DEVITA.LAW©

CYBERSTALKING

LA PERSECUZIONE DIGITALE E LE VITTIME SENZA RETE

Prof. Avv. Roberto De Vita
Avv. Valentina Guerrisi

ABSTRACT

L'uso crescente della tecnologia, anche in ragione dell'accelerazione dettata dalla pandemia e dalle misure di contenimento della diffusione del virus, ha determinato lo spostamento di tutte le relazioni nel mondo digitale, costituendo uno stabile ecosistema di vite digitali dalle quali ognuno di noi non può più prescindere. Questo consolidamento, tuttavia, ha dato maggiore spazio (e conseguente rilevanza) a nuove ed insidiose patologie che non trovano ancora tutele adeguate nel nostro ordinamento penale.

Tra queste, lo stalking digitale - inteso in una accezione molto più ampia del tradizionale concetto di "stalking" e comprendente al suo interno tutti i comportamenti persecutori perpetrati attraverso la rete, a prescindere dalla sussistenza di un rapporto di conoscenza tra l'autore e la vittima - assume un rilievo decisivo in ragione delle serie conseguenze che determina.

Haters, trolls, troll bots e veri e propri stalkers digitali sono solo alcune delle figure paradigmatiche del nuovo macro-fenomeno: nonostante l'impatto con tali soggetti e modi di agire sia pressochè quotidiano, non esiste ancora un rimedio in grado di arginarne le conseguenze e tutelare in maniera efficace la vittima. In un mondo in cui l'accesso ad internet viene considerato sempre più come diritto umano fondamentale per il benessere economico dell'individuo, è ormai imprescindibile la necessità di garantire che questo spazio sia sicuro e diventi luogo di emancipazione e sviluppo per tutti.

Leggi l'articolo anche su devita.law, l'house organ dello Studio Legale De Vita[1]

---

[1]*Devita.law (o devitalaw) è l'house organ dello Studio Legale De Vita del Prof. Avv. Roberto De Vita, sul quale vengono pubblicati contenuti di aggiornamento e approfondimento.*

Foto Raniero Botti ©2013

L'accelerazione continua dello spostamento in rete della quotidianità, dopo le prime luci (rappresentate, soprattutto dall'inizio della pandemia, dai vantaggi per il progresso tecnologico, per la crescita di scambi e comunicazioni e per la continuità delle attività), ha mostrato con sempre maggiore evidenza le proprie ombre.

Gli utenti si sono trovati ad interagire stabilmente - e sempre più in via esclusiva - in un ecosistema complesso, permeato da rischi ed insidie (più o meno evidenti), così come da veri e propri fenomeni criminali, che negli ultimi anni hanno iniziato, anche in Italia, ad essere conosciuti e studiati, fino ad entrare nel lessico quotidiano di giornalisti ed accademici. La contingenza pandemica ed il lockdown nell'emergenza hanno lasciato spazio alla stabilità del distanziamento ed alla quotidianità connessa: di conseguenza, le vittime sono cresciute in misura ancora più allarmante. Ciononostante, legislazione e giurisprudenza si sono adeguate con fatica alle nuove frontiere criminali; in particolare, la visione degli interpreti è rimasta talvolta ancorata a categorie esegetiche che discendono da una cultura analogica, ormai inadeguata per garantire comprensione ed effettiva tutela nella società digitale. Infatti, destano sempre maggiore allarme il numero delle vittime dello stalking digitale, la Non Consensual Pornography [1] o il doxing [2], per citare alcuni dei fenomeni noti e definiti negli Stati Uniti come TFA (Technology-Facilitated Abuse - abusi facilitati dalla tecnologia).

Secondo un recente report americano [3], i TFA sono in costante aumento e il numero di adulti americani che ha vissuto almeno una esperienza di "molestie on line" (con inclusione dei fenomeni di stalking, minacce fisiche, molestie sessuali e maltrattamenti) si colloca tra il 18 ed il 37% [4]. Tra gli utenti dei social media, 1 su 12 è stato vittima di NCP [5], circa il 7% degli adulti americani ha subìto la condivisione di proprie immagini sessuali esplicite senza il proprio consenso [6] e ben il 5% dei ragazzi americani tra i 10 e i 18 anni è stato vittima di sextortion [7].

Molteplici sono gli strumenti attraverso i quali vengono perpetrati i TFA: dai social media alle piattaforme di gaming on line, ai siti di condivisione di immagini e video e le app di messaggistica istantanea. In tutti i casi, la costante presenza in rete e l'uso massivo di tecnologia da parte dei giovani fa sì che questi risultino un facile obiettivo per gli abusanti: la fascia più colpita rimane, infatti, quella dei bambini/ragazzi fino ai 18 anni (maggiormente rispetto ai fenomeni di sextortion e cyberstalking) [8], ma il 45% delle vittime si registra anche nella fascia 18-29 anni [9].

IL CYBERSTALKING E LE "CREEPWARE APPS"

Tra i fenomeni analizzati, il cyberstalking assume un rilievo determinante in ragione delle serie conseguenze che determina, le quali, molto spesso, non si limitano alla sfera prettamente digitale dell'individuo ma diventano un vero e proprio precursore di condotte abusanti fisiche e dirette sulla vittima.

In generale, il cyberstalking viene inteso quale stalking (ovvero una condotta molesta, reiterata e persecutoria) perpetrato attraverso la rete o gli strumenti digitali. Tuttavia, esistono molteplici accezioni, più o meno ampie, dello stesso fenomeno.

La National Conference of State Legislature americana (NCSL) ad esempio, nel classificare i tre comportamenti on line (cyberstalking, cyberharassment e cyberbullying) disciplinati e sanzionati dai legislatori dei singoli Stati, distingue il cyberstalking dal cyberharassment (laddove quest'ultimo si limita alle condotte persecutorie on line che non si trasformano in minacce concrete di danno alla vittima), ritenendo il primo come il più grave e pericoloso tra i tre "*Internet harassment*" [10]. Tuttavia tale distinzione rischia di trascurare e minimizzare le pur gravi ripercussioni che una condotta persecutoria perpetrata on line può avere (ed ha) sulla vita della vittima; e ciò massimamente in un contesto di relazioni caratterizzato (quasi scandito) dall'uso della tecnologia, all'interno del quale l'identità digitale di una persona – e quindi la sua sfera di protezione - assume una rilevanza addirittura superiore a quella fisica in senso strettamente inteso: difatti, la mancata traduzione dell'agire in una condotta offensiva in senso "analogico" non comporta, di per ciò solo, la sua minore pericolosità.

Di maggior respiro risulta la definizione fornita dall'Office on Drugs and Crime delle Nazioni Unite (UNODC), secondo il quale il cyberstalking consiste nell'uso di "*information and communications technology (ICT) to perpetrate more than one incident intended to repeatedly harass, annoy, attack, threaten, frighten, and/or verbally abuse individuals*" [11]. Esso, pertanto, include comportamenti quali mandare e-mail, messaggi istantanei, chiamate e ogni altra forma di comunicazione elettronica per inviare messaggi osceni, violenti, diffamatori o minacciosi alla vittima o anche alla sua famiglia, gli amici o i colleghi di lavoro. A tali condotte si aggiungono anche il monitoraggio costante attraverso la tecnologia (es. attraverso l'installazione di app di tracciamento del segnale GPS sui devices della vittima, la sua vettura o perfino all'interno dei giocattoli dei bambini o degli animali domestici), fino ai veri e propri attacchi informatici per rubare i dati e le informazioni, diffondere on line materiale privato, creare falsi account per distruggere la reputazione della vittima o semplicemente danneggiare i suoi sistemi di comunicazione per impedire ogni interazione con il mondo esterno.

Uno dei modelli di azione più studiati negli ultimi tempi consiste nell'abuso dei sistemi di monitoraggio – perfettamente legali e disponibili sul mercato – che, nell'impiego distorto che ne viene consentito, si tramutano in vere e proprie "app spia", anche definite di recente come "*creepware apps*" [12].

Una importante ricerca [13] condotta per la prima volta sulle applicazioni disponibili nei comuni *digital stores* ha evidenziato come più di 200 di queste offrissero servizi utili per il potenziale stalker, dal comune tracciamento della posizione alle funzioni di registrazione/duplicazione nascosta di messaggi, e-mail e video. Si trattava, nella maggior parte dei casi, di software creati per finalità legittime (come il tracciamento dei figli minori o degli animali domestici), di c.d. utility per rintracciare il proprio *device* e altri oggetti personali smarriti, oppure per "individuare" amici che si trovano nelle immediate vicinanze. Altre, invece, avevano quale specifica finalità il monitoraggio costante del soggetto utilizzatore che, in alcuni casi, non si accorgeva neppure della loro presenza sul dispositivo.

Il profilo più problematico emerso riguardava soprattutto le applicazioni del primo tipo, anche dette "dual use", poiché queste venivano installate per finalità legittime e con il consenso della vittima, la quale, però, ne ignorava il reale utilizzo da parte dell'abusante. Peraltro, l'analisi sui maggiori antivirus e antispyware disponibili sul mercato aveva evidenziato come gli stessi non fossero in grado di identificare le *dual use apps* quali minacce per l'utente che le aveva installate [14].

Lo studio dell'universo dei c.d. "stalkerware" - ovvero spyware [15] per finalità di stalking - evidenziava inoltre l'ingente mole di video e tutorial disponibili in rete (molte volte creati e diffusi dagli stessi produttori e sviluppatori dei software) per spiegare le effettive potenzialità delle app, nonché l'incoraggiamento al loro utilizzo mediante creazione di blog specifici, servizi mirati di "customer care" o messaggi pubblicitari espliciti ("*How to read deleted texts on your lover's phone*" [16] o "*Mobile Spy App for Personal Catch Cheating Spouses*" [17]).

Sulla scorta di questa prima analisi, un ulteriore studio del 2020 [18] ha messo a punto un algoritmo per analizzare le *creepware apps* (CreepRank), identificandone molte usate esclusivamente per finalità persecutorie, sostituzioni di persona, frodi e furti di dati o tracciamento occulto.

L'attenzione mediatica destata dai risultati ottenuti - unitamente al proliferare di casi giudiziari in cui l'autore del reato si era servito di software di questo tipo [19] per perseguitare, violentare o uccidere - hanno indotto le principali Big Tech companies del settore a rimuovere centinaia di app dai loro store, così come i relativi video tutorial, introducendo policy più stringenti per i

Foto Raniero Botti ©2013

produttori e gli sviluppatori. Ciononostante, esse continuano ad essere largamente diffuse e di facile utilizzo per chiunque.

CYBERSTALKING E CYBERHARASSMENT

Il cyberstalking, tuttavia, non deve ritenersi limitato a quella che viene definita come IPV (Intimate Partner Violence) [20], ma impone di essere considerato in una accezione ben più ampia, tale da comprendere al suo interno tutti i comportamenti persecutori perpetrati attraverso la rete, a prescindere dalla sussistenza di un rapporto di conoscenza o di un legame tra l'autore e la vittima. In questi termini, assumono assoluta rilevanza tutti quei fenomeni di c.d. *cyberharassment* che – nella definizione coniata dalle Nazioni Unite – contemplano l'uso della tecnologia "*to intentionally humiliate, annoy, attack, threaten, alarm, offend and/or verbally abuse individuals*" [21] a prescindere da una relazione intima.

In tal senso, paradigma significativo è rappresentato degli "haters", che popolano i social network perseguitando le loro vittime in maniera mirata ed ininterrotta e dietro i quali, molto spesso, si celano veri e propri sistemi organizzati di attacco per le più disparate finalità ("*Cyberharassment may also involve targeted harassment, where one or more persons work together to repeatedly harass their target online over a finite period of time (often a brief period of time) to cause distress, humiliation, and/or to silence the target*") [22].

Si tratta, dunque, di veri e propri "stalker digitali" che utilizzano la rete ed i suoi strumenti per molestare la vittima violando la sua identità digitale, la sfera delle sue relazioni affettive e lavorative e – in una parola – la sua "vita digitale".

Tecnicamente, si parla di "*internet trolls*" per individuare soggetti che postano commenti offensivi non solo per umiliare o provocare risentimento ma anche per generare una discussione violenta che coinvolga più utenti e prenda di mira uno specifico bersaglio. Agli esordi della popolarità dei social network, queste figure della mitologia nordica venivano associate a persone fisiche realmente esistenti che, celandosi dietro l'anonimato di un *nickname*, si accanivano nei confronti di personaggi noti e non per esprimere il loro risentimento [23]. Il fenomeno ha avuto una diffusione tale da diventare oggetto di studio da parte di psichiatri e analisti comportamentali [24] i quali hanno individuato alla base di queste condotte sentimenti di rabbia e frustrazione, il più delle volte derivanti da situazioni personali particolarmente traumatiche (un licenziamento o un divorzio), ma anche vere e proprie psicopatologie (narcisismo, sadismo, disturbi della personalità) [25].

Tuttavia, oggi è più corretto parlare di "*troll bots*", frutto dell'interazione tra umano e algoritmi/AI per organizzare veri e propri sistemi automatizzati di account che postano contenuti offensivi, denigratori o volutamente falsi.

Troll e *troll bots* rappresentano un tipico esempio di stalking digitale (che gli studiosi americani identificano più propriamente nel "*cyberharassment*") che prescinde

completamente dal rapporto di conoscenza tra vittima e carnefice, trovando la sua ragion d'essere nelle più disparate finalità: dalla volontà di denigrare e distruggere la reputazione di una persona (perché famosa o appartenente ad una organizzazione o società), a quella di diffondere false informazioni per motivazioni economiche, sociali e soprattutto politiche.

Gli autori possono arrivare ad hackerare l'account della vittima per rubare le informazioni personali, le immagini e i video e poi pubblicarli, oppure diffondere informazioni false o voci su un individuo per danneggiarne la posizione sociale, le relazioni interpersonali e la sua reputazione. Gli stalker digitali possono anche impersonare le vittime creando account con nomi uguali o simili e, mediante le immagini reperite on line, utilizzarli per inviare richieste di amicizia e/o following a parenti ed amici (con vere e proprie sostituzioni di persona): in tal modo, l'accettazione di tali richieste garantisce ai responsabili l'accesso agli account degli amici e delle famiglie delle vittime e, per estensione, l'accesso agli account reali delle vittime.

Scorrendo le cronache, i casi di stalking digitale come fin qui inteso sono purtroppo all'ordine del giorno e vedono coinvolti non solo personaggi dello spettacolo o del c.d. star system [26], ma anche politici [27], sportivi, imprenditori o – perfino – persone comuni balzate agli "onori della cronaca" a causa di un video o un commento divenuto virale [28], ovvero per essere state coinvolte in manifestazioni pubbliche come, ad esempio, una campagna vaccinale in tempo di pandemia [29].

LA RISPOSTA DEGLI ORDINAMENTI

Azioni di questo tipo possono colpire ognuno di noi, e forse già lo hanno fatto. Secondo un recente sondaggio, il 26% degli utenti dei social media americani nel 2017 è stato vittima di *trolling* e *cyberharassment* [30] e numeri simili si registrano anche nel vecchio continente [31] : secondo una ricerca del 2017 dell'Eurispes, il fenomeno del cyberstalking ha riguardato 8 persone su 10 (83,3% degli intervistati), colpendo soprattutto i giovani (91,2% nella fascia di età 25-34 anni e 87,5% in quella 18-24 anni) [32]. Tuttavia, nonostante la portata crescente del fenomeno, non esiste ancora una risposta unitaria ed efficace.

Lo stalking digitale – così come tutte le altre condotte di tipo criminale che si consumano sulla o attraverso la rete – assume il più delle volte rilievo internazionale, prescindendo da confini nazionali o da regolamentazioni di tipo "analogico" e tradizionale. Attualmente, però, non esistono trattati internazionali o sovranazionali che puniscano nello specifico condotte di tal genere, ma solo alcune disposizioni nazionali, nella maggior parte dei casi nate per disciplinare casi "analogici" e poi adattate per ricomprendere anche i nuovi fenomeni.

Negli USA, ad esempio, non c'è ancora una legge federale che sanzioni in maniera organica ed unitaria le condotte di stalking digitale, ma solo previsioni da parte dei singoli Stati, declinate a volte in maniera distinta per i fenomeni di *cyberstalking* e *cyberharassment*. California, Florida, Pennsylvania e molti Stati del Sud contemplano norme specifiche, ma lo stesso non accade in Nebraska o Kentucky dove esistono leggi mirate per il solo cyberbullismo [33]. Sono

aumentate, in ogni caso, le azioni volte a contrastare in maniera sistematica i TFA, anche e soprattutto attraverso la condivisione e l'analisi dei dati da parte delle forze di polizia e dagli operatori della giustizia e del diritto [34].

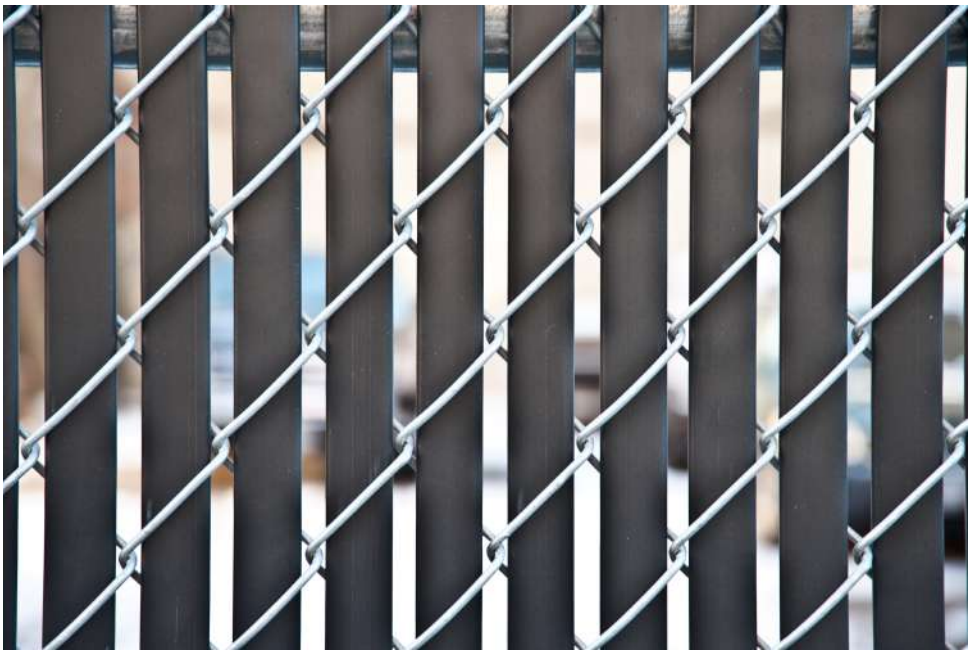
Stati come Singapore e Nigeria hanno previsioni specifiche per *cyberharassment* [35] e *cyberstalking* [36], mentre altre nazioni utilizzano le vigenti norme in materia di stalking c.d. "analogico", di minacce o molestie per disciplinare i nuovi fenomeni digitali. Nel Regno Unito le condotte di stalking digitale vengono perseguite ai sensi del *Protection from Harassment Act* del 1988, modificato nel 2012 con l'introduzione delle condotte perpetrate on line. In altri casi, in assenza di leggi specifiche, molti paesi utilizzano leggi nazionali che contemplano solo alcuni degli aspetti delle condotte di stalking digitale: il ricatto, l'estorsione, gli insulti, le minacce, l'incitamento al crimine, alla violenza e/o all'odio, le comunicazioni dannose, la violazione della privacy, la diffamazione, la sostituzione di persona, le frodi o i furti d'identità, l'hacking e altri reati correlati a crimini informatici.

In Italia, l'art. 612 bis del codice penale, introdotto nel 2009 e rubricato "atti persecutori", punisce chiunque "con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da 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". Il reato è aggravato, peraltro, se commesso con "strumenti informatici o telematici", tuttavia le maglie interpretative della norma rischiano di non ricomprendere tutti quei fenomeni che – come sopra ampiamente descritto – non ricadono all'interno delle patologie dei rapporti interpersonali tra vittima e carnefice ovvero non si traducono in condotte materiali analogicamente intese.

Emblematica, sul punto, appare una recentissima pronuncia della Corte di Cassazione la quale, in una vicenda relativa alla pubblicazione di numerosi post offensivi e denigratori sulla pagina pubblica (e perciò visibile a chiunque) di un noto social network, ha affermato che "la pubblicazione di post meramente canzonatori ed irridenti su una pagina Facebook accessibile a chiunque non integra la condotta degli atti persecutori di cui all'articolo 612 bis c.p., mancando il requisito della invasività inevitabile connessa all'invio di messaggi "privati" (mediante SMS, Whatsapp, e telefonate), e, se rientra nei limiti della legittima libertà di manifestazione del pensiero e del diritto di critica, è legittima" [37]. Secondo il Giudice di legittimità, infatti, la pubblicazione "visibile a tutti gli utenti del social network" non è da ritenersi indirizzata "direttamente" alle vittime, essendone la lettura "rimessa alla scelta individuale".

Appare evidente, dunque, il condizionamento delle lenti analogiche sull'interprete, il quale valuta la rete e gli strumenti digitali solo in quanto mezzi di perpetrazione di un reato comunque connesso ad un rapporto di prossimità tra l'autore e la vittima e dove la lesione è rilevante solo se riconducibile alla sfera personale fisicamente intesa. Analoghe posizioni vengono espresse nella maggior parte delle pronunce su questi temi, ove lo stalking "digitale" viene inteso solo quale diversa modalità di esecuzione materiale delle condotte persecutorie tradizionali, ferma restando la sussistenza dell'evento specifico richiesto dalla norma (lo stato di ansia, il timore per l'incolumità propria o altrui o l'alterazione delle abitudini di vita), comunque da provare [38]: in tali casi, il mezzo digitale rileva, al più, ai fini della gravità della condotta che "*sebbene non abbia comportato contatti diretti tra la persona offesa e l'imputato o atti intimidatori di quest'ultimo, ha comunque svilito la figura della persona offesa cagionandole un grave stato di ansia*" [39], ovvero quale mero antecedente temporale di una successiva "intrusione" fisica nella vita della vittima (l'abitazione privata o il luogo di lavoro) [40].

Foto Raniero Botti ©2013



I post offensivi di un hater, gli attacchi di un troll o lo stalker sconosciuto che monitora tutti i comportamenti ed azioni delle vittime in rete rischiano di rimanere privi di una tutela specifica e mirata (soprattutto in relazione al contenimento degli effetti negativi), e di ricadere nell'ambito di fattispecie (la minaccia, le molestie, la diffamazione o, nei casi più gravi, la sostituzione di persona), che, seppur simili, risultano generiche e mal si attagliano ai citati casi concreti. La principale conseguenza di questa empasse è rappresentata dalla scarsa deterrenza e dalla intempestività delle reazioni dell'ordinamento innanzi alla rapidità che caratterizza gli accadimenti nell'ecosistema digitale: sanzioni e rimedi tradizionali, collocandosi temporalmente molto al di là della consumazione delle condotte, non dispiegano alcuna efficacia rispetto ai gravissimi danni e alle conseguenze che la vittima subisce nell'immediato.

I recenti interventi legislativi (vedasi il c.d. Codice Rosso) e le molteplici iniziative di cooperazione tra organi istituzionali pubblici (di polizia e giudiziari) e soggetti privati (es.

social network e *private enforcement* in generale) sono sicuramente il segnale di una maggiore sensibilità sul tema, ma la strada da percorrere – soprattutto in termini di consapevolizzazione, prevenzione e tutela effettiva dagli specifici fenomeni – è ancora lunga.

Da ultimo, anche le istituzioni dell'Unione Europea hanno puntato un faro specifico sul fenomeno, evidenziando come la violenza virtuale sia da considerarsi vera e propria forma di violenza di genere, atteso che il più alto numero di vittime si riscontra nelle donne e nelle giovani ragazze. In un recente studio dell'Istituto Europeo per l'Uguaglianza di Genere (EIGE), è stata evidenziata la portata globale del fenomeno e le sue gravi ripercussioni [41]: se da un lato, infatti, l'accesso ad internet viene considerato sempre più come diritto umano fondamentale [42] per il benessere economico dell'individuo, è sempre più evidente la necessità di garantire che questo spazio sia sicuro e diventi luogo di emancipazione e sviluppo per tutti, comprese le donne e le ragazze [43]. Tuttavia, le ricerche hanno evidenziato che una donna su tre subirà una forma di violenza nella vita [44] e, tuttora, 1 donna su 10 ha già subìto una forma di violenza virtuale sin dall'età di 15 anni [45].

Purtroppo, allo stato, le vittime di queste gravi condotte sono prive di una tutela effettiva, in particolare nei casi in cui uno sconosciuto inizi a monitorarne la vita online, anche commentandola e denigrandola. Come dimostrano le indagini statistiche e gli studi, tale ultima categoria di condotte non costituisce un'ipotesi meramente teorica. Al contrario, il fenomeno è tristemente reale ed è diventato parte integrante della quotidianità contemporanea di una consistente quota della popolazione. Inoltre, colpendo direttamente l'espressione della personalità e dell'identità degli individui, i danni psicologici che possono essere arrecati alle vittime sono potenzialmente – e spesso effettivamente – gravissimi.

Foto Raniero Botti ©2016

In tal senso, è irrilevante che con troll, bot o haters occasionali spesso non vi sia un rapporto preesistente, né avvenga un contatto nel mondo "fisico". E la soluzione non può essere certo rintracciata nella disconnessione, che rappresenta una ingiusta e gravissima limitazione di libertà per la vittima. Pretendere di risolvere fenomeni complessi consigliando la "chiusura dei

profili" si traduce da un lato, nell'uso incauto di metodi analogici per affrontare problemi digitali, dall'altro restituisce vigore alla pratica del *victim blaming*, tipicamente associata ad ogni tipologia di violenza di genere (come si è visto, infatti, le vittime femminili sono statisticamente le più colpite da tutti i fenomeni di stalking digitale [46]) e che non deve introdursi nelle riflessioni delle autorità.

La rivoluzione digitale (con le sue patologie) ha travolto i comportamenti ma non ancora le consapevolezze e le categorie interpretative. Prima ancora, quindi, di una prospettiva *de iure condendo*, viene in evidenza un problema di carattere culturale, di resistenza rispetto all'evidenza di una realtà nuova non meramente accessoria rispetto a quella "fisica". La vita digitale delle persone prescinde ormai dalla fisicità della vita analogica, rendendosi autonoma nei momenti di espressione della identità e della personalità, e deve essere destinataria di una tutela diretta che solo una rivoluzione di pensiero può garantire.

Roberto De Vita

Valentina Guerrisi

RIFERIMENTI

[1] Cfr. "*Non Consensual Pornography: dal revenge porn alla sexual extortion*", Osservatorio Cybersecurity di Eurispes, R. De Vita, M. Della Bruna, Dicembre 2019.

[2] Con il termine "doxing" si intende far riferimento alla "diffusione pubblica di informazioni private e sensibili di una persona senza il suo consenso" - MacAllister, Julia M., "The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information" Fordham Law Review, Vol. 85, No. 5, 2017, pp. 2451–2483.

[3] "Countering Technology-Facilitated Abuse – Criminal Justice strategies for combating Non Consensual Pornography, Sextortion, Doxing and Swatting" – RAND 2020.

[4] Anti-Defamation League, "Online Hate and Harassment: The American Experience" webpage, 2019. As of November 8, 2019: https://www.adl.org/onlineharassment#survey-report , in "Countering Technology-Facilitated Abuse – Criminal Justice strategies for combating Non Consensual Pornography, Sextortion, Doxing and Swatting" – RAND 2020.

[5] Ruvalcaba, Yanet, and Asia A. Eaton, "Nonconsensual Pornography Among U.S. Adults: A Sexual Scripts Framework on Victimization, Perpetration, and Health Correlates for Women and Men" Psychology of Violence, Vol. 10, No. 1, 2020, pp. 68–78, in "Countering Technology-Facilitated Abuse – Criminal Justice strategies for combating Non Consensual Pornography, Sextortion, Doxing and Swatting" – RAND 2020.

[6] Duggan, Maeve, Online Harassment 2017, Washington, D.C.: Pew Research Center, July 11, 2017. As of November 8, 2019: https://w w w.pewinternet.org/2017/07/11/online-harassment-2017/ in "*Countering Technology-Facilitated*

Abuse – Criminal Justice strategies for combating Non Consensual Pornography, Sextortion, Doxing and Swatting" – RAND 2020.

[7] Patchin, Justin W., and Sameer Hinduja, "Sextortion Among Adolescents: Results from a National Survey of U.S. Youth" Sexual Abuse, Vol. 32, No. 1, 2020, pp. 30–54 in "Countering Technology-Facilitated Abuse – Criminal Justice strategies for combating Non Consensual Pornography, Sextortion, Doxing and Swatting" – RAND 2020.

[8] Lenhart, Amanda, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney, "Online Harassment, Digital Abuse, and Cyberstalking in America", New York: Data and Society Research Institute, 2016 in "Countering Technology-Facilitated Abuse – Criminal Justice strategies for combating Non Consensual Pornography, Sextortion, Doxing and Swatting" – RAND 2020.

[9] Anti-Defamation League, 2019 cit.

[10]https://www.csg.org/sslfiles/dockets/2012cycle/32B/32Bdocmins/Cyberstalking,%20Cyberharassment%20and%20Cyberbullying%20Laws.pdf

[11] UNODC, 2015 https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

[12]"*The Many Kinds of Creepware Used for Interpersonal Attacks*", K.A. Roundy, P. Barmaimom Mendelberg, N. Dell. D. McCoy, D. Nissani, T. Ristenpart, A. Tamersoy, - NortonLifeLock Research Group-NYU-CornellTech, May 2020.

[13] "*The Spyware Used in Intimate Partner Violence*", R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, T. Ristenpart – Cornell Tech, NYU, Cornell University, Hunter College - May 2018.

[14] "The Simple Way Apple and Google Let Domestic Abusers Stalk Victims", WIRED, A. Greenberg, 2019.02.07.

[15] C.d. "Software spia" che introdotti nei devices della vittima possono assumerne il controllo, inabilitarne alcune funzioni, o acquisire dati e informazioni personali da diffondere.

[16] "Hundreds of Apps Can Empower Stalkers to Track Their Victims", J. Valentino-DeVries, New York Times, May 19, 2018.

[17] "The Spyware Used in Intimate Partner Violence", cit.

[18] "*The Many Kinds of Creepware Used for Interpersonal Attacks*", K.A. Roundy, P. Barmaimom Mendelberg, N. Dell. D. McCoy, D. Nissani, T. Ristenpart, A. Tamersoy, - NortonLifeLock Research Group-NYU-CornellTech, May 2020.

[19] "Hundreds of Apps Can Empower Stalkers to Track Their Victims" cit.

[20] "The Spyware Used in Intimate Partner Violence", cit.

[21] UNODC, 2015, cit.

[22] UNODC, 2015, cit.

[23] É nota l'intervista della CNN a Michael Brutsch, uno dei più famosi "troll" americani (conosciuto come "violentacrez") poi smascherato - https://www.youtube.com/watch?v=s6plIjdaVGA

[24] E. March and J. Marrington. "*Cyberpsychology, Behavior, and Social Networking*". Mar 2019, pagg. 192-197 http://doi.org/10.1089/cyber.2018.0210

[25] "*Trolls just want to have fun*", Erin E. Buckels, Paul D. Trapnell, Delroy L. Paulhus, in "*The Dark Triad of Personality*", Vol. 67, pag. 1-122 (September 2014). Anche in: https://thewire.in/communalism/internet-trolls-psychology.

[26] https://www.firenzetoday.it/attualita/chiara-ferragni-critica-uffizi.html

[27] https://www.repubblica.it/politica/2017/08/14/news/boldrini_contro_haters_denuncio_chi_mi_insulta-173037831/

[28] https://www.investireoggi.it/news/video-banca-intesa-san-paolo-virale-bullismo-invade-social/

[29] https://tg24.sky.it/cronaca/2020/12/29/claudia-alivernini-prima-vaccinata-minacce-social

[30] https://www.statista.com/statistics/380057/victims-of-internet-trolling/

[31] https://www.statista.com/statistics/708104/experiences-of-negative-online-activity-among-internet-users-in-the-uk/

[32] Istituto Eurispes, Rapporto Italia 2017, https://eurispes.eu/news/eurispes-rapporto-italia-2017-l875-dei-giovanissimi-e-stato-vittima-di-cyber-stalking/

[33]https://www.csg.org/sslfiles/dockets/2012cycle/32B/32Bdocmins/Cyberstalking,%20Cyberharassment%20and%20Cyberbullying%20Laws.pdf

[34] Come il progetto voluto dall'amministrazione Obama "*Police Data Initiative*" -https://www.policedatainitiative.org/

[35] Singapore's Protection from Harassment Act of 2014.

[36] Nigeria's Cybercrime Act of 2015.

[37] Cass. Sez. V Pen., 3.12.2020 n. 34512.

[38] "In tema di atti persecutori, la prova del nesso causale tra la condotta minatoria o molesta e l'insorgenza degli eventi di danno alternativamente contemplati dall'art. 612 bis cod. pen. (perdurante e grave stato di ansia o di paura; fondato timore per l'incolumità propria o di un prossimo congiunto; alterazione delle abitudini di vita), non può limitarsi alla dimostrazione dell'esistenza dell'evento, né collocarsi sul piano dell'astratta idoneità della condotta a cagionare l'evento, ma deve essere concreta e specifica, dovendosi tener conto della condotta posta in essere dalla vittima e dei mutamenti che sono derivati a quest'ultima nelle abitudini e negli stili di vita. (Fattispecie in cui la Corte ha ritenuto che la pressione ossessiva esercitata dall'imputato su una donna che aveva manifestato l'intenzione di interrompere la relazione sentimentale e la ravvisata invasione della sua sfera privata non includessero "in re ipsa" la determinazione di un perdurante e grave stato di ansia o di paura, potendo cagionare altri e diversi stati psicologici, come per esempio una forte irritazione)". Cass. Sez. III Pen., 18.11.2013 n. 46179.

[38] Cass. Sez. Pen. V, 14.10.2020 n. 28572.

[40] Cfr. da ultimo, Cass. Sez. V Pen., 6.11.2019 n. 45141.

[41] "Violenza virtuale contro le donne e le ragazze", EIGE, 2017.

[42] Consiglio per i diritti umani delle Nazioni Unite (2016) Risoluzione non vincolante, articolo 32: *The promotion, protection and enjoyment of human rights on the Internet*.

[43] "Violenza virtuale contro le donne e le ragazze", EIGE, 2017.

[44] Organizzazione mondiale della sanità, Dipartimento per la salute riproduttiva e la ricerca, London School of Hygiene and Tropical Medicine, South African Medical Research Council (2013). *Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence*", in EIGA 2017 cit.

[45] Agenzia dell'Unione europea per i diritti fondamentali (2014). *Violenza contro le donne: un'indagine a livello di Unione europea — Risultati principali*. Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, pag. 104 – in EIGA 2017 cit.

[46] Pew Research Center (2014). *Online Harassment (Molestie online)* - http://www.pewinternet.org/2014/10/22/online-harassment/;