare un'altra persona. Non dissimile è la posizione di Pittaro (2007) che parla di un "criminale che utilizza Internet quale strumento o arma per molestare, minacciare e generare immensa paura e trepidazione nelle sue vittime attraverso sofisticate tattiche di molestia".

Sebbene in genere si tratti di persone intelligenti e con sofisticate abilità informatiche, nella maggior parte dei casi ci si trova di fronte a soggetti socialmente isolati ed emotivamente immaturi, in cerca nel cyberspazio di attenzioni ed intimità che normalmente non sono in grado di ottenere nella vita reale (Adam, 2002; Spitzberg & Hoobler, 2002). La scelta di agire in questi contesti è infatti giustificata proprio dall'assenza di una reale interazione sociale, dall'anonimato e dalla possibilità di fingere di essere qualcun altro o di assumere più identità, sviluppando così la propria intenzione di controllare e fantasticare su se stessi e sul proprio oggetto del desiderio (Mullen, Pathé & Purcell, 2000). Questi autori di reato non rispecchiano pertanto lo stereotipo del criminale, trattandosi in genere di individui che in un contesto reale, faccia a faccia con la vittima, probabilmente non sarebbero in grado di agire illecitamente o violentemente, agevolati nel loro comportamento dannoso e molesto proprio dall'ambiente virtuale e quindi dall'interporsi del computer tra loro e il destinatario delle loro attenzioni indesiderate (Di Luciano, 2007).

Frequentemente il molestatore "incontra" la vittima online, in una chat o all'interno di community e social network, finendo poi per esserne ossessionato, reagendo, se respinto o rifiutato, attraverso una serie di molestie di tipo telematico, che possono anche estendersi offline nel caso in cui siano stati scoperti o divulgati dettagli per contattare la vittima (Pittaro, 2007; Sgarbi & MGS, 2007). Non di rado l'autore di queste condotte conosce personalmente la vittima, potendo quindi trattarsi di un conoscente, un ex/attuale partner, familiare o amico, così come invece potrebbe essere un perfetto sconosciuto, essere nella stessa stanza della vittima, oppure trovarsi dall'altro capo del mondo.

In generale, il cyberstalker esprime la necessità di controllare la vittima e di esercitare su di essa il suo potere, laddove l'utilizzo del mezzo elettronico è inteso come espressione di forza, modalità di persecuzione diretta a generare paura e timore e quindi ad incrementare anche le motivazioni e i sentimenti sottostanti l'agire del soggetto (McGrath & Casey, 2002).

Nonostante il crescente interesse per le tematiche inerenti gli effetti negativi dell'evoluzione tecnologica, gli studi sugli autori di molestie online sono ancora numericamente ridotti, per cui appare impossibile al momento individuare un profilo tipico, anche psicologico, del cyberstalker, spesso anche difficile da scoprire ed individuare (Phillips & Spitzberg, 2010).

Considerando le caratteristiche demografiche, da un punto di vista statistico, soprattutto sulla base delle analisi condotte in generale sugli atti persecutori, si rilevano dati parzialmente sovrapponibili a quelli riguardanti lo stalker offline. Per quanto riguarda il genere, i molestatori telematici sono prevalentemente uomini (Adam, 2002; McFarlane & Bocij, 2003; WHOA, 2003; Lucks, 2004), con percentuali fin oltre l'80%, di razza bianca con un'età media intorno ai 30 anni (Burgess & Baker, 2002; D'Ovidio & Doyle, 2003; McFarlane & Bocij, 2003). I casi di cyberstalking posto in essere da soggetti di sesso femminile nei confronti di soggetti di sesso maschile sono, quindi, piuttosto rari, anche se appaiono tuttavia in aumento, in relazione anche al progressivo incremento delle competenze tecnologiche delle donne e alla sempre maggiore facilità di accesso delle stesse, contrariamente a quanto avveniva in passato laddove queste conoscenze risultavano quasi ad esclusivo appannaggio degli uomini.

Sul piano dello status socio-economico, i cyberstalker dell'indagine di McFarlane e Bocij (2003) erano prevalentemente single (52.3%), dotati di conoscenze informatiche medio-alte (60%), con una occupazione lavorativa stabile (50%) e in possesso di un diploma o di una laurea universitaria (50%). Per quanto attiene, invece ai precedenti penali o alla presenza di disturbi di personalità, pur esistendo esempi in tal senso, la letteratura sottolinea come sia da escludere una necessaria corrispondenza tra il verificarsi delle molestie online e la sussistenza di queste condizioni negli autori (Pittaro, 2007).

Anche rispetto a questi autori, come nel caso di quelli offline, esistono alcuni tentativi di classificazione e tipizzazione.

McFarlane e Bocij (2003), pur lavorando su di un campione limitato, hanno delineato una prima ipotesi di classificazione dei molestatori online. Attraverso un questionario somministrato negli Stati Uniti a 24 vittime di cyberstalking, sono state individuate quattro tipologie di cyberstalker: vendicativo (vindictive), composto (composed), intimo (intimate) e collettivo (collective). Gli autori appartenenti al primo gruppo, dotati di un livello medio-alto di conoscenze informatiche, tenderebbero ad essere molto violenti e minacciosi, agendo in maniera continuativa con modalità di comunicazione e contatto sia virtuali che reali. Con maggior frequenza rispetto alle altre categorie, tra questi emer-

gerebbero precedenti penali e disturbi psichici. Il cyberstalker composto, invece, agirebbe in maniera pacata e contenuta, prevalentemente in contesti online, al fine di minacciare e molestare, sfruttando le proprie medio-alte competenze in materia di nuove tecnologie. La terza categoria di autori, maggiormente diversificata al suo interno rispetto alle altre e suddivisibile in due sottocategorie, gli ex-intimi e gli infatuati, comprenderebbe gli autori spinti ad agire dal desiderio di creare o ricostituire una situazione di intimità o una relazione con la vittima. Tra questi le competenze informatiche sembrerebbero estremamente differenziate e variabili da individuo a individuo. Infine, i cyberstalker collettivi agirebbero associati, molestando o preseguitando in maniera organizzata una stessa vittima, spesso un'organizzazione, al fine sia di screditarla (corporate cyberstalking) che in cerca di vendetta per un torto percepito (group cyberstalking). Le capacità tecnologiche di quest'ultima tipologia di autori sarebbero estremamente elevate e specializzate rispetto alle altre tre.

Altre posizioni in letteratura (Jaishankar & Sankary, 2006; Glancy, Newman, Potash & Tennison, 2007), hanno ritenuto applicabile anche alle condotte persecutorie online la classificazione multi-assiale introdotta da Mullen et al. (1999) per gli stalker offline, individuando attraverso l'analisi di campioni di molestatori analogie tra i contesti di azione e le motivazioni sottostanti i comportamenti di stalking, reale o virtuale che sia.

Sheridan e Grant (2007), a loro volta, sulla base dello studio condotto nel 2007 su 1051 vittime di stalking autodefinitesi tali, e precedentemente descritto, hanno introdotto una diversa categorizzazione degli stalker che agiscono nel c.d. cyberspace. Al termine della loro ricerca, i due autori hanno così identificato tre principali tipologie di cyberstalker (Phillips & Spitzberg, 2010): i molestatori esclusivamente online (pure cyberstalkers), le cui attività rimanevano confinate al contesto virtuale; i molestatori che dall'online erano passati all'offline stalking (cross-over cyberstalkers), iniziando quindi le molestie nel cyberspazio per poi estenderle al mondo reale; e gli stalker principalmente offline che utilizzavano anche Internet e la tecnologia per molestare le proprie vittime (proximal with online). Una quarta categoria, rappresentante la maggioranza degli autori del campione, comprendeva gli stalker esclusivamente offline, pertanto non riconducibili al contesto informatico e al concetto di cyberstalker.

Per concludere, sulla base delle indagini condotte e dei diversi tentativi di classificazione degli autori di questi reati, è possibile quindi delineare le principali motivazioni sottostanti queste tipologie di azioni persecutorie, parzialmente assimilabili a quelle delle molestie nel mondo reale: un interesse sessuale per la vittima, che viene virtualmente molestata; un'ossessione o infatuazione sentimentale, al fine di costituire una nuova relazione o di ricostruirne una precedentemente interrotta; vendetta e odio, per cui l'autore rivolge sulla vittima la propria rabbia, quale reazione ad un fatto concretamente accaduto o semplicemente per sfogare le proprie frustrazioni; egocentrismo e desiderio di potere, laddove il soggetto agisce per esprimere il proprio ego e soddisfare il proprio desiderio di potere e controllo, talvolta anche solamente per pura vanità o per gioco (Jaishankar & Sankary, 2006; Pittaro, 2007; Haron & Yusof, 2010).

6. Chi sono le vittime di cyberstalking?

Anche per quanto concerne le vittime delle molestie elettroniche, gli studi risultano ancora molto limitati. Prendendo spunto da quanto a nostra disposizione in materia di stalking offline, possiamo affermare che sebbene chiunque possa divenirne vittima, esistono comunque una serie di fattori e caratteristiche che rendono determinati soggetti vulnerabili e potenzialmente più a rischio di altri rispetto a queste tipologie di esperienze (Pittaro, 2007).

Un elemento comune alle vittime di tali condotte è la condizione di debolezza ed inesperienza, a causa oltre che della scarsa conoscenza di Internet e dei nuovi media informatici anche talvolta della immaturità emotiva e/o fisiologica (Bocij, 2003, 2004). L'utilizzo della Rete e delle ICT senza l'adeguata prudenza e consapevolezza, insieme alla mancata adozione di precauzioni e misure di sicurezza online, esponendo in maniera ingenua ed eccessiva se stessi e la propria identità richiama l'attenzione del cyberstalker, alla ricerca di qualcuno da molestare e controllare facilmente.

Le vittime potrebbero, quindi, suddividersi in tre categorie (Bocij, 2003) in relazione al loro livello di alfabetizzazione informatica, ossia principiante, intermedia o esperta, suggerendo una corrispondenza tra le conoscenze a disposizione della vittima e le tipologie di cyber molestie subite, con attacchi più sofisticati rivolti ai soggetti più esperti e una prevalenza di minacce tra i principianti. Così come viene, inoltre, sottolineata la maggior capacità degli utenti più avvezzi alla tecnologia di tutelarsi e proteggersi, in quanto in grado di rintracciare, identificare e localizzare il cyberstalker e di affrontare adeguatamente i suoi comportamenti.

Non di rado la vittima conosce il cyberstalker, legato ad essa da una semplice conoscenza o da qualcosa di più profondo come una relazione amicale o sentimentale, ipotesi in cui le molestie hanno inizio proprio quando questo pseudo-rapporto si interrompe in forza di una scelta esplicita della stessa vittima (Alexy, Burgess, Baker & Smoyak, 2005; Pittaro, 2007). In questi contesti virtuali, tuttavia, come ci si potrebbe aspettare, non mancano i casi di autori sconosciuti, questo soprattutto grazie alla facilità con cui si possono reperire informazioni e dati personali sulle vittime attraverso Internet, rendendo così molto semplice l'agire persecutorio (Mcgrath & Casey, 2002; Bocij, 2003, 2004; Wykes, 2007; Drahokoupilovà, 2007).

Ad essere molestati online sono quindi principalmente i soggetti di sesso femminile (Finn & Banach, 2000), in precedenza legati da qualche rapporto, reale o immaginario, al proprio cyberstalker, di razza caucasica, tra i 18 e i 32 anni di età, talvolta con limitate competenze elettroniche o appartenenti ad alcune minoranze e gruppi (es. bambini e adolescenti, minoranze etniche e religiose, gay e lesbiche, soggetti membri di associazioni a tutela delle vittime di determinati reati ecc.) (Jaishankar & Sankary, 2006).

Da un punto di vista statistico, le indagini epidemiologiche a nostra disposizione confermano l'ipotetico profilo vittimologico appena descritto.

I dati, pur non rappresentativi della popolazione generale[5],

5 Trattandosi di una organizzazione internazionale per la sicurezza di Internet, i campioni analizzati sono costituiti da vittime autodefinitesi tali che hanno contattato direttamente il portale, in cerca di aiuto e tutela.

del WHOA (Haltabuse.org, 2011) riferiscono il 74% di vittime donne, caucasiche (82%), intorno ai 30 anni (35%), single (53%), legate nel 59% dei casi da un qualche attuale o precedente rapporto con il molestatore (56% ex-partner), elemento quest'ultimo spesso catalizzatore dell'agire molesto e persecutorio, sia che il rapporto preesistente fosse reale o immaginario (Reno, 1999). Nella maggior parte dei casi (77.5%) le vittime non avevano denunciato quanto accaduto alle autorità preposte.

Diversi studi scientifici (Burgess & Baker, 2002; Bocij, 2003; D'Ovidio & Doyle, 2003; McFarlane & Bocij, 2003; Aftab, 2004; Sheridan & Grant, 2007) hanno rivelato risultati simili, con percentuali tra il 52% (D'Ovidio & Doyle, 2003) e il 91% (McFarlane & Bocij, 2003) di donne molestate, quasi esclusivamente di razza bianca (McFarlane & Bocij, 2003; Sheridan & Grant, 2007), di età compresa tra i 18 e i 30 anni (45.8%) (McFarlane & Bocij, 2003). Nello studio di Bocij (2003), tuttavia, la maggior parte delle vittime (42%) non conosceva l'identità del proprio cyberstalker, mentre una minoranza veniva molestata da un amico (15.8%), da un ex partner (8.7%) o infine da un collega (1.7%).

Tra le caratteristiche estrinseche delle vittime, il campione di McFarlane & Bocij (2003) era costituito soprattutto da persone single (58.3%), professionalmente occupate (37.5%), con un livello di istruzione piuttosto elevato (50% undergraduate degree) e conoscenze e capacità informatiche di medio livello. Parzialmente in contrasto con quanto appena affermato sono invece gli aspetti qualificanti le vittime dello studio di Bocij (2003), sposate o conviventi (76.5%), prevalentemente studentesse (21%) con una laurea universitaria di primo livello (50%) e medie conoscenze informatiche (categoria "intermediate"). Tali discrepanze nei dati raccolti attraverso le due indagini appena citate, sembrerebbero riconducibili alle differenze esistenti tra i due campioni, uno costituito da vittime e l'altro da utenti di Internet reclutati attraverso il sistema delle e-mail a catena.

Le ricerche appena illustrate ci dimostrano, quindi, sì la prevalenza di alcune caratteristiche ma anche l'impossibilità di definire un unico profilo di vittima, risultando i dati epidemiologici estremamente influenzati dai campioni selezionati ed indagati.

Ciò nonostante, è evidente che diversi fattori pongono determinate categorie di soggetti maggiormente a rischio di subire condotte cyber moleste, quali il sesso femminile, l'età e la scarsa conoscenza delle tecnologie elettroniche in genere.

7. Effetti e conseguenze del fenomeno

Le molestie poste in essere nel c.d. cyberspazio sono in grado di produrre conseguenze ed effetti concreti e gravi, reali e assolutamente non virtuali, talvolta addirittura più pericolosi e lesivi di quelli prodotti dagli atti persecutori offline.

Internet e i contesti di azione e comunicazione elettronica rappresentano, infatti, un mondo parallelo, in cui molestare e violare la privacy altrui è molto più facile e immediato, laddove l'assenza di prudenza e la mancanza di esperienza possono condurre la vittima stessa ad indicare al molestatore gli strumenti e i percorsi d'azione.

Tuttavia, in un primo momento, a fronte del diffondersi di questi comportamenti, la letteratura prevalente ha sottostimato e trascurato gli effetti del cyberstalking (Bocij, 2003, 2004), ritenendoli estremamente diversi da quelli dello stalking offline o addirittura meno importanti e dannosi (Petherick, 1999; Jaishankar & Sankary, 2006; Basu & Jones, 2008).

L'atteggiamento precedente potrebbe trovare una spiegazione nella falsa illusione che la distanza fisica esistente fra vittima e autore, caratteristica delle persecuzioni via mezzi elettronici, renderebbe le stesse meno gravi (McFarlane & Bocij, 2003; Phillips & Morrisey, 2004; Glancy, Newman, Potash & Tennison, 2007), percezione questa in realtà errata, a fronte di diversi casi di cyberstalking terminati in episodi estremamente gravi, anche fisicamente, incluso l'omicidio della vittima (Bocij, Griffiths & McFarlane, 2002; Bocij, 2003; Sgarbi & De Fazio, 2012). Questo tipo di molestie, proprio perché perpetrate in uno spazio privo di limiti, potrebbero addirittura essere più subdole e pericolose di quelle reali, in quanto l'autore sarebbe in grado potenzialmente di osservare, sorvegliare e contattare la vittima in qualsiasi momento, in qualunque luogo, violando profondamente la sua intimità e privacy (Reno, 1999).

Oggi, quindi, appare evidente e certo che il cyberstalking può essere un'esperienza spaventosa, in grado di produrre conseguenze fisiche, psicologiche e socio-comportamentali (Mccall, 2004; Jaishankar & Sankary, 2006), analoghe a quelle subite in forza di una campagna di stalking offline (Glancy, Newman, Potash & Tennison, 2007).

Queste condotte così pervasive producono nella vittima una paura dell'altro e dell'ignoto del tutto incontrollabile, un senso intenso di intrusione e violazione della sfera privata senza avere via di scampo, determinando importanti effetti quali depressione, ansia, senso di impotenza e abbandono, ipervigilanza, disturbo post-traumatico da stress, idee suicide, associati a conseguenze anche a livello fisio-psichico come attacchi di panico, incubi e disturbi del sonno, emicrania, nausea, disturbi dell'alimentazione, atti di autolesionismo, aumento del consumo di alcool e sostanze stupefacenti (Pittaro, 2007; Sheridan & Grant, 2007).

Secondo Bocij (2004) il livello di angoscia subito dalle vittime di cyberstalking risulterebbe strettamente legato al livello di competenze informatico-elettroniche possedute, per cui in generale: maggiore è la conoscenza e l'esperienza in materia di Internet e nuove tecnologie e minore è l'angoscia patita a seguito delle molestie subite. Richiesto alle vittime dello studio condotto nel 2003 di auto valutare il livello di stress subito su una scala da 1 a 10, un quarto del campione aveva riferito il valore massimo (22.8%), con una media del 7. Per i cosiddetti principianti invece il livello medio era pari all'8.6, laddove nessuno aveva riportato valori inferiori al 5 e oltre il 50% riferiva livelli massimi di angoscia (10) (Bocij, 2003).

Non infrequente, come nel caso degli atti persecutori offline, è inoltre il sorgere di sentimenti di colpa, vergogna e imbarazzo nelle vittime, che tendono spesso a giustificare quanto patito sulla base della propria imprudenza e dell'incauto ed errato utilizzo dei media informatici (Phillips & Morrisey, 2004).

Un numero poi non trascurabile di conseguenze coinvolge la vita socio-relazionale del soggetto molestato, portandolo a stravolgere le proprie abitudini e i contesti sociali e lavorativi, in forza della percepita perdita di sicurezza personale e di un senso di incertezza e imprevedibilità.

È certo, infatti, che le invasioni nel mondo virtuale producono effetti diretti sulla qualità della vita reale (Bocij, 2004), incidendo sulla routine quotidiana della vittima costretta ad assumere importanti decisioni al fine di limitare gli effetti negativi del cyberstalking e di tutelare se stesse, come ridurre i rapporti interpersonali, non frequentare più chat room, social network ed altri contesti online a rischio, rimuovere i propri riferimenti da mailing list, modificare frequentemente le credenziali di accesso a computer, cellulari ed altri mezzi informatici, cambiare o rinunciare alla propria attività lavorativa ecc.

In generale, quindi, la scarsità di ricerche sulle conseguenze specifiche del cyberstalking risulta compensata da quanto noto circa gli atti persecutori offline, con una quasi totale sovrapposizione degli effetti negativi nei due diversi contesti, pur tenendo a mente le specificità delle molestie online e dei fattori di rischio prevalenti, in grado di incidere sulle situazioni concrete.

8. Prevenzione e interventi: strategie di difesa e tutela delle vittime

A fronte quindi della accertata pericolosità delle forme elettroniche di disturbo e molestia, importanti sono le strategie di coping dirette ad affrontare in maniera efficace questi fenomeni insieme agli interventi di tutela e protezione delle vittime.

La peculiarità del contesto di riferimento comporta l'adozione anche di soluzioni ed interventi ad hoc, strettamente delineati in accordo con le caratteristiche delle espressioni di abuso attuabili nel cyberspazio (De Fazio, Sgarbi, 2009[b]).

Difendersi dal cyberstalking presuppone necessariamente la conoscenza del fenomeno, così da acquisire la consapevolezza necessaria per muoversi in maniera sicura nel mondo del web ed eventualmente reagire a fronte di episodi di molestie. Il semplice abbandono del mondo online, seppur talvolta appaia l'unica seppur irrealistica scelta risolutiva, non rappresenta la strategia migliore da adottare, laddove il problema non è la tecnologia ma l'uso improprio che ne fa lo stalker (Sheridan & Grant, 2007; Fraser, Olsen, Lee, Southworth & Tucker, 2010).

In un'ottica preventiva, diverse sono le cautele da osservare al fine di limitare o escludere il rischio di subire comportamenti persecutori online (Bocij, 2004; Pittaro, 2007). Si suggerisce, infatti, agli utenti di Internet di essere il più possibile attenti e prudenti, seguendo una serie di regole minime per un utilizzo sicuro e protetto della rete. Tra le principali precauzioni da adottare a questo scopo: mantenere il più possibile riservato il proprio indirizzo email, che dovrebbe essere neutro dal punto di vista del genere; creare due diversi account di posta elettronica, uno lavorativo e l'altro personale; evitare di allegare intestazioni e firme che contengano informazioni personali e riservate alle email inviate; non utilizzare informazioni personali per creare profili online e creare password affidabili per l'accesso agli stessi; proteggere attraverso rigide impostazioni di privacy i profili nei social network; utilizzare nomi di fantasia nelle chat o nei forum; non concedere troppa "confidenza virtuale" a persone che non si conoscono; prestare attenzione a quello che si dice nei contesti online e al materiale (fotografie, video ecc.) pubblicato; utilizzare sistemi di sicurezza come firewall e antivirus, e così via (Petrocelli, 2005; Sgarbi & MGS, 2007; Glancy, Newman, Potash & Tennison, 2007).

In termini invece di coping e quindi di reazione all'esperienza di cyberstalking, le vittime in genere seguono tre diverse modalità di gestione di tali situazioni di crisi, affrontando l'autore, ignorando quanto sta accadendo oppure coinvolgendo altri soggetti e chiedendo il loro aiuto (Haron & Yusof, 2010).

Qualora un soggetto si renda conto di subire condotte riconducibili al concetto di cyberstalking, è fondamentale, alla prima occasione, informare il molestatore che il suo comportamento è inaccettabile, chiedendogli quindi di interrompere qualsiasi altro tentativo di comunicazione (Pittaro, 2007). Tuttavia, come si consiglia nelle ipotesi di stalking offline, bisognerebbe rivolgersi allo stesso con un tono deciso ma neutro, evitando espressioni di rabbia e insofferenza, talvolta controproducenti (Sgarbi & MGS, 2007; Glancy, Newman, Potash & Tennison, 2007). Successivamente, la vittima non dovrebbe più rispondere, né contrattaccare, abbandonando eventuali nuove situazioni spiacevoli, ad esempio uscendo immediatamente dalla chat, cambiando indirizzo email, eliminando il proprio profilo dai Social Network, non navigando su determinati siti, bloccando o ignorando le e-mail sconosciute o disconnettendosi.

Al fine di intercettare l'autore e quindi di intervenire concretamente, anche legalmente, nei suoi confronti, è indispensabile documentare e monitorare le sue attività, memorizzando ora, luogo e ogni forma di contatto o di messaggio inviato. Per raccogliere più prove possibili a carico del cyberstalker, la vittima dovrebbe: scaricare e conservare tutte le e-mail, i messaggi o le altre comunicazioni sia in forma elettronica (CD-ROM, Hard-Disk, ecc.) che cartacea; se possibile, salvare tutte le informazioni delle intestazioni di e-mail e newsgroup; conservare tutte le immagini o altri materiali multimediali ricevuti, ripuliti da eventuali virus allegati agli stessi; ove possibile, registrare eventuali post inviati ai newsgroup; se il programma lo consente, salvare le conversazioni via Istant messenger/chat room e memorizzarle sul disco rigido del computer, altrimenti utilizzare un programma di screen capture (es. Wingrab, Screen Grab Pro) per effettuare una copia dell'intero schermo della conversazione, per poi salvarla come immagine sul computer; registrare il materiale pubblicato dallo stalker su pagine web, guest book, blog o giornali online, salvando la relativa pagina su disco.

Un'ipotetica vittima dovrebbe poi contattare sia il proprio Internet Provider che quello della persona che la sta molestando (Bocij, 2004; Glancy, Newman, Potash & Tennison, 2007). Molti amministratori offrono oggi ai propri utenti strumenti per tutelarsi e proteggersi, prevedendo opzioni per filtrare o bloccare le mail provenienti da determinati indirizzi o soggetti, o escludere dalle chat le persone moleste. Allo stesso tempo esistono politiche contrattuali che vietano l'utilizzo abusivo dei servizi online forniti. Alcuni stanno creando anche comunità chiuse di utenti (gated communities), filtrando il contenuto dei messaggi attraverso un server o ponendo restrizioni sul tipo di informazioni che possono essere inviate agli altri (Reno, 1999). I provider dovrebbero infatti diventare sempre più consapevoli e responsabili dei fenomeni di cyberstalking ed incrementare

le misure di sicurezza a disposizione dei propri clienti (Pittaro, 2007). Possono, inoltre, essere direttamente contattati i moderatori di forum e chat room, i responsabili di newsgroup, o il proprietario o i gestori di un sito web, in caso di utilizzo abusivo e violazione delle regole degli stessi.

In queste situazioni, un altro aiuto efficace può provenire dai principali risorse elettroniche a difesa delle vittime di cyberstalking e a tutela della sicurezza di Internet, come i già citati "Working to Halt Online Abuse" o "CyberAngels", che forniscono supporto, assistenza e consigli in tema di stalking elettronico (Bocij, 2004; Petrocelli, 2005).

Qualora altre soluzioni non fossero efficaci, può essere necessario informare e coinvolgere le Forze dell'Ordine, oggi sempre più preparate ad affrontare queste tipologie di condotte anche attraverso apposite sezioni costituite da specialisti informatici, esperti nella gestione di condotte moleste o illecite online (es. Polizia Postale e delle Telecomunicazioni) (Glancy, Newman, Potash & Tennison, 2007). In queste particolari situazioni, l'intervento delle istituzioni può offrire un efficace supporto in termini di consigli pratici e strategie di difesa, talvolta favorendo l'interrompersi e il terminare delle molestie, dando poi successivamente avvio all'azione legale nei confronti dell'autore (De Fazio, Merzagora Betzos, Sheridan & Sgarbi, 2012).

Soltanto in alcuni paesi sono state emanate apposite normative sul cyberstalking o sulle comunicazioni elettroniche (es. Florida, Carolina del Nord, Regno Unito, Australia), mentre nella maggior parte dei casi le esistenti leggi antistalking o sulle molestie, qualora non sufficientemente flessibili per poter essere applicabili anche a queste particolari tipologie di condotte, sono state innovate e aggiornate (Di Luciano, 2007). In generale, tuttavia, la disciplina in materia appare ancora scarna e limitata, per cui sembra auspicabile una riforma diretta a tutelare maggiormente e in maniera più efficace le vittime, affiancando al legislatore anche magistrati e operatori di polizia adeguatamente formati.

Considerando il dato statistico proveniente dalle principali risorse online (WHOA) la maggior parte dei soggetti molestati reagiscono al cyberstalking contattando l'Internet Provider (52%), le Forze dell'ordine (41.5%) o un avvocato (6.5%), mentre nell'8% dei casi decidono semplicemente di non reagire e di ignorare quanto accaduto (WHOA, 2011). Secondo Bocji (2003), invece, il 33% delle vittime del suo studio si era rivolto al proprio Internet Provider o ad un'associazione a tutela delle vittime (es. CyberAngels). Solamente il 14% invece aveva contattato la polizia, probabilmente a causa del timore di non essere creduto e di non ricevere adeguato sostegno, o per aver sottovalutato quanto subito (Bocij, 2004).

Come per gli atti persecutori offline, possiamo quindi affermare nuovamente che non esiste una strategia o un intervento definitivo e specifico valido per tutte le vittime e per tutte le ipotesi di cyberstalking. Ogni situazione necessità di una valutazione e gestione ad hoc, definita precisamente sulle caratteristiche intrinseche del caso concreto, in un'ottica di continua evoluzione ed innovazione coerentemente con l'esponenziale ed inarrestabile avanzamento di Internet e dei media informatici.

Conclusioni

Il fenomeno del cyberstalking, oggetto di questa sintetica e sicuramente non esaustiva rassegna, risulta essere senza timore di smentita in costante crescita, parallelamente all'aumento dell'utilizzo da parte della popolazione generale di Internet e delle nuove tecnologie.

Nonostante i piuttosto recenti e ancora quantitativamente scarsi dati sulla prevalenza delle modalità persecutorie online, è evidente come la facilità di accesso ai media elettronici e la loro capacità di rendere più efficace e semplice la realizzazione degli obiettivi molesti dello stalker non possa che incrementare il ricorso ad essi. L'offensività di questi soggetti sarà, infatti, proporzionalmente legata al sempre più ampio e massiccio utilizzo che gli strumenti informatici avranno nella nostra quotidianità.

L'espansione del mondo del web e dei social network, unitamente agli altri mezzi di comunicazione elettronica, se da un lato ha portato con sé innumerevoli ed innegabili aspetti positivi, dall'altro ha presto mostrato anche i suoi aspetti più oscuri, incrementando il rischio di subire tentativi di comunicazione e contatto indesiderati.

L'emergere di sempre nuovi casi e nuovi studi sul fenomeno in oggetto, ha portato negli ultimi anni ad una positiva crescita del livello di interesse sia da parte del mondo accademico che da parte della popolazione generale, giungendo talvolta ad un auspicato intervento legislativo teso a disciplinare queste nuove tipologie di reato.

Tuttavia, a fronte delle importanti conseguenze fisiche, psicologiche e sociali, che questi comportamenti producono su chi li subisce, ai fini di un corretto intervento e di una efficace tutela delle vittime, appare indispensabile incrementare la formazione e la sensibilizzazione delle agenzie di aiuto chiamate a valutare e gestire concretamente le ipotesi persecutorie verificatesi nel cyberspace.

Viene salutata, infatti, con favore la nascita di associazioni e siti internet (es. CyberAngels), anche internazionali, contenenti informazioni per la sicurezza della rete o per la tutela degli utenti, e la nascita di apposite sezioni all'interno delle Forze di Polizia con specifiche competenze in materia di gestione della criminalità informatica (es. Polizia postale e delle Comunicazioni).

Gli stessi fruitori dei nuovi media e delle c.d. Internet Technology dovrebbero utilizzare in maniera sempre più consapevole e prudente tali strumenti, essere adeguatamente informati sugli inevitabili rischi e quindi adottare tutte le precauzioni necessarie per proteggersi da eventuali forme telematiche di persecuzione. È evidente infatti che l'innovazione tecnologica facilita le interrelazioni, diminuendo la percezione del contatto diretto, in assenza di una prossimità fisica, e incrementando il rischio di forme di contatto indesiderate.

La ricerca su queste ipotesi delittuose, oggi in costante crescita, deve quindi essere ulteriormente approfondita, al fine oltre che di valutare la prevalenza e i molteplici aspetti qualificanti gli stessi, anche di potenziare gli strumenti di coping e tutela delle vittime, in un'ottica di protezione personale e di controllo e gestione consapevole dei mezzi di comunicazione a disposizione.

Bibliografia

Adam, A. (2002). Cyberstalking and internet pornography: gender and the gaze. *Ethics and Information Technology*, 4, 133-142.

Aggarwal, S., Burmester, M., Henry, P., Kermes, L., & Mulholland, J. (2005). Anti-cyberstalking: the Predator and Prey Alert (PAPA) System. *Computer Society*, 195-205.

Alexy, E.M., Burgess, A.N., Baker, T., & Smoyak, S.A. (2005). Perceptions of cyberstalking among college students. *Brief Treatment and Crisis Intervention*, 5(3), 279-289.

Basu, S., & Jones, R.P. (2008). Regulating cyberstalking. In F. Schmalleger, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 141-165). Upper Saddle River, NJ: Prentice Hall.

Baum, K., Catalano, S., & Rand, M. (2009). *Stalking. victimization in the United States*. Washington DC: Bureau of Justice Statistics, U.S. Department of Justice.

Bergonzi Perrone, M. (2010). La "nuova" figura del cyberstalking. *Ciberspazio e diritto*, 11, 551-566.

Bocij, P. (2002). Corporate cyberstalking: an invitation to build theory. *First Monday,* 7. Retrieved April 2012, from http://-firstmonday.org/issues/issues7_11/bocij/.

Bocij, P. (2003). Victims of cyberstalking, an exploratory study of harassment perpetrated via the internet. *First Monday,* 8. Retrieved April 2012, from http://firstmonday.org/issues/issues8_10/bocij/.

Bocij, P. (2004). *Cyberstalking: harassment in the internet age and how to protect your family*. Westport, CT: Praeger.

Bocij, P., Griffiths, M., & McFarlane, L. (2002). Cyberstalking: a New Challenge for Criminal Law. *The Criminal LAWYER,* 3-5.

Bocij, P., & Mcfarlane, L. (2002). Online harassment: towards a definition of cyberstalking. *Prison Service Journal,* 139, 31-38.

Burgess, A.W., & Baker, T. (2002). Cyberstalking. In J. Boon, & L. Sheridan (Eds.), *Stalking and Psychosexual Obsession* (pp. 201-219). West Sussex: Wiley&Sons.

Carducci, M. (2011). La cooperazione giudiziaria e di polizia nelle indagini sul cybercrime: l'esperienza del pool reati informatici presso la Procura della Repubblica di Milano. In F. Cajani & G. Costabile (Eds.), *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea* (pp. 13-25). Forlì: Experta.

Chik, W. (2008). Harassment through the digital medium: a cross-jurisdictional comparative analysis on the law on cyberstalking. *Journal of international, commercial law and technology*, 3, 13-44.

Clough J. (2010). Cyberstalking. In J. Clough (Ed.), *Principles of Cybercrime* (pp. 365-387). Cambridge, UK: Cambridge University Press.

De Fazio, L., Merafina, R., & Sgarbi, C. (2009). Stalking e Mass Media. *Rassegna Italiana di Criminologia*, *3*, 56-72.

De Fazio, L., & Sgarbi, C. (2009a). Stalking: la diffusione del fenomeno, gli autori e le vittime. In Forum-Associazione Donne Giuriste (Ed.), *Stalking e Violenza alle donne. Le risposte dell'ordinamento, gli ordini di protezione* (pp. 36-45). Milano: Franco Angeli.

De Fazio, L., & Sgarbi, C. (2009b). La rilevanza sociale dello stalking: valutazione e gestione del rischio. In Forum-Associazione Donne Giuriste (Ed.), *Stalking e Violenza alle donne. Le risposte dell'ordinamento, gli ordini di protezione* (pp. 54-64). Milano: Franco Angeli.

De Fazio, L. (2009) The legal situation on stalking among the European Member States. *European Journal on Criminal Policy and Research*, 15, 229-242.

De Fazio, L. (2011), Criminalization of stalking in Italy: one of the last among the current European member states anti-stalking laws. *Behavioral Science and Law*, 29, 317-323

De Fazio, L., Merzagora Betsos, I., Sheridan. L., & Sgarbi, C. (2012). Stalking e violenza: presentazione di uno strumento di valutazione del rischio. In L. De Fazio & C. Sgarbi (Eds.). *Stalking e rischio di violenza. Uno strumento per la valutazione e la gestione del rischio* (pp. 41-60). Milano: Franco Angeli.

Deirmenjian, J.M. (1999). Stalking in cyberspace. *Journal of American Academy of Psychiatry*, 273, 407-413.

Di Luciano, F. (2007). Cyberstalking. Comparazione, situazione italiana e prospettive di riforma. *Diritto dell'Internet*, 5, 503-509.

D'Ovidio, R., & Doyle, J. (2003). A study on cyberstalking: understanding investigative hurdles. *FBI Law enforcement bulletin,* 72, 10-17.

Dowdell Burgess, E., & Bradley, P.K. (2010). Risky Internet Behaviors: A Case Study of Online and Offline Stalking. *Journal of School Nursing*, 26, 436-442.

Drahokoupilová, J. (2007). Cyberstalking. *Masaryk University Journal of Law and Technology*, 2, 145-155.

Ellison, L. (2001). Cyberstalking: tackling harassment on the internet. In D. Wall (Ed.), *Crime and the internet* (pp. 141-151). New York: Routledge.

Finkelhor, D., Mitchell, K., & Wolak, J. (2000). *Online Victimization: A Report on the Nation's Youth*. Alexandria, VA: National Center for Missing and Exploited Children.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence,* 19, 468-483.

Finn, J., & Banach, M. (2000). Victimization Online: The Down Side of Seeking Human Serices for Women on the Internet. *CyberPsychology & Behavior*, 3, 243-254.

Fisher, B.S., Cullen, F.T., & Turner, M.G. (2000). *The sexual victimization of college women*. Washington, DC: National Institute of Justice, Bureau of Justice Statistics.

Fraser, C., Olsen, E., Lee, K., Southworth, C., & Tucker S. (2010). The New Age of Stalking: Technological Implications for Stalking. *Juvenile and Family Court Journal*, 61, 39-55.

Glancy, G.D., Newman A.W., Potash M.N., & Tennison J. (2007). Cyberstalking. In D.A. Pinals (Ed.), *Stalking. Psychiatric Perspectives and Practical approaches* (pp. 212-226). Oxford, UK: Oxford University Press.

Grodzinsky, F.S., & Tavani, H.T (2002). Cyberstalking: moral responsibility and legal liability issues for internet services providers. *Technology and society,* 331-339.

Haron, H., & Mohd Yusof, F. (2010). Cyber Stalking: The Social Impact of Social Networking Technology. *International Conference on Education and Management Technology (ICEMT).*

Hitchcock, J.A. (2003). Cyberstalking and law enforcement. *Police Chief,* 12, 16-26.

Jaishankar, K., & Uma Sankary, V. (2006). Cyberstalking: a global menace in the information super highway. *ERCES Online Quarterly Review.* Retrieved April 2012, from http://erces.com/journal/articles/archives/volume2/v03/v02.htm.

Joseph, J. (2003). Cyberstalking: an international perspective. In Y. Jewkes (Ed.), *Dot. Cons: crime, deviance and identity on the internet* (pp. 105-125). Cullompton, England: Willan.

Kamphuis, J.H., & Emmelkamp, P.G. (2001). Traumatic distress among support-seeking female victims of stalking. *American Journal of Psychiatry*, 158, 795-798.

Lee, R. (1998). Romantic and Electronic Stalking in a College Context. *William and Mary Journal of Women and the Law*, 4, 373-466.

Lessig, L. (1999). The law of the horse: what cyberlaw might teach. *Harvard law Review,* 113, 501-546.

Lloyd-Goldstein, J.D. (1998). De Clèrambault On line: A survey of erotomania and stalking the old world to the world wide web. In J.R. Meloy (Ed.), *The psychology of stalking: clinical and forensic perspectives* (pp. 193-212). San Diego: Academic Press.

Lucks, B.D. (2004). Cyberstalking: Identifying and examining electronic crime in cyberspace. Dissertation Abstracts International: B. *The Sciences and Engineering*, 65, 1073.

MacKenzie, R., Mullen, E.P., Pathè, M., & Purcell, R. (2003). I comportamenti di molestie. In P. Curci, G.M. Galeazzi & C. Secchi (Eds.), *La sindrome delle molestie assillanti (stalking)* (pp. 38-57). Torino: Bollati Boringhieri.

Mccall, R. (2004). Online harassment and cyberstalking: victim access to crisis, referral and support services in Canada, concepts and recommendations. *Victim Assistance online resources (VAON).*

Mcfarlane, L., & Bocij, P. (2003). Cyberstalking: defining the invasion of cyberspace. *Forensic Update,* 72, 18-22.

Mcfarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: towards a typology of cyberstalkers. *First Monday,* 8. Retrieved April 2012, from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1076/996.

Mcgrath, M.G., & Casey, E. (2002). Forensic Psychiatry and the Internet: practical perspectives on sexual predators and obsessional harassers in cyberspace. *Journal of the American Academy of Psychiatry and Law*, 30, 81-94.

Meloy, J.R. (1998). The psychology of stalking. In J.R. Meloy (Ed.), *The psychology of stalking: clinical and forensic perspectives* (pp. 1-23). San Diego: Academic Press.

Merschman, J.C. (2001). The dark side of the web: cyberstalking and the need for contemporary legislation. *Harvard Women's Law Journal,* 24, 255-292.

Moore, R. (2011). Online harassment and cyberstalking. In R. Moore (Ed.), *Cybercrime, investigating high technology computer crime* (pp. 129-143). Elsiever Anderson Publishing.

Mullen, P.E., Pathé, M., Purcell, R., & Stuart G.W. (1999). Study of stalkers. *American Journal of Psychiatry,* 170, 12-17.

Morrison, K.A. (2008). Differentiating between Physically Violent and Nonviolent Stalkers: an Examination of Canadian Cases. *Journal of Forensic Science*, 53, 742-751.

Mullen, P.E., Pathé, M., & Purcell, R. (2000). *Stalkers and their victims*. Cambridge: Cambridge University Press.

Ogilvie, E. (2000). Cyberstalking: Trend Issue Crime. *Criminal Justice*, 166, 1-6.

Petherick, W. (1999). *Cyberstalking: obsessional pursuit and the digital criminal.* www.crimelibrary.com/criminology/cyberstalking/-index.html

Petrocelli, J. (2005). Cyber stalking. *Law & Order*, 53(12), 56-58.

Philips, F., & Morrissey, G. (2004). Cyberstalking and cyberpredators: a threat to safe sexuality on the internet, Convergence. *The International Journal of Research into New Media Technologies,* 10, 1, 66-79.

Phillips, M., & Spitzberg, B.H. (2010). Speculating about Spying on MySpace and Beyond: Social Network Surveillance and Obsessive Relational Intrusion. In K.B. Wright & L.M. Webb (Eds.), *Computer-Mediated Communication in Personal Relationships* (pp. 344-367). New York: Peter Lang.

Pittaro, M.L. (2007). Cyber stalking: an analysis of online harassment and intimidation. *International Journal of Cyber Criminology*, 1(2), 180-197.

Purcell, R., Flower, T., & Mullen, P.E. (2009). Adolescent stalking: Offense characteristics and effectiveness of intervention orders. *Trends and Issues in Crime and Criminal Justice,* 369, 1-6.

Rosay, A.B., Wood, D.S., Postle, G., & TePas, K. (2007*). Descriptive Analysis of Stalking Incidents Reported to Alaska State Troopers: 1994-2005*. Report awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Anchorage, AK: Justice Center, University of Alaska Anchorage. Retrieved May 2012 from http://justice.uaa.alaska.edu/research/2000/0601intimatepartnerviolence/0601.01.stalking.pdf

Reno, J. (1999). *Cyberstalking: a new challenge for law enforcement and industry. A report from the US Attorney General to the Vice president Al Gore.* Washington DC: U.S. Department of Justice, Retrieved April 2012 from http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

Sgarbi, C., & MGS (2007). Appendice. Manuale pratico per vittime di stalking. In Modena Group on Stalking (Ed.), *Percorsi di aiuto per vittime di stalking* (pp. 96-121). Milano: Franco Angeli.

Sgarbi, C. & De Fazio, L. (2012). Stalking e violenza: la ricerca e i fattori di rischio. In L. De Fazio & C. Sgarbi (Eds.). *Stalking e rischio di violenza. Uno strumento per la valutazione e la gestione del rischio* (pp. 13-40). Milano: Franco Angeli.

Sheridan, L.P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law*, 13(6), 627-640.

Sontag, L.M., & Graber, J.A. (2011). Traditional and Cyber Aggressors and Victims: A Comparison of Psychosocial Characteristics. *Journal of Youth Adolescence*, 40, 392-404.

Spitzberg, B.H., & Cupach, W.R. (2007). *The Dark Side of Interpersonal Communication*. UK: Routledge.

Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker S. (2007). Intimate partner violence, technology, and stalking. *Violence against Women,* 13, 842-856.

Spitzberg, B.H., & Cupach, W.R. (2007). Cyberstalking as (Mis)matching. In M.T. Whitty, A.J. Baker & J.A. Inman (Eds.), *Online Matchmaking* (pp. 127-146). UK: Palgrave Macmillan.

Spitzberg, B.H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society,* 14, 67-88.

Tavani, H.T., & Grodzinsky, F.S. (2002). Cyberstalking, personal privacy, and moral responsibility. *Ethics and information technology,* 4, 123-132.

Tjaden, P., & Thoennes, N. (1998). *Stalking in America: findings from the national violence against women survey.* Washington DC: National Institute of Justice and Center for Disease Control and Prevention, U.S. Department of Justice.

Turvey, B. (1999). *Criminal profiling: An introduction to behavioural evidence analysis*. San Diego, CA: Academic Press.

Wykes, M. (2007). Constructing crime: culture, stalking, celebrity and cyber. *Crime media culture,* 3, 158-174.

Working to Halt Online Abuse (2011). *Online Harassment statistics*. Retrieved May 2012, from http://www.haltabuse.org/resources/stats/index.shtml