LA VIOLENZA CONTRO LE DONNE: QUANDO IL DIGITALE CONFERMA IL REALE (I PARTE)

Tra le tante e rapidissime trasformazioni che caratterizzano la società attuale emergono anche nuove modalità di esercitare la violenza: lo zoombombing, un modo per attaccare associazioni, convegni e incontri con l'uso di accessi fraudolenti, portatori di insulti, disturbi sonori e immagini volgari; il cyberstalking, lo stalking realizzato attraverso ripetuti atti, perpetrati dalla stessa persona, svolto con il ricorso a piattaforme di messaggistica quali whatsApp o Telegram; il Deepfake e DeepNude che attraverso l'uso dell'intelligenza artificiale rielabora immagini o video ritraenti persone reali al fine di trasformarli in materiali multimediali a carattere pornografico, falso ma altamente realistico.

In questo numero: 1. Cyberstalking, 2. Molestie online e zoombombing, 3. Deepfake e DeepNude. Nel prossimo numero: 4. Sextortion, 5. Azioni di contrasto e risposte legislative, 6. Considerazioni finali.

Dott. Michele LIPPIELLO, Colonnello Redattore Capo della Rassegna dell'Arma dei Carabinieri.

Elisa MALANGONE, avvocato e collaboratrice esterna della Rassegna dell'Arma dei Carabinieri

Lo scenario contemporaneo è fortemente connotato dall'impatto che le nuove tecnologie hanno su una realtà sempre più filtrata e inglobata dal virtuale, con una digitalizzazione che interessa in maniera capillare e diffusa le nostre vite. Le forme di interazione umana sono oggi così condizionate dalla tecnologia che la stessa distinzione tra "mondo reale" (*life*) e "mondo virtuale" (*online*) risulta superata da una nuova realtà cd. "Onlife"[1], una dimensione relazionale e sociale dove esseri umani e macchine risultano pienamente interdipendenti. In questo contesto, la rivoluzione digitale sembra in grado di offrire nuovi spazi di libertà, di autonomia e di *empowerment,* ai quali tuttavia si associano, non di rado, forme crescenti e subdole di prevaricazione, suscettibili di alimentare azioni di sopraffazione e di violenza mirata. Quello speciale spazio-tempo in cui si realizzano i contatti interpersonali in "rete" è infatti ben lontano dal rappresentare il luogo privilegiato dell'uguaglianza e della parità di genere, tanto da poter raccogliere chiare tendenze ad un utilizzo dello schermo del mondo virtuale sempre più connotato da abusi diversi e atti di violenza basati sul genere, nello specifico contro le donne, che si realizzano attraverso messaggi virtuali molesti e aggressivi, accompagnati da insulti, espressioni intimidatorie fatte di retoriche sessiste, stigmatizzazioni a sfondo sessuale, messaggistiche ossessivamente ripetute, quando non si arriva anche alla diffusione di materiale dai contenuti sessuali espliciti, in scenari violenti, talvolta con l'impiego di contraffazione e alterazione delle immagini.
Sebbene anche gli uomini siano vittime di molestie online che includono insulti, derisioni e minacce fisiche, secondo uno studio effettuato dal *Pew Research Center*[2], le donne hanno più del doppio della probabilità di subire molestie sessuali virtuali rispetto agli uomini.
Già alcuni anni fa, nel 2017, a dare risonanza al problema è stato l'Istituto Europeo per l'Uguaglianza di Genere (EIGE) che, sollevando il problema della violenza cd. «virtuale» contro donne e ragazze[3], ha sottolineato l'altissima percentuale delle vittime femminili e dei danni da loro subiti; sul tema veniva peraltro riportata una interessante ricerca[4] che forniva indizi sulla sospetta continuità degli abusi e delle violenze contro le donne perpetrati online con le analoghe coercizioni *offline*, che tanto pesano sulla libertà individuale, nella vita pubblica e privata delle persone coinvolte.
A ben vedere, ciò che desta dunque allarme per la violenza di genere nel quotidiano si ripete con uguali caratteristiche e devastanti effetti reali anche nel vissuto della rete, qui in forme diverse, che di però di "virtuale" hanno solo la modalità di approccio, mentre la sofferenza psicologica non è meno grave.
Di queste diverse forme di violenza virtuale contro le donne e le ragazze[5] ci è sembrato utile svolgere qui di seguito una breve ricognizione volendo partecipare a quell'impegno corale mirato al contrasto di crimini tanto odiosi quanto culturalmente irrazionali.

1. Cyberstalking

Il *cyberstalking* è lo *stalking* realizzato attraverso ripetuti atti, perpetrati dalla stessa persona[6], svolto con il ricorso a strumenti o canali virtuali, come le piattaforme di messaggistica quali whatsApp o Telegram, i social network o SMS (*Short Message Service*, servizio messaggi brevi) e che consistono in comportamenti e interazioni intrusive dei *cyberstalker* nei confronti delle loro vittime. Si tratta di un vasto ed eterogeneo insieme di azioni che hanno come scopo congiunto quello di minare il senso di sicurezza delle donne, provocando angoscia, paura e allarme. In tale categoria rientrano "pedinamenti online", molestie diverse, quali l'invio di messaggi offensivi o minacciosi, la pubblicazione di commenti offensivi su internet, fino alla condivisione di fotografie o video

1 L. Floridi, The Onlife Manifesto. Being Human in a Hyperconnected Era, Springer, 2014.

2 Online Harassment 2017 link: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

3 Istituto europeo per l'uguaglianza di genere – L'EIGE https://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf

4 https://eige.europa.eu/sites/default/files/documents cyber_violence_against_women_and_girls.pdf o anche Stop alla violenza online, in "Amnesty International Italia", 2019. https://www.amnesty.it/appelli/stop-alla-violenza-online-su-toxictwitter/

5 Per la definizione di ciascuna forma si veda https://www.womensmediacenter.com/speech-project/online-abuse-101/

6 Così come emerge da rapporto "Violenza virtuale contro le donne e le ragazze" su file:///C:/Users/39375/Downloads/ti_pubpdf_mh0417543itn_pdfweb_20171026164002%20(1).pdf

intimi della persona su siti online o tramite scambio diretto per messaggistica istantanea. Il *cyberstalking*, tipicamente perpetrato online, è equiparato al reato di *stalking* e ne segue le stesse previsioni di legge. Il reato di stalking è entrato nel codice penale nel 2009, con l' art. 612-*bis* c.p. In effetti, il secondo comma di tale articolo sanziona quale aggravante l'agire degli atti predatori nel caso in cui vengano posti in essere attraverso strumenti telematici o informatici, ciò che si è realizzato con le disposizioni del D. L. 14 agosto 2013, n.93, art. 1, comma 3, lett.a), convertito dalla L. 15 ottobre 2013, n.119.
In tale ottica, anche di recente (febbraio 2020), la Corte di Strasburgo ha individuato obblighi ineludibili per gli Stati di adottare tutte le misure, preventive e sanzionatorie, necessarie a contrastare indebite intrusioni nei dati sensibili contenuti negli apparati tecnologici e negli account dei personali profili social che si verificano spesso ai danni di donne in un contesto domestico, configurando una vera e propria violenza domestica da perseguire senza deboli atteggiamenti, tanto da veder evocati, da parte della Corte Europea dei Diritti dell'Uomo, il divieto di tortura e il diritto al rispetto della vita privata e familiare con una sentenza del 2020[7].

2. Molestie online e zoombombing

I recenti periodi di condizionato confinamento legati alla pandemia da Covid-19 hanno visto un significativo aumento delle violenze nei confronti delle donne, in particolare *online.* L'isolamento cautelare ha costretto le ridotte relazioni umane quotidiane a ricercare una compensazione nei contatti *online,* con l'effetto di una maggiore esposizione ai rischi della rete, dove lo stato di frustrazione vissuto nel particolare momento ha finito per agevolare una diffusa aggressività, odio e rabbia inusitate.
Tra le tante e rapidissime trasformazioni che caratterizzano la società attuale emergono anche nuove modalità di esercitare la violenza, e tra queste appare con sempre maggiore frequenza quella che va sotto la denominazione di *zoombombing*, un modo per attaccare associazioni, convegni e incontri con l'uso di accessi fraudolenti, portatori di insulti, disturbi sonori e immagini volgari, al fine di destabilizzare con il proprio attacco (di qui il termine "bomb") proprio la piattaforma (da cui deriva il termine "zoom") che ospita e gestisce una riunione, una videoconferenza, un tranquillo seminario. Tale fenomeno indesiderato viene qui censito a ragione di un frequente uso, nelle dette circostanze, di una comunicazione-simbolo, propria della società patriarcale, ancora restia ad accettare le libertà e l'emancipazione del mondo femminile, e che nell'occasione adotta non di rado materiale pornografico, violento, con ricorrente esposizione di genitali, nell'intento di creare sconcerto e intimidire proprio gli incontri e i convegni dedicati a temi sociali e legati a tematiche femministe e alle questioni di genere, spesso con il solo obiettivo di denigrare le donne[8]. Gli autori, disturbatori singoli o gruppi organizzati, sfruttano in qualche caso la possibilità del libero ingresso ad eventi di carattere pubblico, e male si farebbe a considerare queste intrusioni quali episodi di mera e minima goliardia, atteso che i tentativi di limitare certe libertà non sembrano aver scelto obiettivi casuali.
Negli Stati Uniti l'FBI ha ricevuto così tante segnalazioni di episodi di "Zoombombing" da aver diffuso un avviso[9] sul problema, invitando le vittime a denunciare. La stessa organizzazione ha sottolineato l'urgente necessità di sviluppare efficienti strumenti per la tutela della privacy e dei dati personali.

7 Corte Edu, Causa Buturuga contro Romania, Sent. 11 Febbraio 2020 (RIC. N. 56867/15) Nel caso di specie, si era rivolta alla Corte una cittadina rumena che aveva denunciato l'ex marito per i ripetuti episodi di violenza domestica e per l'utilizzo abusivo dei suoi account informatici, inclusa la sua pagina Facebook, l'intromissione nel computer, lo stalking via web e l'acquisizione di dati e immagini. Il pubblico ministero aveva archiviato il procedimento perché i comportamenti dell'uomo non erano stati considerati come "particolarmente gravi". La decisione era stata impugnata dalla donna ed il tribunale di primo grado aveva disposto una misura di protezione applicabile per 6 mesi che, però, secondo i giudici di Strasburgo non era da ritenersi effettiva.

8 A tal proposito ricordiamo l'attacco hacker del convegno in webinar "La rete contro la violenza sulle donne" tenuto il 25 novembre 2020. Per un approfondimento su altri casi https://www.stopstalkingitalia.it/blog/1023-zoombombing/

9 FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI Boston. Kristen Setera(857) 386-2905https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Va da sé che la crescita di questo fenomeno impone rinnovate attenzioni sotto il profilo organizzativo, cercando di blindare possibili intrusioni nei modi più opportuni, come la tecnologia consente (per esempio impostando una password da comunicare solo alla ristretta cerchia dei partecipanti selezionati, con la raccomandazione di non divulgarla) ma nella consapevolezza della vulnerabilità ineliminabile che quella stessa tecnologia concede, riportandoci così alla conclusione che certe battaglie combattute sul fronte dei problemi di civiltà, si conducono comunque sul piano della crescita culturale.

3. Deepfake e DeepNude

Di recente ha iniziato a diffondersi un fenomeno chiamato "*Porno Deepfake*" che sta destando una serissima preoccupazione a livello mondiale soprattutto per il devastante impatto che genera sull'esistenza delle vittime[10].
Si tratta di una tecnica[11] che attraverso l'uso dell'intelligenza artificiale rielabora immagini o video ritraenti persone reali al fine di trasformarli in materiali multimediali a carattere pornografico, falso ma altamente realistico. Tali prodotti manipolati sono poi diffusi online attraverso i siti porno, i social network e le app di messaggistica istantanea.
Una ricerca condotta da *Sensity* (ex *Deeptrace*) ha evidenziato, attraverso la redazione di due report[12], la preoccupante capacità di diffusione del fenomeno, se si pensa che nel solo mese di luglio 2020 nelle chat private dell'app di messaggistica Telegram le immagini di ben 104.852 donne sono state virtualmente "spogliate" con l'uso dell'intelligenza artificiale, per poi essere pubblicamente condivise. La situazione è ulteriormente peggiorata con il lancio nel 2019 di un'app chiamata "*Deep Nude*" funzionante solo con immagini femminili, che permette di manipolare e "spogliare" artificialmente le immagini di qualsiasi donna vestita trasformandole in foto di nudo con un risultato finale di inquietante verosimiglianza.
Il fenomeno in questione è di tale pervasività da poter assumere rilevanza penale[13]; al riguardo, nel quadro di un complessivo studio mirato al contrasto della violenza contro le donne, si è pervenuti, forse con colpevole ritardo, ad un presidio normativo strutturato con l'entrata in vigore della legge 19 luglio 2019, n. 69 nota come "Codice Rosso" che, tra molto altro, ha introdotto nel nostro codice penale il c.d. *Revenge Porn.*
In effetti si deve rammentare che il nostro codice penale prevede una specifica tutela per il nuovo reato di cui all'art. 612 *ter*[14] rubricato "Diffusione illecita di immagini o video sessualmente espliciti", punendo non solo la condotta di chi, dopo aver realizzato o ottenuto le immagini, le diffonde per primo senza il consenso della persona ritratta, ma anche quella di coloro che hanno ricevuto tali immagini da altri o le hanno scaricate dal web e le hanno diffuse, al fine di recare nocumento alle vitti-

10 Sara Royle, Deepfake porn images still give me nightmares, 6 gennaio 2021 https://www.bbc.com/news/technology-55546372

11 La tecnica è appunto quella del "Deepfake"- neologismo inglese coniato nel 2017, che incrocia la locuzione deep learning (insieme di tecniche che permettono all'Intelligenza artificiale di imparare a riconoscere le forme) con la parola fake (falso, notizia falsa) – e permette di combinare e sovrapporre tra loro le immagini mediante reti neurali generative (in gergo tecnico, GAN).

12 Prime report pubblicato nel settembre 2019 dal titolo "The state of deepfakes-landscape, threats, and impact" disponibile sul link http://regmedia.co.uk/2019/10/08/deepfake_report.pdf. Secondo report dal titolo "Automating Image Abuse, Deepfakes Bots on Telegram" è consultabile al link https://www.medianama.com/wp-content/uploads/Sensity-AutomatingImageAbuse.pdf.

13 Amore N., La tutela penale della riservatezza sessuale nella società digitale. contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612-ter c.p., La legislazione penale, 20 gennaio 2020, http://www.lalegislazionepenale.eu/wp-content/uploads/2020/01/N.-Amore-Approfondimenti-1.pdf, p. 7: "In effetti, il Revenge porn, il Vouyerismo digitale, i Deep Sex Fake e così via hanno come elemento indefettibile la strumentalizzazione dell'intimità della vittima, compiuta attraverso l'ostensione della sua sessualità. La riservatezza che presidia la dimensione privata della vita, infatti, viene in ogni caso squarciata, trasformando il corpo e l'appartenenza di genere della persona in oggetti funzionali al soddisfacimento arbitrario dell'aggressore."

14 https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.progressivo=0&art.idArticolo=10&art.versione=1&art.codiceRedazionale=19G00076&art.dataPubblicazioneGazzetta=2019-07-25&art.idGruppo=0&art.idSottoArticolo1=10&art.idSottoArticolo=1&art.flagTipoArticolo=0

Istituto Poligrafico e Zecca dello Stato — Maria C. Perrini

me. Tuttavia, ad una attenta lettura, emerge che l'applicazione dello stesso articolo è previsto solo nell'ipotesi in cui foto o video a contenuto sessualmente esplicito siano stati originariamente realizzati con il consenso della vittima e poi condivisi e diffusi in maniera non consensuale, quindi "destinati a rimanere privati". Purtroppo, il dispositivo dell'articolo non fa alcun riferimento a contenuti multimediali non reali, fenomeno più recente, così che attualmente, avuto riguardo al principio della tassatività della norma penale[15] e alla mancanza di un preciso riferimento normativo, potrebbe risultare ardua l'inclusione del porno *deepfake* nella fattispecie incriminatrice del R*evenge Porn.*

È bene chiarire che i dubbi circa l'applicabilità del *Revenge Porn* ai reati di pornografia artefatta non impediscono alle vittime di rivolgersi ad altre forme di tutela penale previste nel nostro sistema; in primo luogo, è possibile tutelarsi sporgendo querela per diffamazione ex art. 595 c.p., in quanto tali *fake* sono comunque in grado di determinare la diffusione della denigrazione tramite il web, i social o le chat private e di offendere la reputazione di soggetti spesso ignari o vittime di relazioni abusanti.

E' appena il caso di aggiungere che i contenuti di *porno-deepfake* vengono creati in via prevalente al fine di estorcere qualcosa alla vittima con minacce di diffusione, così che nei casi di specie, la richiesta di denaro in cambio della non pubblicazione o della distruzione delle immagini realizzate, può configurarsi come un tentativo di estorsione ex art. 629 c.p.

È di tutta evidenza come i nuovi mezzi tecnologici (fra cui social e app) abbiano enormi potenzialità negative, con un impatto devastante sulla dignità, sulla reputazione, e più in generale, sull'esistenza stessa della vittima, relegata a sofferenze senza fine. E' dunque fondamentale e urgente sollecitare nuovi sforzi perché, non solo a livello legislativo, ma anche con il concorso di ogni altro attore sociale, vengano attivati ulteriori presidi di prevenzione per contrastare la diffusione del fenomeno in parola, e tempestivamente ogni altra malevola creatività di certi *hater* di professione.

Un approfondimento sul tema si può ritrovare nella Rassegna dell'Arma dei Carabinieri n. 2/2021 [16]. ©

15 Il principio di tassatività della fattispecie penale, corollario del principio di legalità di cui agli artt. 1 c.p., 199 c.p. e 25 Cost., implica che la norma penale deve individuare con precisione gli estremi del fatto reato in essa contenuti.

16 https://www.carabinieri.it/editoria/rassegna-dell-arma/la-rassegna