RASSEGNA ITALIANA DI CRIMINOLOGIA
ANNO VI N.3 2012

Cyberstalking e molestie portate con strumenti elettronici: aspetti informatico-giuridici

Cyberstalking and electronic devices: relevant legal-informatics issues

Giovanni Ziccardi

Parole chiave: cyberstalking • Internet • furto d'identità • anonimato • molestie

Riassunto
il presente studio tratta del fenomeno del cosiddetto *cyberstalking*, una fattispecie di reato già regolamentata esplicitamente in ordinamenti giuridici differenti da quello italiano (ad esempio: in Nordamerica e in Belgio) o, di contro, solamente abbracciata in maniera implicita in normative che disciplinano l'attività di stalking per così dire "tradizionale". Si vedrà come per *cyberstalking* s'intenda un'attività di stalking attuata *tramite mezzi elettronici* e come molti Stati abbiano portato avanti la scelta legislativa di formulare in dettaglio l'elenco dei comportamenti informatici che rientrerebbero in tale categoria e di definire con cura le locuzioni "mezzi elettronici" e "comunicazioni elettroniche". In particolare, la prima parte dell'analisi ricostruisce la definizione di *cyberstalking*, traendo spunti interpretativi dalla grande riforma normativa occorsa a metà degli anni Novanta negli Stati Uniti d'America e che si è, successivamente, concretizzata in un'articolata legislazione a livello locale. Sono analizzati numerosi articoli di legge che forniscono una definizione di *cyberstalking*, prendendo in considerazione sia normativa generica sullo stalking con occasionali riferimenti al *medium* elettronico, sia articoli espressamente dedicati al mondo digitale. L'analisi prosegue, poi, dedicando attenzione alla normativa e alla giurisprudenza italiana, al fine di valutare l'estensibilità dell'articolo 612-*bis* del codice penale a ipotesi di attività elettroniche o in ambienti "virtuali". Si noterà immediatamente che, data la genericità dell'articolo del codice penale italiano, non è particolarmente problematico fare rientrare tali ipotesi nell'alveo della disciplina codicistica. Nel corso dello studio si analizzeranno, infine, temi prettamente informatico-giuridici quali l'anonimato, il furto di identità, la sostituzione di persona e la OSINT (*Open Source Intelligence*), tecniche tipicamente utilizzate per finalizzare azioni di stalking.

Keywords: cyberstalking • Internet • identity theft • anonymity • harassment

Abstract
this study addresses the issue of the so-called 'cyberstalking', a crime figure formalized in several legal systems, especially in the United States of America, and included even in the text of more general laws on stalking. Generally, cyberstalking is a stalking activity using "electronic devices"; many States have decided to detail the behaviors, the meanings of "electronic" or "electronic communications", and the typical conduct. In particular, the first part of the study deals with the definition of cyberstalking, which refers to a wide regulatory reform in the mid-Nineties that occurred in the United States of America and has, since then, materialized also in a legislation reform at a State level. We will analyze several articles which give a definition of cyberstalking, taking into account both general legislation on stalking with occasional references to the electronic *medium* and norms specifically dedicated to cyberstalking. The analysis, then, moves towards the Italian legislation, to assess the extensibility of Article 612-*bis* of the Italian Criminal Code in electronic or "virtual" issues. The second part of the Article deals with purely computer-legal issues, such as anonymity, identity theft, impersonation and OSINT (Open Source Intelligence): these methods are typically used during stalking activities.

Per corrispondenza: Giovanni Ziccardi, Università degli Studi di Milano – Dipartimento "Cesare Beccaria" – via Festa del Perdono n. 7 – 20122 Milano, Tel. 02-50312714 - e-mail • *giovanni.ziccardi@unimi.it*

GIOVANNI ZICCARDI, Professore Associato Confermato di Informatica Giuridica, Università degli Studi di Milano, Fondatore e Coordinatore del Corso di Perfezionamento in Computer Forensics e Investigazioni Digitali

Cyberstalking e molestie portate con strumenti elettronici: aspetti informatico-giuridici

1. Considerazioni introduttive

Il termine *cyberstalking* (o *cyber-stalking*, o *cyberstalk*) è di semplice comprensione anche da parte di chi non vanti profonde competenze tecnologiche[1]. È un concetto, però, capace di sollevare sin dall'inizio, si vedrà a breve, alcune questioni definitorie che non sono banali e che è bene risolvere già in una fase preliminare.

Ora, l'origine del termine, si diceva, è chiara: si tratta dell'accostamento del termine in lingua inglese *cyber* (il medesimo contenuto in *cibernetica*, *ciberspazio*, etc.) con il verbo che connota l'azione di stalking[2].

Vuole indicare, in estrema sintesi e a puri fini introduttivi, un'attività di stalking che abbia una forte connotazione "cyber", ossia nella quale la componente telematica e informatica sia d'importanza rilevante. In particolare, la componente informatica e telematica nell'azione dello stalker deve permettere (eventualmente in concorso con altre azioni) (Lo Monte, 2011) di approdare ad almeno uno dei tre eventi tipizzati[3] dalla norma, di modo che i comportamenti di minaccia o molestia generino nella vittima:

i) un perdurante e grave stato d'ansia o di paura, o
ii) un fondato timore per l'incolumità propria o altrui, o
iii) un'alterazione delle abitudini di vita.

A connotare il *cyberstalking* in senso lato sarebbe quindi, innanzitutto, la presenza di Internet o di reti di comunicazione di altro genere. L'impatto del fenomeno inizia a essere preso in grande considerazione sia da parte degli studiosi sia da parte delle Forze dell'Ordine: anche in questo ambito, come già è avvenuto, ad esempio, nel campo della diffamazione, si sta paventando un netto prevalere delle "ipotesi telematiche" rispetto alle forme di stalking "tradizionali"; si teme, di conseguenza, che le molestie portate con mezzi tecnologici possano diventare, ben presto, una *regola* e non

1 Nella dottrina italiana più recente, interessante è l'Articolo di Natalini, A. (2010). Quando le molestie persecutorie usano le più recenti tecnologie è "cyberstalking". E si configura il delitto di cui all'art. 612-bis Cp. *Diritto e Giustizia*, 0, 407 (nota a Cassazione Penale 16/07/2010, n. 32404). L'Autore definisce *cyberstalking* "[…] l'impiego spregiudicato e sempre più insidioso delle nuove tecnologie in funzione persecutoria e assillante ai danni delle vittime prescelte", e nel caso *de quo* i comportamenti dello stalker consistevano nel "[…] tempestarla di telefonate, di messaggini, di mail e finendo col divulgare un filmato su Facebook che lo ritraeva durante un rapporto sessuale con la donna". Ciò indica, secondo Natalini, "[…] un orientamento favorevole ad un riconoscimento ad ampio raggio degli estremi del reato di stalking in tutti quei comportamenti persecutori ed ossessionanti, comunque perpetrati - anche col mezzo telefonico o telematico […] purchè siano tali da indurre la persona offesa a cambiare le proprie abitudini di vita, ovvero ingenerino nella stessa un grave stato di ansia o di paura". Si veda, su questo punto, anche Minnella, C. (2011). Restano incerti i confini della punibilità del delitto di atti persecutori. *Cassazione Penale*, 3, 968 (nota a Cassazione Penale 16/07/2010 n. 32404), che dedica un Paragrafo del suo studio proprio al *cyberstalking*. Nel pensiero di questo Autore "Il canale informatico offre al cyberstalker diverse modalità d'azione: l'invio di quantità enormi di e-mail spesso con toni offensivi o sgradevoli; l'intrusione nel sistema informatico della vittima con programmi atti ad assumerne il controllo (trojan horses) o a danneggiarlo (virus); l'assunzione dell'identità del perseguitato spendendo il relativo nome in rete (in chat, newsletters, message boards) associandovi contenuti lesivi della diginità della persona come la presenza di questa identità rubata in siti porno o la spendita del nome della vittima per fargli allacciare relazioni hot nella società off line con soggetti che continuano ripetutamente a chiamare al numero di cellulare diffuso o a contattare l'indirizzo e-mail comunicato senza il consenso della persona offesa".

2 Per una corretta introduzione giuridica e medico-legale al comportamento dello stalker, con particolare attenzione agli aspetti criminologici e psichiatrico-forensi, si veda, *inter alia*, Benedetto G., Zampi M., Ricci Messori M., & Cingolani M. (2008). Stalking: aspetti giuridici e medico legali. *Rivista Italiana di Medicina Legale*, 1, 127. Gli Autori individuano in una definizione del 1997 di Pathé e Mullen (si riferiscono in particolare all'opera Pathé M., & Mullen P.E. (1997). The impact of stalkers on their victims. *British Journal of Psychiatry*, 170, 12) un concetto più "allargato" di stalking che potrebbe agevolmente comprendere anche comportamenti tecnologici, specificando che "[…] intendendo per intrusioni comportamenti quali il pedinare, il sorvegliare, il sostare nelle vicinanze o tentare approcci con la vittima, mentre per comunicazioni si intendono l'invio di lettere e-mail, l'effettuare telefonate, e lasciare messaggi". Interessante, nelle righe di questo studio, l'individuazione della *sorveglianza*, della *comunicazione*, della *ricerca di contatto* e del *controllo* come *quattro* dei fini tipici dello stalker. Sorveglianza e controllo, comunicazione e ricerca di contatto che ben si addicono anche al mondo elettronico. Anche l'attenzione ai comportamenti tipici, nello studio di questi Autori, richiama spesso il possibile aspetto telematico: si pensi, ad esempio, al "pedinamento cibernetico" e a "l'appropriazione della posta".

3 Si veda, per uno studio introduttivo su un possibile identikit dello stalker, Agnino, F. (2011). Delitto di atti persecutori e ricerca per tipo d'autore dello stalker. *Giurisprudenza di Merito*, 9, 2237 (nota a Tribunale di Napoli, 12/11/2010 n. 14877). Circa, invece, un interessante studio sugli avvocati come tipologia di vittima si veda Merzagora I., Bana A., Chinnici N., & de' Micheli A. (2011). L'avvocato come vittima di stalking. *Rivista Italiana di Medicina Legale*, 4-5, 979. Interessante anche lo studio di Morano Cinque E. (2011). L'abuso del processo come forma di stalking giudiziario: è lite temeraria. *Responsabilità Civile e Previdenziale*, 12, 2580 (nota a Tribunale di Varese, 22/01/2011 n. 98 e tribunale di Piacenza, 22/11/2010). Sui profili procedimentali e sui rapporti tra Autorità Giudiziaria e Autorità di Polizia si veda Pulvirenti A. (2011). Note problematiche su alcuni profili procedimentali del delitto di "atti persecutori" (stalking). *Diritto di Famiglia*, 02, 939.

un'eccezione dal punto di vista della frequenza della condotta più comune che connota un simile reato.

Da un punto di vista strettamente giuridico, d'altro canto, il percorso definitorio si rivela leggermente più articolato. Per ora, in senso molto ampio e mutuando una definizione corretta di Maffeo (2009), potremmo definire il *cyberstalking* come "l'utilizzazione di *ogni tipo di comunicazione elettronica* per molestare in forma ossessiva la vittima".

Alcuni ordinamenti giuridici (ad esempio: quello italiano[4]) non presentano, nell'elenco delle fattispecie di reato, sia nel codice sia nelle leggi speciali, una definizione di *cyberstalking*, ma si "limitano" a punire lo stalking con qualsiasi mezzo esso sia commesso.

Altri ordinamenti (tipici sono quello nordamericano o quello del Regno Unito) prevedono figure *ibride*: solo lo stalking è punito ma, nel momento in cui il testo di legge descrive la condotta, si specifica, ad esempio, che il comportamento criminoso può essere portato "anche con l'uso di un mezzo di comunicazione", oppure sono state emendate norme che riguardano i reati commessi con le comunicazioni elettroniche comprendendo esplicitamente anche le molestie.

Un *tertium genus*, infine, molto diffuso nella normativa statale nordamericana (ma anche, ad esempio, nell'ordinamento belga[5]) e di particolare interesse per il nostro studio, prevede proprio il reato di *cyberstalking* o *cyberstalk* (come indicato nella normativa della Florida) esponendo una definizione accurata, accanto alle condotte tipiche, del *cyberstalking*. Non ci si limita, in pratica, a una semplice "attività di molestia commessa con comportamenti fisici o telematici" ma si descrive, in dettaglio, la condotta telematica tipica (ad esempio: "invio ripetuto di e-mail alla vittima o a conoscenti della vittima", e simili).

L'esperienza, anche giuridica, ci insegna che non è spesso necessario un lavoro di dettaglio simile a quello nordamericano per abbracciare tutte le ipotesi e, al contempo, che il problema del divieto di analogia *in malam partem* in materia penale e, soprattutto, l'evoluzione rapidissima delle tecnologie pongono all'interprete, in casi simili, non pochi problemi.

Vero è anche, però, che, mentre il *cyberstalking*, nell'ordinamento nordamericano, è collocato in una sistematica precisa anche a fini esaustivi, in Italia, ad esempio, comportamenti tipici del *cyberstalking* possono essere puniti anche da altri reati che hanno origine e fini completamente diversi. Anticipo, uno per tutti, l'esempio della *sostituzione di persona*, già oggetto di pronuncie anche italiane[6]: il reato di sostituzione di persona, si sa, è collocato in una sistematica e ha fini, nonché tutela interessi (la fede pubblica *in primis*) ben lontani da quelli protetti dalla fattispecie di molestie. Però, comportamento tipico di attività di stalking può essere quello di sostituirsi alla persona presa di mira (ad esempio: creando un indirizzo di posta elettronica *ad hoc* od offrendo in una bacheca prestazioni sessuali al fine di far ricevere alla vittima costantemente telefonate o e-mail offensive o, addirittura, far sì che sconosciuti si presentino presso la sua abitazione in cerca di prestazioni sessuali).

In questo quadro un po' fumoso sono quattro, ad avviso di chi scrive e riprendendo la già vista classificazione di Benedetto et al. (2008), i comportamenti dello stalker che potrebbero connotare l'attività di *cyberstalking*:

i) un'attività di *sorveglianza* nei confronti della vittima. Ed è noto quanto le nuove tecnologie possano aiutare nell'effettuare un'azione capillare di sorveglianza grazie alla loro invasività (si pensi alle recenti funzioni di geo-localizzazione e indicazione del posizionamento del soggetto (Burdon, 2010; Nezhad, Miri & Makrakis, 2008), quali ad esempio *Foursquare*, che dall'utente spesso sono utilizzate come funzioni ludiche – ad esempio: segnalare l'ingresso in un locale o in un parco divertimenti – ma

4 Per un primo commento si veda Maffeo V. (2009). Il nuovo delitto di atti persecutori (stalking): un primo commento al D.L. n. 11 del 2009 (conv con modif. dalla L. n. 38 del 1009). *Cassazione Penale,* 7-8, 2719. Si veda anche Resta F. (2009). Il delitto di stalking verso un nuovo habeas corpus per la donna? *Giurisprudenza di Merito*, 7-8, 1924; Valsecchi A. (2009). Il delitto di "atti persecutori" (il CD. stalking). *Rivista Italiana di Diritto e Procedura Penale*, 3, 1377. Galuppi G., & Macario E. (2010). Lo stalking. *Diritto di Famiglia*, 2, 865, con anche una precisa ricognizione dello stato normativo internazionale. Morano Cinque E. (2010). Stalking: una ricostruzione del fenomeno alla luce delle categorie civilistiche. *Responsabilità Civile e Previdenziale*, 12, 2517 (nota a Cassazione Penale 12 /01/2010 n. 11945 sez V). Quest'ultima nota, in particolare, è interessante perché riguarda anche l'inquadramento, nella fattispecie di atti persecutori, della condotta di chi minaccia altri tramite video e messaggi inviati su *Facebook*. Interessante è anche lo studio di Agnino F. (2011). Il delitto di atti persecutori e lo stato dell'arte giurisprudenziale e dottrinale. *Giurisprudenza di Merito*, 02, 584. Si veda anche, più recente, Bastianello A. (2011). Il reato di stalking ex art. 612-bis C.p. *Giurisprudenza di Merito*, 3, 673 (nota a Tribunale di Salerno 19/10/2011).

5 In Belgio stalking e *cyberstalking* sono previsti in due norme separate. Il crimine generico di stalking è previsto nell'articolo 442-*bis* del Codice Penale, è stato introdotto nel 1998 e punisce chiunque, con una condotta specifica, turba la pace di una persona. Vi è, poi, una previsione di *cyberstalking* nell'articolo 145 §3bis del *Electronic Telecommunications Act* del 2005, introdotto nel 2007 che punisce l'utilizzo di un network di comunicazioni elettroniche, mezzo o servizio o *device*, per ottenere lo stesso risultato.

6 Si veda, *inter alia*, l'interessante studio di Flick, C. (2008). Falsa identità su Internet e tutela penale della fede pubblica degli utenti e della persona. *Rivista di Diritto dell'Informazione e dell'Informatica*, 4-5, 526, a commento di una sentenza che riguardava il caso di un uomo che, dopo aver creato un account di posta elettronica a nome di una amica, l'ha utilizzato per allacciare rapporti con altri utenti rappresentando una sua disponibilità ad avere incontri sessuali e fornendo il suo numero telefonico. Nota l'Autrice come: "Tra gli uomini italiani, in particolare, si va diffondendo l'abitudine di usare internet come strumento per mettere in atto vendette personali a danno di inconsapevoli donne con cui, spesso, hanno avuto rapporti sentimentali o per molestare donne desiderate e irraggiungibili. La procedura è semplice: si apre un account di posta elettronica o un sito Internet a nome della vittima; si instaurano rapporti e-mail o si espongono sul sito foto "accattivanti", dichiarando la disponibilità della ragazza a incontri nel mondo reale e fornendo il numero telefonico della ragazza. Non è difficile immaginare le conseguenze sgradevoli a cui tali situazioni possono portare: nella migliore delle ipotesi la donna ritrova la propria immagine pubblicata su siti di dubbio gusto; in molti casi viene bersagliata di telefonate, in cui le vengono fatte proposte poco edificanti".

per il controllore possono costituire informazioni preziose per la sua attività di sorveglianza);

ii) un'attività di *comunicazione* (spesso ossessiva) nei confronti della vittima. Con riferimento a questo punto assume particolare interesse, in Italia, il caso di *divieto di comunicazione* con la vittima che può essere disposto dal giudice ai sensi dell'articolo 282-*ter* del codice di procedura penale (Macrì, 2009) quale misura cautelare introdotta dal divieto di avvicinamento, nonché il concetto di *comunicazioni indesiderate* (Valsecchi, 2009);

iii) un'attività di *ricerca di contatto*. Si tratta di una via di mezzo tra un pedinamento elettronico e un "aggiramento" compiuto anche collegandosi ad amicizie (ad esempio sui *social network*) e non con contatti iniziali *diretti* con la vittima;

iv) un'attività di *controllo*. E spesso, si sa, le tecnologie, se usate con accortezza, possono permettere per mesi un controllo costante (ad esempio: della posta elettronica) anche all'insaputa della vittima.

Queste quattro categorie (*sorveglianza*, *comunicazione*, *ricerca di contatto* e *controllo*) beneficiano poi, nella loro efficacia, di altri due aspetti fondamentali: la possibile *incompetenza tecnologica* del soggetto controllato, e la possibilità di *correlazione* dei dati offerta dalla tecnologia.

Il primo punto è semplice da comprendere: se la vittima non usa correttamente la tecnologia che ha a disposizione (computer, telefono cellulare, tablet) può offrire, a sua insaputa, informazioni preziose allo stalker. Si pensi, ad esempio, alla configurazione di una *privacy policy* di Facebook debole, all'indicazione nei meta-dati delle fotografie scattate, delle informazioni relative alla latitudine e longitudine geografica, alla connessione *Bluetooth* del proprio telefono cellulare lasciata aperta e visibile, al sistema di GPS del proprio tablet impostato come attivo e in grado di rilevare la posizione dell'utente.

Il secondo punto è più delicato: nel mondo elettronico, la *correlazione di dati* è strumento fondamentale per ricavare una *nuova informazione*, anche con riferimento a un individuo. Spesso la disattenzione in tal senso (e per *disattenzione* s'intende il rendere pubblico un dato che apparentemente, *ex se*, sembra non essere importante ma che, se unito ad altri dati già presenti in rete e magari rilasciati in un momento temporale precedente, *genera una nuova informazione*) porta a facilitare l'attività di controllo da parte di un terzo soggetto ostile.

In un ordinamento complesso quale quello italiano, dunque, dove non è presente una definizione accurata e specifica di *cyberstalking*, la situazione si può rivelare frammentaria.

Nel presente studio, di conseguenza, si è ritenuto opportuno procedere per gradi.

In primis, si effettuerà una sintetica analisi delle definizioni normative più accurate in tema di *cyberstalking*, al fine di cercare di comprendere correttamente ogni tipo di comportamento che si possa presentare all'interprete. Come anticipato, si dovrà attingere da norme di ordinamenti stranieri che, sin dalla metà degli anni Novanta, soprattutto in Nordamerica, hanno riservato attenzione al problema.

Una volta definito il *cyberstalking*, si analizzeranno alcuni comportamenti nel quadro normativo italiano dove, come si è accennato, le attività telematiche sembrano potersi comprendere senza particolari problemi interpretativi nella fattispecie generica dell'articolo 612-*bis*. A margine di tali, brevi osservazioni, si farà cenno anche a qualche recente pronuncia giurisprudenziale che ha "sfiorato" il tema.

La seconda parte della ricognizione riguarderà più prettamente le tecniche informatico-giuridiche tipicamente utilizzate in simili contesti. In particolare, ci si soffermerà sull'*anonimato* (Maggipinto & Iaselli, 2005; Finocchiaro, 2008; Mengoni, 2012) per un motivo che il lettore avrà sicuramente chiaro: la (apparente) maggiore facilità di essere anonimi in Internet che porta molti stalker a cercare di superare, in questo ambiente virtuale, i limiti fisici che tradizionali metodi di stalking pongono (si pensi, ad esempio, alle telefonate e ai pedinamenti).

La parte conclusiva dello studio affronterà i temi del *furto d'identità* (Ziccardi, 2011c; Cajani, Costabile & Mazzarago, 2008; Cajani, 2007; Flor, 2007; Perri, 2007; Ferola, 2009; Di Ronzo, 2009) (anch'esso molto attuale, e sovente correlato ad attività di stalking telematico) e della cosiddetta *Open Source Intelligence* (OSINT), un metodo non invasivo di ricerca d'informazioni relative a individui o società. Per *non invasivo* s'intende un metodo che non consiste, ad esempio, nell'accedere illecitamente a una casella di posta elettronica o a un sito ma, semplicemente, nell'effettuare ricerche utilizzando *fonti aperte*, collegando e correlando i dati anche grazie all'utilizzo di software specifico[7], al fine di ricostruire il profilo di una persona (Olcott, 2012; Tekir, 2009; Bean & Hart, 2011).

2. La disciplina del cyberstalking nella normativa internazionale

2.1. *Il quadro normativo nordamericano e un primo percorso definitorio*

Come si è anticipato, l'ordinamento giuridico degli Stati Uniti d'America è stato uno dei primi a cercare di ordinare, in maniera sistematica, il rapporto tra quel mondo elettronico che oltreoceano, negli anni Ottanta e Novanta, si stava rapidamente espandendo e il tema delle molestie, delle espressioni d'odio, della violenza verbale e del bullismo. Ciò ha dato vita a un quadro che, agli occhi dell'interprete, appare molto interessante e, soprattutto, ricco di spunti.

In primis, a livello di normativa federale, nel 1994 è stato approvato il *Violent Crime Control and Law Enforcement Act*[8], un provvedimento che affrontava anche il problema della violenza contro le donne includendovi i maltrattamenti all'interno delle mura domestiche, lo stalking e le aggressioni sessuali. Successivamente, nel 1996, è stato emanato l'*Interstate Stalking Punishment and Prevention Act*[9], con il quale è

7 Ad esempio il software open source *Maltego*, reperibile in Internet all'indirizzo http://www.paterva.com/web5/o le soluzioni offerte dalla casa di software *Kapow*, all'indirizzo http://www.kapowsoftware.com.

8 Informazioni sul testo sono in Internet all'indirizzo http://-www.nij.gov/pubs-sum/000067.htm

9 Informazioni sul testo sono in Internet all'indirizzo https://-www.ncjrs.gov/ovc_archives/nvaa/supp/t-ch21-2.htm

stato introdotto lo specifico reato di stalking a livello interstatale. Sempre a livello federale il Congresso ha poi elaborato il *Violence Against Women Act* (VAWA) del 2000 che, tra l'altro, punisce l'uso della posta elettronica o di ogni altro mezzo di scambio d'informazione, tra gli Stati o da e verso l'estero, volto a perseguitare la vittima o i membri della sua famiglia. Infine, nel 2005, è stato emendato lo stesso *Violence Against Women Act*[10] prevedendo come ipotesi di reato qualunque condotta che possa causare alla vittima una rilevante angoscia emozionale (*substantial emotional distress*).

Accanto a questo primo approccio "generico", d'interesse marginale per il nostro studio (tranne il riferimento alla *posta elettronica* contenuto nel VAWA), preme invece notare che sono numerosi gli Stati che, negli Stati Uniti d'America, hanno previsto leggi che menzionano esplicitamente il reato di "cyberstalking" o "cyberharassment" (e non più solo il "semplice" stalking) o che hanno emanato normativa che prevede esplicitamente forme elettroniche di comunicazione all'interno delle più tradizionali leggi sullo stalking o sull'*harassment*. Vi è, poi, un settore in forte espansione (anche normativa) che è quello del cyber-bullismo, che sta generando un corpo di leggi *ad hoc* per prevenire il "cyberbulling" e che contiene all'interno norme chiaramente mutuate dalla disciplina in tema di stalking. Anzi, ci sia consentito di scrivere che molto spesso siamo in presenza semplicemente di norme sullo stalking ricondotte, però, a un contesto di minori: in sostanza, azioni di stalking da minore contro minore.

Si noti una cosa: il fatto che uno Stato non preveda una normativa *ad hoc* in tema di cyberstalking non significa che in quello Stato tali comportamenti non siano puniti. Alcuni Stati hanno mantenuto "l'approccio italiano", non avvertendo l'esigenza di specificare l'aspetto elettronico del fenomeno. La maggiore specificità del linguaggio, certo, può rendere sia più facile la punizione del colpevole sia alimentare un maggiore attenzione e sensibilità nei confronti del fenomeno, ma da un punto di vista della possibilità di sanzionare lo stalker, spesso non vi è differenza.

Nella normativa statunitense che andremo, per sommi capi, ad analizzare, sono tre le fattispecie più ricorrenti:

i) il *cyberstalking*,
ii) il *cyberharassment* e
iii) il *cyberbulling*.

Ora, non è semplice definire queste tre ipotesi con un approccio che muova dal nostro ordinamento giuridico e dalle categorie italiane. Cercando però d'interpretare la volontà del Legislatore nordamericano, potrebbero essere corrette le seguenti tre definizioni:

a) per *cyberstalking* s'intende, da un punto di vista normativo, l'uso di Internet, della posta elettronica o di un altro mezzo di comunicazione per portare avanti un'attività di stalking. Di solito la norma presa come riferimento specifica un comportamento, o un "percorso elettronico", che viene usato per portare avanti comportamenti offensivi o minacciosi. Nell'economia della legge americana questa è la più grave delle tre ipotesi, in quanto prevede quasi sempre che si sia posta una *credibile minaccia di danno o di violenza alla persona*.

b) Per *cyberharassment* s'intende, quasi sempre, una fattispecie più lieve di quella illustrata al punto precedente (tranne in quegli Stati dove l'ipotesi a) non è prevista e l'*harassment* è, di conseguenza, il comportamento più grave). Si differenzierebbe dal *cyberstalking* in quanto, di solito, non coinvolge una minaccia *credibile* bensì riguarda l'azione di minacciare o molestare un terzo tramite messaggi di posta elettronica, messaggi istantanei o *post* sui blog o su siti web al solo fine di tormentare un individuo. Sembrerebbe quindi *prima facie* una fattispecie più correlata al *linguaggio utilizzato* in ambiente elettronico che alla *reale minaccia* di un pericolo. Si veda, a puro titolo di esempio, il testo del *Code of Alabama*: non prevede una norma sul *cyberstalking*, ma ne prevede una specifica sul *cyberharassment*[11] tanto da dar vita alla fattispecie *sui generis* delle *harassing communications* dove vengono specificate le attività compiute (si noti: anche in maniera anonima) con e-mail o comunicazioni elettroniche.

c) per *cyberbulling* s'intende un comportamento che non riguarda, se non marginalmente, i temi di nostra cura ma che viene ricondotto ad attività di stalking, di bullismo e di violenza operate fra minori nelle scuole.

2.2. *Le definizioni di stalking comprensive del* cyberstalking

Spostandoci dal quadro federale e interstatale a quello statale, si può osservare come molti Stati abbiano adottato approcci diversi in fase di definizione del *cyberstalking*. La nostra analisi prenderà le mosse dalle ipotesi più semplici, sino ad arrivare a esporre quelle più articolate.

10 Informazioni sul testo sono in Internet all'indirizzo http://www.govtrack.us/congress/bills/109/hr3402/text

11 Ci si riferisce, in particolare, al testo presente nella Section 13A-11-8 del Code of Alabama ("Harassment or harassing communications") e alla fattispecie delle *harassing communications*. Interessante, a nostro avviso, è che subito dopo la fattispecie tradizionale di Harassment: ("(a) (1) HARASSMENT. A person commits the crime of harassment if, with intent to harass, annoy, or alarm another person, he or she either: a. Strikes, shoves, kicks, or otherwise touches a person or subjects him or her to physical contact. b. Directs abusive or obscene language or makes an obscene gesture towards another person. (2) For purposes of this section, harassment shall include a threat, verbal or nonverbal, made with the intent to carry out the threat, that would cause a reasonable person who is the target of the threat to fear for his or her safety. (3) Harassment is a Class C misdemeanor" sia stata introdotta la fattispecie di *harassing communications* (" (b) (1) HARASSING COMMUNICATIONS. A person commits the crime of harassing communications if, with intent to harass or alarm another person, he or she does any of the following: a. Communicates with a person, anonymously or otherwise, by telephone, telegraph, mail, or any other form of written or electronic communication, in a manner likely to harass or cause alarm. b. Makes a telephone call, whether or not a conversation ensues, with no purpose of legitimate communication. c. Telephones another person and addresses to or about such other person any lewd or obscene words or language. Nothing in this section shall apply to legitimate business telephone communications. (2) Harassing communications is a Class C misdemeanor").

Il *Revised Code of Washington*, nel 2004, ha introdotto esplicitamente una delle definizioni più semplici di *cyberstalking*[12], che si sofferma anche su alcune nozioni "informatiche" e che, quindi, può essere presa come ottimo punto di partenza, seppure di base.

Nel testo in oggetto si nota, infatti, come ciò che distingue lo stalking "semplice" dal *cyberstalking* sia semplicemente la frase "[…] and under circumstances not constituting telephone harassment, makes an electronic communication to such other person or a third party".

Siamo in presenza, nella pratica, di una definizione che esclude, da un lato, tutte le attività *telefoniche* dal novero del *cyberstalking* e, dall'altro, che comprende nello stesso la definizione di *electronic communication*.

Ora, il primo punto (se si utilizza il telefono siamo nell'alveo dello stalking, e non del *cyberstalking*) è chiaro nella sua genesi, ma può mostrare il fianco ad alcune critiche. È chiaro in quanto, come è noto, la telefonata è il mezzo principe per portare attività di stalking nei confronti della vittima; è anche vero, però, che nei tempi moderni, con le reti telefoniche digitali e, soprattutto, con il Voice over IP (si pensi al software *Skype*) la distinzione tra telefonia tradizionale e mezzi di comunicazione digitale è un po' scemata.

La norma che stiamo analizzando, al punto (5), definisce poi le *electronic communications* come "the transmission of information by wire, radio, optical cable, electromagnetic, or other similar means. 'Electronic communication' includes, but is not limited to, electronic mail, internet-based communications, pager service, and electronic text messaging".

Da un lato, quindi, la legge cerca di definire il più possibile i mezzi elettronici ma, dall'altro, lascia comprensibilmente e giustamente aperta tale definizione a ogni altro mezzo che in futuro si possa diffondere.

Anche il *Code of Virginia* segue l'approccio minimalista inaugurato dal *Revised Code of Washington*, ma lo fa aggiungendo elementi interessanti che ci pare opportuno commentare[13]. Si noti, in particolare, il seguente passaggio: "Any person who knowingly communicates, in a writing, including an electronically transmitted communication producing a visual or electronic message…".

Ora, appare chiaro come la definizione, in questo caso, rispetto alla generica dizione dello Stato di Washington, si sia spinta un po' oltre e abbia aggiunto *transmitted*. "Una comunicazione trasmessa elettronicamente" dà sicuramente una maggiore idea di dinamicità, così come la dizione "la produzione di un messaggio visuale o elettronico" è pensata al fine di comprendere anche, ad esempio, l'invio di immagini o video.

Il *Criminal Code* dello Utah, al *Title 76*, *Chapter 5*, *Section 106-5*[14], specifica come si possa definire un *cyberstalker* chi "[…] uses a computer, the Internet, text messaging, or any other electronic means to commit an act that is a part of the course of conduct".

Sono specificate quattro "categorie elettroniche", quindi, di cui una di chiusura: i) un computer, ii) Internet, iii) messaggi di testo o iv) qualsiasi altro mezzo di comunicazione.

Sempre questa normativa stabilisce, poi, come vadano intesi come "messaggi di testo" "[…] a communication in

12 Ci si riferisce al RCW 9.61.260 dello Stato di Washington e al reato di "Cyberstalking". In particolare la parte citata recita: (1) A person is guilty of cyberstalking if he or she, with intent to harass, intimidate, torment, or embarrass any other person, and under circumstances not constituting telephone harassment, makes an electronic communication to such other person or a third party: (a) Using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act; (b) Anonymously or repeatedly whether or not conversation occurs; or (c) Threatening to inflict injury on the person or property of the person called or any member of his or her family or household. (2) Cyberstalking is a gross misdemeanor, except as provided in subsection (3) of this section. (3) Cyberstalking is a class C felony if either of the following applies: (a) The perpetrator has previously been convicted of the crime of harassment, as defined in RCW 9A.46.060, with the same victim or a member of the victim's family or household or any person specifically named in a no-contact order or no-harassment order in this or any other state; or (b) The perpetrator engages in the behavior prohibited under subsection (1)(c) of this section by threatening to kill the person threatened or any other person. (4) Any offense committed under this section may be deemed to have been committed either at the place from which the communication was made or at the place where the communication was received. (5) For purposes of this section, "electronic communication" means the transmission of information by wire, radio, optical cable, electromagnetic, or other similar means. "Electronic communication" includes, but is not limited to, electronic mail, internet-based communications, pager service, and electronic text messaging".

13 Ci si riferisce alla seguente norma: "§ 18.2-60. Threats of death or bodily injury to a person or member of his family; threats to commit serious bodily harm to persons on school property; penalty. A. 1. Any person who knowingly communicates, in a writing, including an electronically transmitted communication producing a visual or electronic message, a threat to kill or do bodily injury to a person, regarding that person or any member of his family, and the threat places such person in reasonable apprehension of death or bodily injury to himself or his family member, is guilty of a Class 6 felony. However, any person who violates this subsection with the intent to commit an act of terrorism as defined in § 18.2-46.4 is guilty of a Class 5 felony. 2. Any person who communicates a threat, in a writing, including an electronically transmitted communication producing a visual or electronic message, to kill or do bodily harm, (i) on the grounds or premises of any elementary, middle or secondary school property, (ii) at any elementary, middle or secondary school-sponsored event or (iii) on a school bus to any person or persons, regardless of whether the person who is the object of the threat actually receives the threat, and the threat would place the person who is the object of the threat in reasonable apprehension of death or bodily harm, is guilty of a Class 6 felony. B. Any person who orally makes a threat to any employee of any elementary, middle or secondary school, while on a school bus, on school property or at a school-sponsored activity, to kill or to do bodily injury to such person, is guilty of a Class 1 misdemeanor. A prosecution pursuant to this section may be either in the county, city or town in which the communication was made or received".

14 Si veda in Internet all'indirizzo http://le.utah.gov/~code/TITLE76/htm/76_05_010605.htm

the form of electronic text or one or more electronic images sent by the actor from a telephone or computer to another person's telephone or computer by addressing the communication to the recipient's telephone number". Saremmo in presenza, quindi, di un'ipotesi ibrida, che unisce il telefono alle immagini (si pensi all'invio di MMS).

Il codice del South Dakota[15] sanziona, invece, il comportamento di chi "[…] Willfully, maliciously, and repeatedly harass another person by means of any verbal, electronic, digital media, mechanical, telegraphic, or written communication". In questo caso vi è una chiara equiparazione esplicita tra il mezzo scritto, il mezzo verbale e i *digital media*.

In Ohio, all'articolo 903.211[16], il comportamento definito *menacing by stalking* prevede che: "No person, through the use of any electronic method of remotely transferring information, including, but not limited to, any computer, computer network, computer program, or computer system, shall post a message with purpose to urge or incite another to commit a violation of division (A)(1) of this section".

Si noti che, rispetto agli esempi citati poco sopra, una definizione più dettagliata sta prendendo corpo. Si parla infatti di *qualsiasi mezzo* per trasferire in remoto le informazioni e si fa cenno alle *reti per computer* e all'azione di "post a message" (inteso, nel testo, come "transferring, sending, posting, publishing, disseminating, or otherwise communicating, or attempting to transfer, send, post, publish, disseminate, or otherwise communicate, any message or information, whether truthful or untruthful, about an individual, and whether done under one's own name, under the name of another, or while impersonating another"). Questo aspetto del "posting" è molto interessante non solo per la definizione in sé ma anche, si noti, per la specificazione di tre tipiche possibilità di impersonificazione assai semplici in Internet:

i) a proprio nome,
ii) a nome di un altro,
iii) prendendo le sembianze e l'identità di un soggetto terzo.

2.3. *Due ipotesi specifiche di cyberstalking: North Carolina e Florida*

Le definizioni generiche e ibride illustrate sommariamente nei paragrafi precedenti sono pienamente idonee, si è visto, a comprendere all'interno dei comportamenti di stalking anche attività portate dall'agente con mezzi elettronici.

Alcuni Stati, però, hanno preferito affiancare all'ipotesi di stalking la vera e propria nozione di *cyberstalking*, definendo meglio tale comportamento al fine di garantire una maggiore protezione anche contro il potenziale dannoso delle nuove tecnologie. In questo paragrafo accenneremo a due esempi tipici: la normativa del North Carolina e quella della Florida.

In North Carolina[17] l'ipotesi di *cyberstalking* è stata elaborata prestando particolare attenzione al mezzo elettronico[18]; l'esempio di questo Stato è un esempio che potremmo definire "puro" (meglio: formalizzato) di *cyberstalking*.

In particolare, il Legislatore ha proceduto a una distinzione preliminare tra:

i) *comunicazioni elettroniche*, intese come qualsiasi tipo di trasferimento in "ambiente elettronico" di scritti, immagini, suoni e dati di qualsiasi natura, e
ii) *posta elettronica*, intesa come un messaggio di e-mail inviato da un qualsiasi dispositivo, incluso un telefono.

All'esito di questa prima bipartizione, la norma sanziona, poi, quattro condotte specifiche, prevede una norma molto utile (nella pratica) sul *locus commissi delicti* e una norma finale di garanzia.

Le quattro condotte disciplinate consistono in:

1. utilizzare espressioni testuali ("parole") o portare minacce tramite messaggi di e-mail o utilizzando altri sistemi di comunicazione elettronica;
2. scrivere a una persona ossessivamente o abusare ripetutamente del mezzo della posta elettronica anche semplicamente per mettere in imbarazzo o annoiare il ricevente;

15 Si veda in Internet all'indirizzo http://legis.state.sd.us/statutes/DisplayStatute.aspx?Statute=22-19A-1&Type=Statute

16 Si veda in Internet all'indirizzo http://codes.ohio.gov/orc/2903.211.

17 Il testo è reperibile in Internet all'indirizzo http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-196.3.html.

18 Ci si riferisce in particolare al punto § 14 196.3: "Cyberstalking. (a) The following definitions apply in this section: (1) Electronic communication. – Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or in part by a wire, radio, computer, electromagnetic, photoelectric, or photo optical system. (2) Electronic mail. – The transmission of information or communication by the use of the Internet, a computer, a facsimile machine, a pager, a cellular telephone, a video recorder, or other electronic means sent to a person identified by a unique address or address number and received by that person. (b) It is unlawful for a person to: (1) Use in electronic mail or electronic communication any words or language threatening to inflict bodily harm to any person or to that person's child, sibling, spouse, or dependent, or physical injury to the property of any person, or for the purpose of extorting money or other things of value from any person. (2) Electronically mail or electronically communicate to another repeatedly, whether or not conversation ensues, for the purpose of abusing, annoying, threatening, terrifying, harassing, or embarrassing any person. (3) Electronically mail or electronically communicate to another and to knowingly make any false statement concerning death, injury, illness, disfigurement, indecent conduct, or criminal conduct of the person electronically mailed or of any member of the person's family or household with the intent to abuse, annoy, threaten, terrify, harass, or embarrass. (4) Knowingly permit an electronic communication device under the person's control to be used for any purpose prohibited by this section. (c) Any offense under this section committed by the use of electronic mail or electronic communication may be deemed to have been committed where the electronic mail or electronic communication was originally sent, originally received in this State, or first viewed by any person in this State. (d) Any person violating the provisions of this section shall be guilty of a Class 2 misdemeanor. (e) This section does not apply to any peaceable, nonviolent, or nonthreatening activity intended to express political views or to provide lawful information to others. This section shall not be construed to impair any constitutionally protected activity, including speech, protest, or assembly".

3. comunicare tramite messaggi di e-mail delle *false informazioni* che riguardino, ad esempio, la morte, un infortunio, una malattia o condotte criminali, indecenti o imbarazzanti della persona ricevente;
4. essere pienamente consapevoli, e permettere, che uno strumento elettronico sotto il controllo di un soggetto sia usato da un terzo per i fini indicati nei punti precedenti (si tratta, in sostanza, di una responsabilità per l'uso illecito da parte di terzi dello strumento elettronico con la consapevolezza del proprietario).

La norma sul *locus commissi delicti* prevede che il reato si consideri commesso nel luogo da cui la e-mail originaria, o la comunicazione originaria, ha avuto origine (ad esempio: da dove è stata spedita) o, in alternativa, nello Stato in cui è stata ricevuta per la prima volta o, infine, nello Stato in cui è stata per prima vista da un soggetto.

La norma di garanzia, infine, stabilisce che il reato di *cyberstalking* non si applichi in quei casi in cui siano svolte attività pacifiche, non violente e non minacciose, finalizzate a esprimere opinioni politiche o a fornire informazioni legittime a terzi.

La normativa della Florida[19] prevede, a sua volta, il reato di *cyberstalk*, individuato come "[…] to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose".

La definizione, in questo caso, include esplicitamente *testo* e *immagini* e l'utilizzo di posta elettronica o l'effettuazione di comunicazioni elettroniche al fine di ossessionare una persona specifica e causare ansia nella stessa senza alcun motivo legittimo.

2.4. *L'ordinamento del Regno Unito e l'asserita urgenza di una riforma normativa*

In Regno Unito, da un punto di vista legislativo, qualsiasi tipo di minaccia portata con mezzi elettronici e correlata al reato di stalking è, per tradizione, disciplinata da due atti normativi abbastanza risalenti: il *Protection from Harassment Act* del 1997[20] e il *Malicious Communications Act* del 1998[21].

Sono, questi, due importanti provvedimenti che erano stati pensati, però, per fini differenti rispetto alla repressione del *cyberstalking*. Il primo, in particolare, mette al centro dell'attenzione normativa il fenomeno dell'*harassment*; il secondo, invece, si focalizza sulle cosiddette *malicious communications*, ossia l'uso dei mezzi di comunicazione per veicolare informazioni reputate offensive o con fini non leciti.

La stampa generalista, intervistando sovente funzionari di polizia e investigatori, ha spesso sollevato dubbi circa l'adeguatezza di una normativa così risalente, addirittura precedente al boom di Internet e della telefonia cellulare, nel gestire i fenomeni attuali, così diffusi e, soprattutto, così insidiosi[22].

Il *Malicious Communications Act* del 1998, si diceva, è un provvedimento che era stato elaborato attorno al comportamento criminale di chi invia o consegna "fisicamente" scritti e articoli pensati per causare ansia o dolore nel ricevente. Al *Chapter 27*, in particolare, si parla esplicitamente di *electronic communication* come vettore che può portare messaggi indecenti o offensivi, minacce o informazioni consapevolmente false[23].

In particolare, un aspetto che nello studio *de quo* ci interessa specificamente, per *electronic communication* s'intende ogni comunicazione orale o scritta fatta ai sensi del *Telecommunications Act* del 1984 e ogni comunicazione, in qualsiasi modo inviata, che sia *in forma elettronica*.

3. La normativa e la giurisprudenza italiana e l'articolo 612-bis

Dopo le premesse, anche definitorie, e dopo avere anticipato la scelta di politica legislativa del Legislatore italiano, ossia quella di *non prevedere* la fattispecie del *cyberstalking* ma di prevedere, al contrario, una fattispecie così ampia del 612-*bis* sì da poter agevolmente ricomprendere anche tutte le condotte riportate sopra, l'analisi del quadro nazionale risulta lineare.

Chi scrive è anche dell'avviso che non sia necessario specificare nel dettaglio ogni aspetto tecnologico, con il rischio, da un lato, di demonizzare la tecnologia stessa e, dall'altro, di non riuscire a stare al passo dei ritrovati tecnologici (si pensi alla diffusione, in questi mesi, di software per la geo-localizzazione anche in ambienti urbani che possono, in prospettiva, diventare strumenti utili per attività di stalking).

Può essere interessante, per l'interprete, rileggere un articolo così ad ampio spettro come il 612-*bis* al fine di valutare la sua applicabilità anche in condizioni non tipiche, ad esempio in ambienti di realtà virtuale (*Second Life*) o di giochi online complessi: «Art. 612-bis (Atti persecutori). - Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a quattro anni chiunque, **con condotte reiterate**, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da

19 Si veda il testo della legge in Internet all'indirizzo http://www.haltabuse.org/resources/laws/florida.shtml

20 In Internet all'indir izzo http://www.legislation.gov.uk/ukpga/1997/40/contents

21 In Internet all'indirizzo http://www.legislation.gov.uk/ukpga/1988/27/contents

22 Esemplare, in tal senso, è un articolo veicolato da BBC News nel maggio del 2011 e firmato da Samantha Fenwick dal significativo titolo "Cyber-stalking laws: police review urged", in Internet all'indirizzo http://www.bbc.co.uk/news-/13200185.

23 Il testo del provvedimento normativo recita: "**Offence of sending letters etc. with intent to cause distress or anxiety**. Any person who sends to another person a letter, electronic communication or article of any description which conveys (i) a message which is indecent or grossly offensive; (ii) a threat; or (iii) information which is false and known or believed to be false by the sender; or b) any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature".

ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita. […] La pena è aumentata fino alla metà se il fatto è commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, ovvero con armi o da persona **travisata**. Il delitto è punito a querela della persona offesa.».

A tal proposito, la Sezione VI della Corte di Cassazione italiana, con sentenza n. 1279 del 16 luglio 2010, 32404/10 (R.G. n. 17992/10), si è occupata di un caso estremamente interessante.

Si discuteva, in particolare, della sostituzione della misura cautelare in carcere con quella degli arresti domiciliari nei confronti di un soggetto che era indagato per il reato di cui al 612-*bis* oltre che per il reato di calunnia nei confronti della ex fidanzata e del nuovo compagno della stessa.

Le attività investigative avevano rilevato azioni di molestie concretizzatesi in telefonate, invio di e-mail, di SMS nonché di messaggi tramite *Facebook*, oltre alla trasmissione tramite Facebook al nuovo compagno della donna di un filmato che ritraeva un rapporto sessuale, e l'invio di un compact-disc in ufficio con immagini intime che la riguardavano.

Tutte queste ipotesi (comprese quelle "elettroniche") per i giudici contribuivano in egual modo a configurare il reato di stalking senza dare origine a particolari problemi interpretativi.

4. Il furto d'identità come strumento per attività di cyberstalking

Il cosiddetto *identity theft*, il "furto d'identità", che le statistiche indicano anche in Italia come il comportamento "malevolo" più diffuso degli ultimi anni tra gli utilizzatori di Internet e delle nuove tecnologie ma cui ancora non è dedicato un articolo *ad hoc* nella sistematica penalistica italiana, assume una particolare importanza anche quando si discute di *cyberstalking*, dal momento che può essere associato e può essere, spesso propedeutico, ad attività di molestia telematica.

Il furto d'identità si caratterizza, a livello generale e da un punto di vista informatico-giuridico, per i seguenti fattori:

i) la presenza di alcuni elementi tipici;
ii) la presenza, al contempo, di alcuni elementi estremamente mutevoli, anche in spazi temporali molto rapidi;
iii) una stretta connessione all'evoluzione tecnologica che ne consente la realizzazione in forme sempre nuove che creano notevoli problemi alle Forze dell'Ordine, alle attività investigative e all'interprete.

Con riferimento al primo punto, ossia agli elementi tipici, il furto di identità, volendo procedere a una prima qualificazione per sommi capi, è, appunto, una sorta di "furto" di una identità umana. In caso di *cyberstalking*, si può parlare sia di furto dell'identità della vittima sia di furto dell'identità di un terzo amico, conoscente o vicino alla vittima.

In primis, si noti che il termine "furto" non deve in alcun modo essere inteso come strettamente connesso al reato previsto e punito dall'articolo 624 del codice penale, ipotesi tipicamente forgiata avendo attenzione ai beni mobili o, comunque, fisicamente asportabili.

Nel caso che ci interessa si è utilizzato, probabilmente in maniera non corretta, il termine "furto" per indicare l'accadimento conseguente a un'azione che porta un soggetto ad appropriarsi dell'identità di un altro individuo, causando un danno, anche dal punto di vista psicologico, molto forte o, nel caso di cyberstalking, tentando di garantire una sorta di anonimato o di "sviare" i sospetti.

Gran parte della letteratura, soprattutto tecnica, ritiene quindi il concetto stesso di "furto d'identità" scorretto, essendo preferibile il termine "clonazione", "impersonificazione" o "frode" d'identità.

Nonostante simili rilievi, però, il termine "furto d'identità" è diventato di uso comune ed è stato incorporato, negli ultimi anni, in testi di legge di ordinamenti anglo-americani con l'espressione *identity theft*.

Stessa attenzione occorre dedicarla, in questa fase definitoria preliminare, al termine "identità".

Anche in questo caso, la nozione di "identità" va intesa in termini molto ampi e non, a parere di chi scrive, aderente alle categorie dell'identità e dei suoi diritti proprie del nostro sistema giuridico.

Il "furto", ad esempio, può avvenire nei confronti dell'identità globale del soggetto ma anche di alcune "parti" significative dell'identità stessa (dati bancari, dati medici, numeri di carte di credito, altri dati sensibili d'interesse del criminale informatico o dello stalker).

Non sempre vi è, quindi, un reale furto di "tutta" l'identità del soggetto (s'immagini il caso di una "nuova" persona circolante al posto dell'originale, come rappresentato in alcuni film di successo) ma l'appropriazione, egualmente pericolosa e dannosa, di alcuni dati specifici correlati al soggetto preso di mira.

Si noti che il concetto d'identità in rete è, per molti versi, molto più debole di quello che si esplica nella vita reale.

In molti casi è nota la facilità con cui si può creare un'identità in rete (una casella di posta elettronica, un profilo sul *social network Facebook*, una utenza su un sistema di messaggistica) senza dover affrontare gli ostacoli che potrebbero condizionare tale operazione nel mondo reale.

In sintesi, vi è una estrema facilità nella creazione di una identità in rete per due motivi: i) garantire all'utente una certa semplicità durante la procedura di "registrazione" e ii) aggirare la burocrazia, ed evitare che il fornitore di servizi elettronici debba ritardare l'attivazione degli stessi perché sottoposto all'obbligo di controlli troppo accurati. Con riferimento a quest'ultimo punto, è noto che un sistema di controllo capillare anche nell'offerta di servizi di non importanza critica porterebbe, nella pratica, grosse difficoltà di attuazione; la creazione di una falsa identità nel mondo elettronico è, quindi, un'operazione alla portata di ogni soggetto anche dotato di minime competenze informatiche.

Il furto di identità è un tipico comportamento che prende di mira l'ingenuità, la buona fede e le scarse competenze del soggetto/vittima.

Siamo in presenza di comportamenti che, a tal fine, sono solitamente diretti, nelle fasi iniziali, nei confronti di migliaia di soggetti contemporaneamente, al fine di "scremare" da tutti gli obiettivi le persone più competenti e sospettose,

poco idonee a cadere nella trappola, e sfruttare invece i punti di debolezza di altre. In caso di *cyberstalking* la strategia (e la motivazione) alla base del furto di identità può essere differente: l'identità della vittima viene presa di mira proprio per causare alla stessa un danno sia psicologico sia patrimoniale.

Tipicamente, i punti deboli presi di mira da parte di chi si attiva per operare un furto di identità sono i seguenti:

a) *incompetenza informatica*. Il soggetto attaccato non è in grado di comprendere che i comportamenti che gli vengono suggeriti, siano essi la lettura urgente di un SMS (Perri, 2008) o di messaggio di posta elettronica, il seguire un collegamento, il compilare un modulo o l'installare un *software* sul proprio computer, sono finalizzati a portare un danno nei suoi confronti;
b) *inganno portato con artifizi e raggiri e con falsificazioni accurate*. Il soggetto che viene attaccato può essere mediamente esperto, ma la trappola è così ben congegnata (messaggi di posta elettronica che apparentemente, anche graficamente, sembrano genuini e provenienti dal soggetto reale, mascheramento dei collegamenti, anche sfruttando vulnerabilità dei *software* comunemente usati, affinché al soggetto appaia un collegamento corretto, numeri di telefono, anche fissi, da chiamare e dati apparentemente reali) che anche una simile vittima viene convinta a tenere determinati comportamenti;
c) *inganno portato prospettando profitti molto alti in breve tempo e in assoluta sicurezza*. In tal caso, la proposta che perviene da chi sta cercando di ingannare la vittima è apparentemente chiara e lineare, si potrebbe dire quasi veritiera, e prospetta all'agente profitti molto alti se lo stesso contribuirà alla effettuazione di operazioni finanziarie che vengono prospettate come legittime.

Si noti che il furto d'identità, così come illustrato anche dalla casistica, è un tipo di reato che richiede una forte cooperazione e collaborazione, quasi sempre involontaria, della vittima.

Non è possibile indicare in maggiore dettaglio il comportamento tipico, per un motivo molto semplice: le modalità di attuazione mutano con il mutare delle tecnologie.

Negli ultimi quattro anni si sono registrati centinaia di tipi diversi d'azione, tra i quali si possono delineare solamente alcuni punti in comune.

Il primo è l'uso, solitamente, della tecnologia più diffusa al momento dell'azione. Il furto d'identità è nato utilizzando la posta elettronica e si è evoluto sfruttando (anche) quei sistemi che, a seconda della diffusione della tecnologia nella popolazione, diventavano comuni. La diffusione capillare dei telefoni cellulari ha portato al furto d'identità tramite SMS, la diffusione di *Facebook* e dei *social network* ha portato le azioni su quel nuovo territorio, e così via. Non vi è, quindi, un ambiente preferito per le azioni di furto di identità: si tratta di una fattispecie che si plasma e si adegua alle tecnologie del momento.

Il furto d'identità, dal punto di vista giuridico, ha avuto, in tutto il mondo, un'evoluzione particolare.

Alcuni Stati hanno pensato, data la gravità del fenomeno e i danni economici portati dallo stesso, nonché il grande numero di vittime, di elaborare una fattispecie penale nuova.

Negli Stati Uniti d'America, ad esempio, la fattispecie dell'*identity theft* come reato a sé stante e punito con sanzioni specifiche è da tempo prevista. Nel 1998 il Congresso ha approvato infatti l'*Identity Theft and Assumption Deterrence Act*, un provvedimento normativo che ha introdotto la nuova fattispecie di *identity theft*, intesa come il comportamento di chi consapevolmente trasferisce o utilizza, senza averne diritto, un mezzo di identificazione di un'altra persona con l'intento di commettere, o per coadiuvare, una attività criminale. In quel Paese la fattispecie di *identity theft* occorre nel momento in cui un soggetto utilizza le informazioni identificative personali di un altro, come ad esempio il nome della persona, il numero di sicurezza sociale, il numero di carta di credito o altre informazioni finanziarie, senza permesso, per commettere frodi o altri crimini.

Oltreoceano già ventinove Stati vantano previsioni codicistiche specifiche per sanzionare il furto d'identità, e undici Stati hanno addirittura creato dei programmi di prevenzione e di repressione *ad hoc* con riferimento al furto d'identità, anche al fine di aiutare le vittime che lo hanno subito. Analizzando i semplici titoli di simili previsioni normative, è facile comprendere la sostanza di tale reato: si parla di *Consumer Identity Protection Act* (focalizzando l'attenzione normativa sulla tutela del consumatore), di *Trafficking in stolen identities* (contrabbando di identità rubate), di *Obstructing justice using a false identity* (ostacolo all'amministrazione della Giustizia utilizzando una falsa identità), *Taking identity of another person or entity* (furto di identità di una persona o società), *knowingly accepting identity of another person* (consapevole accettazione dell'identità di un'altra persona), *Financial identity fraud & non-financial identity fraud* (furto d'identità in ambito finanziario), *Possession of identity theft tools* (possesso di strumenti idonei a falsificare l'identità), *Obtaining property by false personation* (ottenimento di diritti di proprietà utilizzando informazioni personali false), *Use of deceased's personal identification information* (utilizzo di informazioni identificative di persone decedute) sino al *False personation of attorney, judicial, or governmental officials* (falsa impersonificazione di avvocato, giudice o funzionario governativo). Si noterà, come anticipato in premessa, che anche nell'ordinamento statunitense sono decine le forme attraverso le quali il reato di furto d'identità si possa manifestare in concreto nel tessuto sociale. La normativa federale e statale statunitense ha ritenuto opportuno indicare il più possibile nel dettaglio i singoli comportamenti riunendoli nella fattispecie dell'*identity theft*.

Altri Stati, tra cui l'Italia, hanno affrontato questo nuovo fenomeno estendendo, ove possibile, reati già previsti per il mondo "fisico" ma considerati applicabili anche a tali circostante e comportamenti.

Come si accennava poco sopra, non è possibile tipizzare comportamenti che si terranno nei prossimi mesi o anni grazie alla diffusione di nuove tecnologie, né prevedere a cosa porterà l'ingegno criminale.

Si vedrà che sinora, nel nostro ordinamento, sono state numerose le previsioni di reato che la giurisprudenza ha riconosciuto applicabili ai comportamenti *de quo*. *In primis*, il reato di sostituzione di persona, previsto e punito dall'articolo 494 c.p.. Se l'attacco all'identità altrui è, poi, unito a un accesso abusivo a un sistema informatico o telematico, alla detenzione di codici d'accesso o all'invio di un *virus*, si aggiungono i reati previsti e puniti dal 615-*ter*, 615-*quater* e dal 615-*quinquies*. Occorrono poi, spesso, le due fattispecie della truffa "tradizionale" ex art. 640 e della frode informatica ex art. 640-*ter*. In diverse occasioni è stato contestato

anche l'articolo 648-*bis*, nel caso circolassero somme di denaro grazie a complici (*financial managers*), e il trattamento illecito dei dati personali come previsto dal d.lgs 196 del 2003 in tema di privacy.

5. La sostituzione di persona nella tutela dell'identità in rete

Nel testo di una sentenza del 2007[24] della Corte di Cassazione si propone un primo approccio alla regolamentazione dei comportamenti che possono costituire il furto di identità, analizzando la possibilità di estendere le ipotesi previste dall'articolo 494 del codice penale ("Sostituzione di persona") al mondo elettronico.

La Corte nota come integri il reato di sostituzione di persona anche la condotta di colui che crei e utilizzi un *account* di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete Internet nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese.

Nel caso di specie, a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale. Si noti l'attenzione centrale, nel caso *de quo*, all'interesse alla buona fede, che può essere sorpresa da inganni relativi alla vera essenza di una persona, alla sua identità o ai suoi attributi sociali.

Il delitto, secondo la Corte, si consuma nel momento in cui taluno è stato indotto in errore con i mezzi indicati dalla legge e non occorre che il vantaggio perseguito dall'agente sia effettivamente raggiunto.

Diverso, secondo i giudici di legittimità, è se si è in presenza di anonimato, quando l'agente non solo utilizza un nome di fantasia non direttamente riconducibile a un soggetto realmente esistente ma, al tempo stesso, non persegue quel fine di procurarsi un vantaggio o di arrecare un danno ad altri, elemento psicologico che ne costituisce il dolo specifico. Nel caso giunto all'attenzione dei giudici l'*account* era stato creato a nome della donna per poi allacciare rapporti con gli utenti della rete inducendoli in errore. Il soggetto indotto in errore, in questo caso, non è chiaramente il fornitore del servizio di posta elettronica, ma sono gli utenti della rete Internet.

6. La tutela dell'identità nel social network Facebook

Il *social network Facebook* si è rivelato, negli ultimi anni, ambiente ideale per la manifestazione di nuovi comportamenti, da parte degli utenti, ascrivibili al *genus* dello stalking, del furto d'identità e non solo. Già si è visto poco sopra come la Suprema Corte abbia notato[25], ad esempio, come il reiterato invio alla persona offesa di SMS e di messaggi (di posta elettronica o tramite il *social network Facebook*) nonché la divulgazione attraverso simili mezzi di filmati ritraenti rapporti sessuali intrattenuti dall'autore del reato con la vittima, possano integrare l'elemento materiale del delitto di atti persecutori *ex* art. 612-*bis*.

Con riferimento, più specificamente, al furto d'identità, in questo ambiente telematico molto frequentato si sono manifestati comportamenti, anche criminosi, sempre più diffusi. Tipica è la sostituzione nello *status* (o profilo) di un altro soggetto, o la creazione di profili fittizi per tenere comportamenti criminosi.

Questo aspetto merita, anche in un'ottica informatico-giuridica, un maggior approfondimento. L'ambiente telematico *Facebook* non prevede barriere d'ingresso particolarmente rigide né effettua controlli (se non occasionalmente e a campione, o su segnalazione da parte di altri utenti) circa la veridicità di una identità o di un profilo. Ciò comporta che sia egualmente semplice utilizzare il *social network* in maniera "legittima" o, comunque, rispettando i termini di contratto del servizio o, al contrario, creare un profilo fittizio o, persino, creare un profilo riferibile a una terza persona, celebre o meno. Risiede quindi nella buona volontà (e intenzioni) dell'utente la decisione se abusare o meno del servizio. Frequente è, quindi, l'interazione da parte di alcuni soggetti con altri del *social network* utilizzando una finta identità, al fine, ad esempio, di carpire informazioni o di ottenere un contatto ("amicizia") che altrimenti, utilizzando la vera identità, non avrebbero ottenuto.

Un secondo fattore del *social network* utilizzato per fini criminosi è la sua pubblicità e la possibilità di rendere un'informazione visibile a tutta la cerchia di relazioni ("amici") correlata al soggetto preso di mira. Un individuo che volesse rendere un'informazione "delicata" pubblica, potrebbe semplicemente pubblicarla sul profilo di un altro soggetto o riferirla al soggetto medesimo affinché tutta la cerchia di amici, a volte migliaia di soggetti, la possa consultare. Appare quindi evidente il potenziale lesivo di comportamenti tenuti in un simile ambiente, un ambiente che ha fatto proprio della connessione tra individui il fattore del suo successo.

Il possibile furto d'identità su *Facebook* (o, meglio, un non provato furto d'identità sul *social network*) ha connotato una recente sentenza del Tribunale di Monza[26]: secondo il giudice di merito, è tenuto al risarcimento a titolo di danno morale il soggetto che leda diritti e valori costituzionalmente garantiti (quali la reputazione, l'onore o il decoro altrui) mediante l'invio di messaggi offensivi condivisi sul *social network Facebook* e portando un non corretto uso del mezzo stesso.

Nel caso *de quo* non era avvenuto un furto d'identità ma, accanto al carattere pubblico delle offese arrecate, proprio l'assenza di una denuncia formale da parte del convenuto di aver subito un furto di identità (e, quindi, di non essere l'autore materiale di tali messaggi) ha garantito la provenienza del messaggio. Il problema della riconducibilità del messaggio all'agente si è rivelato centrale e ha ripreso un tema tipico delle problematiche giuridiche delle nuove tecnologie, ossia il possibile "errore" nel ricondurre un agire informatico a un soggetto in un contesto, quello telematico, dove la facilità nel sostituire (apparentemente) un'altra persona in un'azione è estrema.

24 Cfr. Cassazione penale sez.V 8.11.2007, n. 46674.

25 Si noti, *inter alia*, Cassazione penale sez. VI, 16.7.2010 n. 32404.

26 Cfr. Tribunale di Monza, Sez. IV civile, 2.3. 2010, n. 770.

7. Alcuni aspetti tecnici

L'attività di stalking operata su reti telematiche, o comunque con l'utilizzo delle tecnologie più moderne, porta con sé problemi prettamente tecnologici e investigativi di particolare interesse. Non è questa la sede per un approfondimento dettagliato, ma alcuni cenni possono completare un quadro così fluido.

Come si è detto, *pedinamento* e *uso del telefono* sono stati, negli ultimi decenni, i due mezzi tipici, con relativi "pregi" e difetti, utilizzati dallo stalker nelle sue azioni. Il difetto principale era senza dubbio la facilità di individuazione del soggetto; il "pregio" era che la presenza fisica si mostrava particolarmente idonea a incutere paura e a generare uno stato di ansia o di timore; il telefono fisso, d'altro canto, costringeva, soprattutto se utilizzato in orario notturno, a un cambio di numero con relativi disagi esistenziali. Altri metodi, quali l'invio di lettere o di fiori al domicilio, scritte sui muri e altro erano egualmente idonei a generare quantomeno imbarazzo.

Prendendo come riferimento tali comportamenti "classici", può essere interessante cercare di individuare, seppur a grandi linee, quel processo di migrazione che ha visto manifestarsi tecniche tradizionali dello stalking nel mondo digitale.

Il pedinamento, oggi, avviene su Internet, nei *forum* frequentati dalla vittima e su *Facebook*; l'invio di lettere o di fotografie al soggetto è stato da tempo sostituito dall'invio di e-mail; l'SMS, il servizio più utilizzato nel settore della telefonia mobile, è diventato strumento tipico di molestia anche ossessiva; la lettera diffamatoria che una volta era inviata sul posto di lavoro o al nuovo compagno della vittima è stata ora sostituita da fotografie digitali, Cd-Rom o video resi pubblici o inviati alla cerchia di amici o al nuovo partner. Il pedinamento tradizionale viene ora svolto anche grazie alle nuove tecnologie e ai GPS, seguendo i percorsi del soggetto preso di mira e confidando spesso anche nella poca conoscenza delle tecnologie che la vittima ha. Il controllo della posta elettronica, infine, può oggi avvenire a totale insaputa del soggetto, senza dover accedere alla posta fisica come in passato, violare la cassetta della posta o intercettare la consegna del postino.

In questo quadro sensibilmente mutato, lo studioso di informatica giuridica ha da tempo rilevato alcuni aspetti interessanti che sono strettamente attinenti all'attività di stalking.

In primis, si pensi all'intensivo utilizzo di SMS e MMS al fine di molestare o tenere sotto pressione la vittima, e la contestuale difficoltà nel mantenere l'anonimato durante simili azioni e in un contesto tecnologico di telefonia mobile.

Altrettanto complesso può essere l'utilizzo di posta elettronica non sollecitata che sia realmente anonimo (ad esempio con falsificazione o mascheramento degli *headers*) e che resista a una investigazione accurata, così come una sostituzione di persona e di indirizzo che possa realmente trarre in inganno gli investigatori.

Molto più efficace, si accennava all'inizio, può essere un processo di pedinamento virtuale tramite il monitoring del comportamento del soggetto e la cosiddetta *Open Source Intelligence* (OSINT). Come è facile comprendere, tale tecnica è maggiormente efficace quante tracce lasci realmente la vittima su reti pubbliche. A tal proposito, i motori di ricerca, i blog e i social network sono le tre "zone" principali della rete che possono alimentare sistemi simili di ricerca su fonti aperte.

Una menzione particolare merita *Twitter*, strumento di aggiornamento delle proprie attività che permette di essere letteralmente "seguiti" da altri utenti di *Twitter*, anche con identità non corrispondenti al vero o mascherate.

Di particolare interesse per l'interprete, poi, è l'annoso problema della ricerca dell'anonimato in rete. Si tratta di un tema di grande interesse per il *cyberstalking* in quanto la *identificabilità* è sempre stato il limite di attività svolte in presenza della vittima. Internet può consentire di operare con un buon grado di anonimato, ad esempio utilizzando software quali Tor.

Di grande rilevanza è, poi, il tema delle false accuse e della modifica (o lesione) della reputazione della vittima, anche questi tipici comportamenti "vendicativi" alla base dello stalking tradizionale. Questo tema è molto delicato a causa del potenziale diffusivo della rete e della facilità di diffusione delle comunicazioni su larga scala e in maniera molto rapida: la reputazione della vittima è uno dei *target* preferiti da parte degli stalker, e Internet consente un attacco rapido e su larga scala.

Il furto di identità è tema, si è visto, di grande interesse anche per gli studiosi del fenomeno dello stalking, soprattutto sotto due aspetti: i) come sistema per individuare lo stalker, e ii) come identità intesa come un bene della vittima e, quindi, il furto di identità della vittima visto come un mezzo per danneggiarla ulteriormente.

Infine, una sempre maggiore attenzione, anche da parte dell'utente comune, è rivolta alle cosiddette tecniche di *anti-forensics*. Per anti-forensics s'intende un'attività che è pensata appositamente per cercare di *ingannare* un eventuale investigatore che, un domani, potrà mettersi sulle tracce dello stalker (ad esempio: subito dopo la querela della vittima).

Le attività di anti-forensics possono prendere le forme più varie: da un uso di strumenti di anonimato all'offuscamento o furto di indirizzo IP, dalla cifratura dei dati a attacchi portati da Paesi esteri, sino alla sostituzione dell'identità di una persona per sviare le indagini.

8. Considerazioni conclusive

Il presente studio conduce ad alcune riflessioni conclusive che, a parere di chi scrive, rivestono particolare interesse.

La prima considerazione è che l'ampio "arco" descrittivo elaborato in diversi ordinamenti, sovente anche all'interno di uno stesso sistema giuridico, e che spazia da una previsione normativa *dettagliata* del *cyberstalking* sino a una assoluta "non menzione" dello stesso, solleva il problema di tecnica legislativa se sia giusto o meno *specificare*, per fini di maggiore consapevolezza, di diffusione di conoscenza o di maggiore efficacia della norma, *tutte* le possibili modalità d'azione dello stalker telematico.

Il rischio, come si è già detto, è di non riuscire poi, in un secondo tempo, a fronteggiare l'evoluzione tecnologica che sta facendo migrare intere aree del diritto, e intere categorie di comportamenti, sempre di più verso il mondo elettronico (Ziccardi, 2011a). A tal proposito, non sembra peregrino ribadire che, a breve, tutto lo stalking sarà *cyber* e che lo stalking "tipico", ben presto, sarà quello elettronico e non più quello portato con mezzi "fisici" o analogici (Parodi, 2009; Zanasi, 2006; Sorgato, 2010; Sarno, 2012).

Il secondo punto, derivato dall'analisi informatico-giuridica, è se si possa evidenziare o meno un *aumentato pericolo per la vittima* grazie all'uso degli strumenti elettronici, se vi sia una maggiore o minore *rintracciabilità* del soggetto (di qui l'importanza dell'anonimato) e, infine, se il mezzo elettronico possa garantire una maggiore "potenza di fuoco" in un'attività, quella dello stalker, che, come è noto, può assumere spesso connotazioni ossessivo-compulsive (Ziccardi, 2011b).

Tre sono, a nostro avviso, gli aspetti su cui riflettere:

a) circa la "maggior potenza di fuoco", è indubbio che i sistemi attuali di messaggistica consentano un'attività di molestie estremamente potente sia con riferimento all'*one-to-one* (ossia all'attacco diretto alla vittima, o a un conoscente della vittima) sia per quanto riguarda la capacità diffusiva di immagini, video o messaggi nocivi. In alcuni casi si potrebbe addirittura arrivare a parlare di *automatizzazione* degli attacchi (lo stalker si limita ad avviare il processo e l'attività di invio messaggi – o altri tipi di molestia – procede senza bisogno della sua presenza fisica o di un'attività di verifica costante);
b) saremmo invece più cauti nell'affermare che sarebbe molto più facile, grazie alle tecnologie, operare da stalker *anonimi*. Il percorso verso l'anonimato è estremamente complesso, e necessita dell'utilizzo di tecniche specifiche che sono, spesso, ben lontane dalle competenze in capo allo stalker tipico. La tecnologia può dare un senso di invincibilità dietro a uno schermo, un'illusione di anonimato immediato, ma un'analisi investigativa su file di log, tabulati, indirizzi IP e altre informazioni porta spesso a superare il velo superficiale di segretezza (Lupària & Ziccardi, 2007) creato dall'agente;
c) saremmo anche cauti, in conclusione, nell'affermare che, data la diffusione delle tecnologie nella nostra società e vista la loro potenza, possa essere utile che il Legislatore *specifichi* sempre di più gli aspetti tecnologici dello stalking, sino ad arrivare a un vero e proprio livello di dettaglio.

Ciò per i due motivi già anticipati:

i) un rischio inutile di *demonizzazione* delle tecnologie che, certo, sono usate anche dagli stalker ma rivestono un ruolo molto più importante nella società per il loro utilizzo lecito, e
ii) il rischio di redigere una normativa già *obsoleta*, vista l'impossibilità di cristallizzare in un dato momento (anche normativo) una tecnologia che si sta evolvendo in maniera così rapida.

Vi è poi da rilevare, ultimo ma non ultimo, un grave problema di politica legislativa tipico dell'ordinamento giuridico italiano (ma non solo). Sin dalla normativa informatico-giuridica degli anni 1992 e 1993, quando furono emanate le prime disposizioni che, nel nostro Paese, si apprestavano a regolamentare l'informatica nei due delicati ambiti della duplicazione abusiva dei programmi per elaboratore (c.d. "pirateria del software") (Ristuccia & Zencovich, 1993) e della criminalità informatica (c.d. *computer crimes*) (Picotti, 1992, 2000; Galdieri, 1997; Pica, 1999) l'approccio del nostro Legislatore è sempre stato, in questi ultimi vent'anni, molto timoroso e, in alcuni casi, di aperta paura nei confronti della tecnologia, con la conseguenza della previsione di sanzioni molto pesanti, di frequenti derive liberticide e di ipotesi di responsabilità oggettiva per chi si trova a trattare dati con strumenti elettronici (si pensi, a tal proposito, alla vigente normativa in tema di protezione dei dati personali e alle ipotesi di responsabilità ex art. 2050 del codice civile).

Ciò ha sempre impedito nel nostro Paese una valutazione lucida delle modalità migliori per regolare la tecnologia; in una materia delicata come lo stalking, che tocca la persona nei suoi aspetti, diritti e sentimenti più delicati, un approccio di questo tipo potrebbe mostrare gli stessi difetti già evidenziati in altri settori, con conseguenze, però, ben peggiori dati i valori in gioco.

Bibliografia

Agnino, F. (2011b). Il delitto di atti persecutori e lo stato dell'arte giurisprudenziale e dottrinale. *Giurisprudenza di Merito*, 2, 584.

Agnino, F. (2011a). Delitto di atti persecutori e ricerca per tipo d'autore dello stalker. *Giurisprudenza di Meri*to, 9, 2237.

Bastianello, A. (2012). Il reato di stalking ex art. 612-bis C.p. *Giurisprudenza di Merito*, 3, 673.

Bean, H., & Hart, G. (2011). *No More Secrets: Open Source Information and the Reshaping of U.S. Intelligence*. Greenwood: Praeger.

Benedetto, G., Zampi, M., Ricci Messori, M., & Cingolani, M. (2008). Stalking: aspetti giuridici e medico legali. *Rivista Italiana di Medicina Legale*, 1, 127.

Burdon, M. (2010). Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws. *University of Illinois Journal of Law, Technology and Policy*, 1, 1.

Cajani, F., Costabile, G., & Mazzaraco, G. (2008). *Phishing e furto d'identità digitale*. Milano: Giuffrè.

Cajani, F. (2007). Profili penali del phishing. *Cassazione Penale*, 6, 2294.

Di Ronzo, A. (2009). Uso non autorizzato di carte di credito e concorso di reati nel phishing. *Rivista di Diritto dell'Informazione e dell'Informatica*, 1, 83.

Ferola, L. (2009). Il riciclaggio da phishing: tra vecchie e nuove questioni interpretative. *Giurisprudenza di Merito*, 11, 2831.

Finocchiaro, G. (2008). *Diritto all'anonimato: Anonimato, nome e identità personale*. Padova: CEDAM.

Flick, C. (2008). Falsa identità su Internet e tutela penale della fede pubblica degli utenti e della persona. *Rivista di Diritto dell'Informazione e dell'Informatica*, 4-5, 526.

Flor, R. (2007). Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente. *Rivista Italiana di Diritto e Procedura Penale*, 2-3, 899.

Galdieri, P. (1997). *Teoria e pratica nell'interpretazione del reato informatico*. Milano: Giuffrè.

Galuppi, G., & Macario, E. (2010). Lo stalking. *Diritto di Famiglia*, 2, 865.

Lo Monte, E. (2011). L'individuazione delle "condotte reiterate" (art. 612-bis c.p.) tra lacune legislative e discutibili applicazioni giurisprudenziali. *Cassazione Penale*, 1, 158.

Lupària, L., & Ziccardi, G. (2007). *Investigazione penale e tecnologia informatica: Progresso scientifico e garanzie fondamentali*. Giuffrè: Milano.

Macrì, M. (2009). Stalking e prospettive di tutela cautelare, nota a Tribunale Napoli, 30/06/2009, sez IV. *Responsabilità Civile e Previdenziale*, 11, 2323.

Maffeo, V. (2009). Il nuovo delitto di atti persecutori (stalking): un primo commento al D.L. n. 11 del 2009 (conv con modif. dalla L. n. 38 del 1009). *Cassazione Penale,* 7-8, 2719.

Maggipinto, A., & Iaselli, M. (2005). *Sicurezza e anonimato in rete: Profili giuridici e tecnologici della navigazione anonima*. Milano: Nyberg.

Mengoni, E. (2012). Interferenze illecite nella vita privata: il reato

sussiste anche se il soggetto ritratto non può essere identificato. *Cassazione Penale*, 2, 523.
Merzagora, I., Bana, A., Chinnici, N., & de' Micheli, A. (2011). L'avvocato come vittima di stalking. *Rivista Italiana di Medicina Legale*, 4-5, 979.
Minnella, C. (2011). Restano incerti i confini della punibilità del delitto di atti persecutori. *Cassazione Penale*, 3, 968.
Morano Cinque, E. (2010). Stalking: una ricostruzione del fenomeno alla luce delle categorie civilistiche. *Responsabilità Civile e Previdenziale,* 12, 2517.
Morano Cinque, E. (2011). L'abuso del processo come forma di stalking giudiziario: è lite temeraria. *Responsabilità Civile e Previdenziale*, 12, 2580.
Natalini, A. (2010). Quando le molestie persecutorie usano le più recenti tecnologie è "cyberstalking". E si configura il delitto di cui all'art. 612-bis Cp. *Diritto e Giustizia*, 0, 407.
Nezhad, A.A., Miri, A., & Makrakis, D. (2008). Location privacy and anonymity preserving routing for wireless sensor networks. *Computer Networks*, 52, 3433–3452.
Olcott, A. (2012). *Open Source Intelligence in a Networked World*. London-New York: Continuum.
Parodi, C. (2009). *Stalking e tutela penale*. Milano: Giuffrè.
Pathé, M., & Mullen, P.E. (1997). The impact of stalkers on their victims. *British Journal of Psychiatry*, 170, 12.
Perri, P. (2008). Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo a un sistema informatico o telematico con l'aggravante dell'abuso della qualità di operatore del sistema. *Giurisprudenza di Merito*, 6, 1651.
Perri, P. (2008). Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia. *Diritto dell'Internet*, 261.
Pica, G. (1999). *Diritto penale delle tecnologie informatiche: Computer's crimes e reati telematici*. Torino: UTET.
Picotti, L. (2000). Reati informatici. *Enciclopedia giuridica*, 1-33.
Picotti, L. (1992). *Studi di diritto penale dell'informatica*. Verona: s.n.
Pulvirenti, A. (2011). Note problematiche su alcuni profili procedimentali del delitto di "atti persecutori" (stalking). *Diritto di Famiglia*, 2, 939.
Resta, F. (2009). Il delitto di stalking verso un nuovo habeas corpus per la donna? *Giurisprudenza di Merito*, 7-8, 1924.
Ristuccia, R., & Zeno Zencovich, V. (1993). *Il software nella dottrina, nella giurisprudenza e nel DL 518/1992: Con 65 decisioni di giudici italiani*. Padova: CEDAM.
Sarno, F. (2012). *Il nuovo reato di atti persecutori (612-bis)*. Milano: Giuffrè.
Sorgato, A. (2010). *Stalking*. Torino: Giappichelli.
Tekir, S. (2009). *Open Source Intelligence Analysis: A Methodological Approach*. Saarbrücken: VDM Verlag.
Valsecchi, A. (2009). Il delitto di "atti persecutori" (il CD. stalking). *Rivista Italiana di Diritto e Procedura Penale*, 3, 1377.
Zanasi, F. (2006). *Violenza in famiglia e stalking*. Milano: Giuffrè.
Ziccardi, G. (2011a). *Hacker – Il richiamo della libertà*. Venezia: Marsilio.
Ziccardi, G. (2011b). *Informatica Giuridica, Tomo I e II*. Milano: Giuffrè.
Ziccardi, G. (2011c). Voce "Furto d'identità". *Digesto delle Discipline Penalistiche*. Torino: UTET.