UNIVERSITA' TELEMATICA "e-Campus"

Facoltà di Giurisprudenza

Corso di Laurea in Servizi Giuridici curr. Criminologia

LO STALKING IN UN MONDO ONLINE

Relatore: Prof. Armando Palmegiani

Tesi di Laurea di: Marco Cesa
Matricola numero 2144901

Anno Accademico 2021/ 2022

LO STALKING IN UN MONDO ONLINE

Introduzione

Lo *stalking*: cenni storici e la sua evoluzione nel mondo *online*

Capitolo I ***CYBERSTALKING:*** **VESSAZIONI *ON LINE***

1.1 Il fenomeno del *cyberstalking*

1.2 La normativa vigente e il suo sviluppo

1.3 Identikit del *cyberstalker* e della vittima

1.4 Lo smodato utilizzo dei mezzi di comunicazione in era pandemica

CAPITOLO II **REVENGE PORN: IL REATO NASCOSTO DIETRO UN CLICK**

2.1 Introduzione alla nuova fattispecie criminosa

2.2 Casi di cronaca

2.3 Confronto tra normativa italiana e normative emergenti

2.4 Rischi e conseguenze del *revenge porn*

CAPITOLO III ***DEEPFAKE*****: LA NUOVA MINACCIA PER LA REPUTAZIONE**

3.1 *DEEPFAKE*: una minaccia crescente

3.2 Conseguenze del cattivo utilizzo del *DEEPFAKE*: le due facce della medaglia

3.3 Il *DEEPFAKE* nell'ordinamento giuridico

3.4 *DEEPFAKE* E *REVENGE PORN*: punti contatto

Introduzione

Per poter analizzare ed entrare nel merito della fattispecie criminosa del Cyberstalking, è necessario operare prima un *excursus* sul reato di stalking.

Il fenomeno dello stalking trova le origini dal verbo inglese "*to stalk*", ossia "inseguire, dare la caccia, andare di soppiatto".

Analogamente ad un cacciatore che dà la caccia alla sua preda, anche lo stalker nella sua azione persecutoria, insegue, pedina la vittima. La sottile ma fondamentale differenza risiede nel modo di agire: mentre il cacciatore realizza delle vere e proprie imboscate al fine di non essere percepito dalla sua preda, per poi palesarsi solo al momento opportuno, lo stalker fa invece "pesare" alla vittima la sua presenza, palesandosi nei modi più svariati (pedinamenti, scritte, biglietti, chiamate), intromettendosi con insistenza e frequenza nella vita privata della vittima.

Il comportamento del vessatore si traduce nel mettere in atto condotte che, in apparenza, fanno parte di un corteggiamento o di normali dimostrazioni di affetto con conseguenti attenzioni, ma in realtà, proprio perché diventano morbose e patologiche, causano forte disagio alla vittima, oltre che un costante stato d'ansia e di timore che le rendono difficoltoso anche solo vivere normalmente la propria routine quotidiana.

Per la prima volta si è cominciato a parlare di stalking negli anni 80, ma con riguardo agli atti persecutori e alle ripetute molestie che subivano personaggi

famosi dai loro stessi fan: sono stati proprio episodi di questo tipo a sensibilizzare sull'argomento, attirando molta attenzione e generando notevole interesse.

Nel 1997, gli studiosi Mullen e Pathè, definirono la condotta di stalking come "una costellazione di comportamenti tramite i quali un individuo affligge un altro con intrusioni e comunicazioni ripetute e indesiderate a un punto tale da provocargli timore per la propria incolumità"[1].

Mullen e colleghi (1997), rimarcarono che gli elementi che identificano il fenomeno non devono far riferimento alle mire del persecutore, ma basarsi sulle reazioni della persona offesa, che si ritrova a dover subire abitualmente attenzioni indesiderate e assillanti oltre che non desiderate. Quanto detto è essenziale per dare maggiore importanza e rilievo a quei comportamenti che ,altrimenti, potrebbero anche essere avvertiti come un consueto corteggiamento.

L'introduzione del concetto di "sindrome delle molestie assillanti", dovuta a due psichiatri italiani, Curci e Galeazzi (2001), ha una notevole importanza poiché da qui è possibile identificare i tre elementi caratterizzanti lo stalking:

- la presenza di uno stalker, soggetto persecutore;
- l'attuazione di una serie di azioni sorveglianti, di contatto e di comunicazione con la vittima;

[1] *Diaz R., Garofano L., I labirinti del male, Infinito Edizioni, 2013, p. 66*.

- la presenza di una vittima, soggetto passivo, che subisce tali comportamenti come sgraditi, fastidiosi ed intrusivi per il proprio progetto di vita.

Ancor prima che l'ordinamento italiano riconoscesse il reato di stalking grazie alla legge 38 del 2009, il crimine in esame veniva collegato al reato identificabile nella definizione di "molestia o disturbo delle persone" di cui si occupa l'art 660 c.p. secondo cui "*Chiunque, in luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo è punito con l'arresto fino a sei mesi o con l'ammenda fino a € 516".* Tale reato, quindi, prevede una pena per *"la condotta, insistente e petulante, idonea a turbare in modo apprezzabile le normali condizioni nelle quali si svolge la vita della persona molestata".* (Cass. 25 gennaio 1978, Laglia).
Quanto previsto dall'art. 660 c.p., differentemente dalla normativa attualmente vigente che configura lo *stalking* come un reato a tutti gli effetti, prevede delle contravvenzioni: ciò comporta che per potersi configurare l'elemento soggettivo basta che la condotta sia volontaria e che, rispetto ai delitti, ci siano più brevi termini di prescrizione.

Molti i casi emblematici di questo fenomeno: le atlete Hingis e Williams furono perseguitate nel corso di tutti i tornei internazionali dai propri vessatori così come l' attrice Theresa Saldana che fu pugnalata dal suo stalker a Los Angeles.

Proprio a causa di episodi di tal genere, venne emanato nel 1996 "l'Interstate Stalking Punishment and Prevention Act", legislazione prevista a livello federale. Nel Regno Unito si parla, invece, di harassment, fattispecie disciplinata e regolamentate nel *"Protection of Harassment Act"* del 1996. All'interno del nostro ordinamento,soltanto a partire dal 23 febbraio 2009, il governo dispose di emanare il decreto legge n. 11, "*Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori"*, detto "Decreto legge Anti-violenze", che ha parlato per la prima volta del reato di "*Atti persecutori*".

Si è assistito, quindi, all'ideazione di una nuova fattispecie di illecito al fine di penalizzare e punire la condotta persecutoria che si rivela rischiosa, soprattutto ma non soltanto nei confronti del sesso femminile. Il decreto legge è stato successivamente convertito in legge tramite il provvedimento del 23 aprile 2009, n. 38 (art. 7-12), rubricato "Disposizioni in materia di atti persecutori", la quale ha aggregato alla legislazione previgente, quanto disposto per la difesa e la salvaguardia delle vittime del reato di stalking. Tramite la predetta normativa, è stato introdotto nel codice penale l'art. 612-bis, rubricato "Atti persecutori", che recita "*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 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 se il fatto è commesso dal coniuge legalmente separato o divorziato o da persona che sia stata legata da relazione affettiva alla persona offesa. 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. Il termine per la proposizione della querela è di sei mesi. Si procede tuttavia d'ufficio se il fatto è commesso nei confronti di un minore o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio." [Art .612-bis CP 2009].

Con la diffusione sempre maggiore dei mezzi telematici, si sente sempre più la necessità di rimodulare il diritto penale attuale, poiché, le forme di evoluzione dello stalking non consentono l'applicazione della legge vigente. Ad esempio, per fronteggiare gli episodi di stalking al fine di tutelare la vittima, si possono emettere ordinanze restrittive nei confronti dello stalker; ciò, ovviamente, non ha nessuna applicazione nei confronti di un cyberstalker.

Un importante intervento a tutela delle vittime dello stalking online, potrebbe essere proposto prendendo spunto dalla legge 69 del 19 luglio 2019 che ha introdotto il *revenge porn*.

Dunque, in questo lavoro di tesi, focalizzeremo in primis l'attenzione sul fenomeno del cyberstalking e sulle figure coinvolte nell'attuazione di questa modalità di stalking, approfondendo la normativa vigente in Italia e nel resto del mondo. Inoltre, faremo un focus più approfondito sugli effetti che la pandemia Covid-19 ha prodotto nei confronti dell'utilizzo dei mezzi di comunicazione e dunque sullo stalking online.

Nel secondo capitolo, analizzeremo una specifica tipologia di cyberstalking, identificabile nel *revenge porn*, con riferimento a casi di cronaca italiani, così come nel capitolo seguente in cui, invece, dedicheremo attenzione al *deepfake*, analizzando anche i punti di distacco e di contatto con il *revenge porn*.

Concluderemo l'elaborato con un'ampia discussione sulle misure di prevenzione da poter attuare per prevenire e contrastare la diffusione di questi fenomeni, sia da un punto di vista giuridico che psicologico.

Capitolo I

CYBERSTALKING:* VESSAZIONI *ON LINE

1.1 Il fenomeno del *cyberstalking*

Nell'era dell'informazione, Internet è uno strumento essenziale sia nella gestione della vita privata, compreso il settore lavorativo, che nell'intrattenere rapporti tra soggetti pubblici.

Il processo che ha portato alla sua diffusione, spesso smodata, ha inciso notevolmente sulla quotidianità di ognuno di noi. Contenuti virtuali, tecnologie, e profonda diffusione dei *social media* hanno notevolmente decrementato rapporti umani, accrescendo, al contrario, quelli virtuali: per questi motivi, anche l'aspetto negativo di tali rapporti, che spesso si tramuta in vera e propria violenza, viene a galla nella problematica della cyberviolenza, oramai di interesse comune e con ragguardevoli ripercussioni sociali.

La legislazione penale ha subito recentemente un' evoluzione, tutelando maggiormente le vittime di violenza e riconoscendo l'esistenza della cosiddetta cybercriminalità.

Oltre alle molteplici possibilità fornite dai social media, bisogna considerare anche i cospicui *dark side* fra i quali troviamo i cybercrime, ossia "qualunque atto illecito

condotto o facilitato ad altri, agito intenzionalmente tramite internet e che causa danni materiali e /o immateriali a persone, animali o cose." [2]

Hayes et al. (2000) precisano, però, che il cybercrime è soltanto una maniera, spesso più efficiente ed efficace, di portare a compimento reati già conosciuti. Per Brenner (2006) servirebbe saper fare la differenza tra crimini tipici commessi attraverso l'utilizzo di nuovi mezzi e reati nuovi, anziché far rientrare tutto nel calderone unico del cybercrime. Da ultimo, Yar (2005) constata che, quando parliamo di cybercrime, dovremmo riferirci ad una specifica e nuova fattispecie criminosa .

Il mondo cybernetico fornisce all'essere umano una possibilità sempre maggiore di poter compiere atti illegali e violenti, soprattutto da un punto di vista psicologico, capaci di ledere la vittima nella sua sfera più intima e riservata: tutto ciò, si può sintetizzare nel termine di cyberstalking. L'origine del termine, si deve all'accostamento della parola inglese "cyber" (cibernetico) con il verbo che denota l'azione del fenomeno dello stalking.

Dunque, per poter parlare di Cyberstalking, l'azione telematica dello stalker deve caratterizzarsi per almeno uno dei seguenti tre eventi tipizzati dalla norma, con il fine ultimo di generare nella vittima, tramite minacce e molestie:

[2] Attrill-Smith e Wesson, *The Psychology of Cybercrime*, The Palgrave Handbook of International Cybercrime and Cyberdeviance, 2020, pp 653-678

1. grave e duraturo stato di paura e ansia;
2. timore eccessivo per la propria o altrui incolumità;
3. alterazioni delle tradizionali abitudini di vita.

Potrebbe convenire parlare, *ab initio*, della circostanza per cui, in numerosi casi, proprio come ci conferma anche la giurisprudenza, non siamo di fronte a nuove fattispecie di reati, ma a reati già esistenti con diverse modalità di attuazione: difatti, concettualmente, il fenomeno del Cyberstalking è similare a quello dello Stalking che, potremmo definire, la sua versione "offline".
Con il termine Stalking definiamo "una serie di atteggiamenti tenuti da un individuo che affligge un'altra persona, perseguitandola ed ingenerandole stati di ansia e paura, che possono arrivare a comprometterne il normale svolgimento della quotidianità. Il fenomeno è anche chiamato sindrome del molestatore assillante[3]".

Si ricorre all'espressione Cyberstalking quando si vogliono designare quelle condotte che, tramite l'impiego di dispositivi e risorse informatiche, vengono attuate da offensori definiti, appunto, cyberstalker allo scopo di tormentare le vittime, pretendendo un contatto di qualsivoglia natura, inoltrando messaggi indesiderati e minacciosi o che contengano intimidazioni e

[3] Giangrande A., *Anno 2021, La Giustizia Prima parte*, *Volume 232 di L'Italia del Trucco, l'Italia che siamo*, Giangrande, 2021

insulti. Il cyberstalker ha come fine quello di importunare, assillare e angosciare la vittima, annientando la sua reputazione e mettendo fine anche alle sue amicizie e può spingersi fino all'aggressione fisica.

Tuttavia, a lungo andare, il rischio in cui si può incorrere, è quello di non riuscire più a far fronte alla costante evoluzione tecnologica che fa traslare intere categorie di comportamenti, in maniera sempre maggiore, verso il mondo elettronico (Ziccardi, 2011a).
In riferimento a ciò, è dunque doveroso, ribadire che, a breve, la maggioranza delle forme di stalking verranno esercitate in maniera cyber, elettronica e non più perpetrate tramite mezzi "fisici" o analogici.

1.2 La normativa vigente e il suo sviluppo

In primo luogo, gli Stati Uniti hanno normato il rapporto che intercorre tra il mondo del web e tutto ciò che rientra nelle molestie, nelle manifestazioni d'odio e dell'aggressività verbale, generando una visione d'insieme che, a parere dell'interprete, risulta particolarmente stimolante e interessante.
Nel 1994, da un punto di vista della normativa federale, il Violent Crime Control and Law Enforcement Act, ha approvato il provvedimento con cui si approfondiva anche la problematica questione dei maltrattamenti e degli abusi perpetrati sulle donne, includendo in essa anche i maltrattamenti casalinghi, le forme di stalking

e le violenze a sfondo sessuale. Negli anni a seguire, nello specifico nel 1996, venne approvato l'Interstate Stalking Punishment and Prevention Act, a cui va il riconoscimento di aver introdotto lo stalking come reato a livello interstatale.

Bisogna specificare che nel codice penale italiano, proprio come riscontrato in altre fonti giuridiche, non c'è una definizione precisa di Cyberstalking, anche se è possibile riscontrare segnali a tal riguardo proprio in alcuni provvedimenti giurisdizionali attuali. Allo scopo di determinare la fattispecie criminosa in oggetto, occorre prima elaborare una digressione riguardo ai reati di minaccia (art. 612 c.p.), atti persecutori (art 612 bis c.p.) e molestia (art. 660 c.p.).

In base a quanto stabilito dalla dottrina e a quanto deciso dalla Suprema Corte, per poter parlare di stalking basta che ricorra anche una soltanto delle tre componenti criminose riportati nella norma: *"Salvo che il fatto costituisca più grave reato, chiunque reiteratamente, con qualunque mezzo, minaccia o molesta taluno in modo tale da infliggergli un grave disagio psichico ovvero da determinare un giustificato timore per la sicurezza personale propria o di una persona vicina o comunque da pregiudicare in maniera rilevante il suo modo di vivere, è punito, a querela della persona offesa, con la reclusione da sei mesi a quattro anni".* [Art .612-bis CP 2009].

D'altra parte, secondo la Cassazione, anche soltanto due episodi di molestia o minaccia possono essere fatti rientrare nella macro-area del reato indicato come "atti persecutori", qualora abbiano causato un continuo stato di paura o di ansia nella vittima, dato che si riferisce ad una fattispecie criminosa che deve obbligatoriamente articolarsi in più condotte messe in atto per un dato arco

temporale. Il criterio suddetto orienta anche le decisioni dei giudici di merito, con specifico riferimento all'attuazione di condotte moleste attraverso l'utilizzo delle tecnologie informatiche.

D'altro canto, si è reputato che perfezionino tale reato anche soltanto due comportamenti di intimidazione o di molestia che siano tali da integrare la ripetizione ricercata dalla norma, anziché il reiterato inoltro di email, sms, contenuti postati attraverso social, come anche la diffusione attraverso internet di filmati che ritraggono rapporti sessuali tra l'autore del reato e la vittima.

Risulta particolarmente interessante anche la circostanza per cui il tribunale di Termini Imerese, attraverso la sentenza del 9 febbraio 2012, per quanto attiene al delitto di cui all'art 612-bis c.p. ha messo in chiaro che "*integrano l'elemento materiale del delitto di atti persecutori le condotte riconducibili alle categorie del c.d. stalking vigilante (controllo sulla vita quotidiana della vittima), del c.d. stalking comunicativo (consistente in contatti per via epistolare o telefonica, sms, scritte sui muri, ed altri messaggi in luoghi frequentati dalla persona offesa) e del c.d. cyberstalking (costituito dall'uso di tutte quelle tecniche di intrusione molesta nella vita della vittima rese possibili dalle moderne tecnologie informatiche e, segnatamente, dai social network*)".

1.3 Identikit del *cyberstalker* e della vittima

Nonostante la recente diffusione della questione del cyberstalking e l'aumento delle ricerche condotte in merito, fare un identikit della vittima e ancor più del cyberstalker, può risultare abbastanza difficile.

La ricerca condotta da Cavezza e colleghi (2014) ha rilevato che il profilo del cyberstalker è generalmente associato ad un soggetto di sesso maschile; tuttavia, negli anni, il divario esistente con il genere femminile, si è notevolmente ridotto (Dreßing et al., 2014).

Da ulteriori ricerche è emerso che, generalmente, al cyberstalker viene attribuita un'età maggiore di 21 anni e l'essere impegnato in relazioni, con la stessa vittima o con altri soggetti. A conferma di ciò, Dreßing et al. (2014) nella loro ricerca hanno evidenziato che il 35% dei cyberstalker ha avuto in passato un rapporto con la persona perseguitata e che il 28.5% dei cyberstalker ha avuto rapporti di amicizia o conoscenza con la stessa vittima.

Per cercare di stilare un identikit del profilo del cyberstalker, dobbiamo sicuramente considerare i quattro tratti che costituiscono la Dark Tetrad (Smoker e March, 2017; Kircaburun et al., 2018; Ménard and Pincus, 2012).

La Dark Tetrad ha visto l'aggiunta agli iniziali tre tratti, quali narcisismo, machiavellismo e psicopatia (Glenn e Sellbom, 2015), grazie anche alle ricerche di Paulhus e Williams (2002) e Chabrol et al. (2009), del tratto del sadismo, poichè tutti e quattro, accomunano i soggetti nell'essere caratterizzati da un atteggiamento antisociale.

L'inserimento del tratto del sadismo fu dovuto al miglior contributo nel poter meglio spiegare la varianza dei comportamenti antisociali degli studenti delle scuole superiori rispetto ai soli tre tratti rilevati dalla Dark Triad.

Difatti, nella ricerca condotta da Buckels et al. (2014) è stato evidenziato come la Tetrade oscura sia associata a comportamenti antisociali ma anche a comportamenti dirompenti, come il *trolling online:* con tale termine, si intende l'attività di alcuni soggetti che postano in rete commenti offensivi e denigratori, con il solo obiettivo di umiliare o provocare terzi soggetti, o per innescare discussioni violente tra più utenti che prendono di mira un solo soggetto, vittima, che può essere un personaggio noto, famoso o un comunissimo individuo.

Smoker e March (2017) hanno rilevato che la compresenza dei tratti che caratterizzano la Tetrade oscura, è caratteristica esclusiva del cyberstalking attuato dal cyberstalker nei confronti della vittima, sua ex.

Il cyberstalker, differentemente dallo stalker che può mantenere o meno l'anonimato, utilizza nelle sue azioni di cyberstalking, dei nomignoli, falsi nomi o nickname, allo scopo di preservare l'anonimato della sua persona. La pericolosità e l'opportunità per cui è possibile restare anonimo, rendono il cyberstalker potenzialmente offensivo. Inoltre, poiché per poter esercitare le sue azioni, necessita solo di un mezzo di comunicazione online, ha la facoltà di nascondersi in ogni dove, chat room, social network, email.

A riprova di quanto detto, nel pensiero di Minnella C. (2011), il canale online dello stalking, offre all'aggressore diversi metodi di interazione per perpetrare i suoi atti persecutori, tra i quali:

- l'invio di enormi quantità di mail, scritte con toni sgradevoli o offensivi;
- l'intrusione nel sistema informatico della vittima tramite l'uso di programmi specifici con l'obiettivo di assumere il controllo di dati privati della vittima;
- furto o appropriazione di identità del perseguitato, con successiva diffusione tramite internet del suo nome associato a contenuti lesivi (associazione a newsletters, siti porno).

Dai risultati elaborati grazie all'indagine condotta dal Pew Research Center,è stato rilevato come le donne giovani siano le vittime maggiormente colpite dal cyberstalker. Tra il persecutore e il soggetto vessato può esserci stato un legame sentimentale passato, o, in altri casi, la vittima diventa un pensiero ossessivo per il cyberstalker, dovuto ad un rapporto diretto tra i due soggetti o un contatto con elementi come foto, video della stessa vittima. Si sottolinea che, attraverso una scrupolosa analisi dei dati delle ricerche effettuate in questo ambito, le donne di giovane età sono oggetto di cyberstalking con una frequenza maggiore rispetto a quanto lo sia il genere maschile.

Ulteriori studi, hanno acceso i riflettori sulle notevoli ripercussioni che la vittima vive e sui sintomi che quest'ultima sviluppa. Nello specifico, Cupach e Spitzberg

(2011) nella loro ricerca, hanno descritto gli effetti che il cyberstalking ha sulle vittime:

- effetti generali, con conseguenti modifiche sulla qualità di vita della vittima;
- effetti comportamentali ed affettivi, con modificazioni sul comportamento che la vittima ha quando si trova da sola o in compagnia di altre persone;
- effetti cognitivi, che incidono sulla qualità generale di vita del soggetto;
- effetti sulla salute fisica/ fisiologica
- effetti minimi, lievi e rare modifiche nello stile di vita della vittima.

In base alla gravità di tali effetti che la vittima stessa percepisce, gli effetti fisici e psicologici possono avere un carattere deleterio tanto da poter rientrare negli schemi di un disturbo psicologico, come ad esempio:

- *Disturbo da Stress Post Traumatico*, per cui la portata degli eventi sottopone l'individuo ad un livello di stress così elevato da non riuscire più a fargli fronte grazie al solo utilizzo delle strategie di coping. La vittima, anche dopo essersi liberata del suo Cyberstalker, continuerà a rivivere, attraverso incubi, ricordi, flashback, le angherie subite.Ciò porta la vittima ad un allontanamento dalle attività sociali.
- *Depressione, chiusura emotiva e relazionale*: la vittima si chiude in se stessa, isolandosi dal resto del mondo, con conseguenti effetti negativi

sulla sua vita sociale, lavorativa, ma soprattutto, sulla sua salute psicofisica.

Dunque, analizzando gli studi sul cyberstalking, fenomeno che si sta diffondendo a macchia d'olio sempre più frequentemente, non si possono negare le conseguenze negative che questo si porta dietro.
Risulta quindi importante, sensibilizzare le persone ad un uso corretto di internet, in primis, per prevenire che il fenomeno si diffonda ancor di più e, una volta riconosciuta la posizione di vittima di cyberstalking, fornire subito aiuto tramite richiesta alle Forze dell'Ordine e ai vari professionisti del settore, capaci di aiutarla nella gestione della situazione evitando che la tensione emotiva generata provochi problematiche ancora più gravi.

Nel caso in cui la vittima intenda procedere con una querela ai danni del Cyberstalker, in base all'art. 612 bis c.p., si ricorda che essa ha a disposizione sei mesi per la presentazione della querela; quest'intervallo temporale è stato creato per tutelare la vittima, al fine di darle maggiore tempo per attivarsi e tutelarsi.
Qualora le vittime, invece, fossero minori o persone con disabilità, si può procedere d'ufficio.
Nella fase prevista, poi, la vittima potrà comunque depositare un atto di costituzione di parte civile richiedendo, così, un risarcimento per i danni subiti e connessi alla condotta che l'aggressore ha attuato nei suoi riguardi.

1.4 Lo smodato utilizzo dei mezzi di comunicazione in era pandemica

Come già premesso nei precedenti capitoli, l'aumento dei mezzi tecnologici, della disponibilità di utilizzo della rete digitale e del facile accesso che oggi si ha nel mondo telematico, verrà ora analizzato anche in riferimento al periodo storico che il mondo ha vissuto e, purtroppo, vive ancora, da due anni a questa parte.

La presenza della pandemia Covid-19 ha imposto in maniera prepotente ed improvvisa, delle forti limitazioni ai contatti personali face to face. Ciò ha determinato una traslazione di ogni tipo di comunicazione dal mondo reale a quello digitale.

Ovviamente, bisogna tenere sempre presente le due facce della medaglia: se, da una parte, la tecnologia ha permesso di poter continuare a vivere in maniera "normale", introducendo la DAD per le scuole o lo smart working per le più svariate tipologie di lavoro, dall'altra, ha incentivato lo sviluppo delle forme di interazione patologiche virtuali.

L'essere rinchiusi in casa per la maggior parte delle ore del giorno, dovuto alle restrizioni ministeriali, ha dato maggiori opportunità allo svilupparsi delle situazioni criminose online, tra cui, come precedentemente detto, le forme di Cyberstalking che consentono allo stalker di agire in rete, in un mondo il più delle volte sconfinato.

Dunque, l'emergenza sanitaria dovuta al contagio da Covid ha portato dietro di sé conseguenze non soltanto sanitarie, ma anche da un punto di vista sociale e

della violenza. Difatti, i lock-down a cui tutti siamo stati costretti, sono stati vissuti in modo notevolmente peggiore dalle vittime di abusi e violenza, che si sono ritrovate imprigionate con il loro persecutore, aumentando i disagi, oltre che fisici, anche e soprattutto psicologici.

Prendendo in esame alcuni studi condotti nella prima fase della pandemia, ossia da marzo a giugno del 2020, sono stati rilevati aumenti nei numeri degli episodi di abuso domestico e, purtroppo, sono state registrate 58 vittime di omicidio in ambito familiare.

Come detto però, la pandemia, ha influenzato anche gli ambiti di violenza che hanno come scena di attuazione non quella domestica.

E' importante sottolineare che le forme di persecuzione virtuali come il cyberstalking sono molto spesso collegate a forme di stalking fisico: difatti, una cybervittima, molto probabilmente, ha prima subito violenze psicologiche, sessuali, fisiche; il cyberstalker, dalla sua parte, può infatti alternare forme di stalking offline a forme online.

Quindi, proprio per questa importante precisazione fatta, bisognerebbe analizzare la questione del Cyberstalking non solo come un problema legato al mondo tecnologico, ma anche legato al mondo sociale. Purtroppo, però, i riflettori accesi su questa problematica non sono ancora molto forti.

Le misure utilizzate per prevenire la diffusione dei contagi hanno quindi incrementato in modo smisurato e rapido l'ecosistema delle relazioni nel mondo

virtuale; proprio per questo motivo, la CEDU, acronimo che sta per Corte Europea dei Diritti Dell'Uomo, durante il mese di febbraio del 2020, ha riconosciuto la Cyberviolenza come " un aspetto della violenza contro le donne"[4], incentivando tutti i Paesi appartenenti all'Unione Europea a non sottovalutare gli episodi di violenza, anche e soprattutto, effettuati in modo virtuale.

Il mondo cibernetico è un posto in cui si perdono tutti i confini della sfera privata, tutti i limiti spaziali e temporali, incrementando in modo esponenziale il potere offensivo delle azioni esercitate e, conseguenzialmente, anche i danni psicologici per le vittime.
Nello specifico, l'Italia, con la legge n. 71 del 2017 ha regolamentato il cyberbullismo, offrendo così la chance di elaborare in modo più accurato tutte le forme di violenza telematica.

In conclusione, quindi, la pandemia non ha purtroppo fermato le forme di violenza, anzi, paradossalmente, ha creato territori di azione più ampi. Ciò ha posto il Governo Italiano alla predisposizione di un piano strategico antiviolenza 2021-2024, con la finalità ultima di incrementare la protezione delle vittime di violenza, qualsiasi tipo essa sia.

[4] CEDU: La Corte europea dei diritti del'uomo si pronuncia sulla cyber-violenza contro le donne (CEDU 11 febbraio 2020, ricorso n. 56867/15).

CAPITOLO II

REVENGE PORN: IL REATO NASCOSTO DIETRO UN CLICK

2.1 Introduzione alla nuova fattispecie criminosa

Come già citato nel precedente capitolo, il recente sviluppo dell'utilizzo di cellulari di ultima generazione e il conseguente boom dei social media, ha notevolmente aumentato anche l'invio di foto, video, messaggi e l'utilizzo delle webcam come mezzo di comunicazione, soprattutto nei giovani adulti (Walker, Sleath, 2017).
L'oggetto di tale scambio può essere identificato sia in foto, video dal normale contenuto, sia in media con contenuti che fanno riferimento esplicito alla sessualità: proprio su questa tipologia di materiale inviato e condiviso attraverso l'utilizzo di dispositivi digitali, si sono concentrate molte ricerche, le quali hanno etichettato questo fenomeno con il nome di *sexting*.
La ricerca condotta da Dir & Cyders (2015) ha stimato che, nella fascia d'età compresa tra i 18 e i 24 anni, la percentuale di giovani adulti che abbiano utilizzato i nuovi strumenti tecnologici per inviare, ricevere e condividere foto con contenuto sessualmente esplicito, vada dal 18 al 68%. Inoltre, i dati hanno anche sottolineato che spesso tale fenomeno, può coinvolgere soggetti che non si sono dimostrati consenzienti nella diffusione e pubblicazione online di immagini personali a sfondo sessuale (Döring, 2014).

Ad aggravare tale situazione è, sicuramente, non solo il libero accesso ad internet e, dunque, alla reperibilità e visione di tale materiale in maniera molto semplice, ma, soprattutto, la permanenza di tali info private e compromettenti, nel mondo online.

Quindi, con il termine di *Revenge Porn*, si fa riferimento alla pubblicazione, condivisione di foto, video, con un chiaro riferimento sessuale; tale materiale, è stato inviato dalla stessa "vittima" che, instaurato un rapporto di fiducia con l'altro soggetto, ha condiviso tale materiale compromettente e, magari a seguito di un rifiuto o una rottura, nel caso di soggetti legati da una relazione di coppia, ha visto pubblicare online tale materiale personale senza il suo consenso.

La ricerca elaborata e condotta negli USA dagli studiosi Citron & Franks (2014), ha posto l'accento su come la pubblicazione di contenuti personali a sfondo sessuale abbia un effetto negativo sulle vittime, le quali vanno incontro, secondo una prospettiva personale, ad un forte calo dell'autostima, all'insorgenza di attacchi di ansia e di panico, ad un opprimente senso di vergogna e di umiliazione e, dal lato sociale, anche a problematiche nel contesto di vita, nel contesto lavorativo (che spesso può portare anche al licenziamento), ad essere vittime di molestie verbali e fisiche, ma anche, all'essere vittime di stalking o cyberstalking.

E' doveroso sottolineare che spesso il *revenge porn* è descritto come una tipologia di pornografia non volontaria o non consensuale, per cui si attua una condivisione

di contenuto sessualmente esplicito, con alcuni autori che lo identificano solo nell'invio di foto, mentre altri, come invio di foto e video. Solitamente, alla base di tale condivisione, gli autori si accomunano nell'identificare nella vendetta la molla che dà vita a tale fenomeno per cui, il partner lasciato, non accettando tale decisione, chiede vendetta.

D'altra parte, altri autori, come ad esempio DeKeseredy & Schwartz (2016) e McGlynn & Rackley (2016), dopo aver esaminato i dati raccolti nelle varie ricerche sul fenomeno del *revenge porn*, lo hanno definito come "abuso sessuale basato sulle immagini" e, secondo il loro pensiero, la responsabilità non è da attribuire solo ad un ex partner mosso dalla vendetta, ma anche a persone che condividono tale materiale per scherzo, denaro o senza una reale motivazione, non dando il giusto peso a quanto si sta facendo.

Il non avere una definizione chiara e che accomuni la gran parte degli studiosi non consente spesso di poter stabilire se la diffusione di materiale a sfondo sessuale sia avvenuta con o senza l'esplicito consenso della persona oggetto di tali atti sessuali; tuttavia, tutte le definizioni, si accomunano per l'effetto che il *revenge porn* causa alle sue vittime.

In merito al *Revenge Porn*, è possibile identificare due punti di vista differenti: il primo, come già detto, per cui il *Revenge Porn* è considerato come una vera e propria violenza sessuale e/o intima verso il partner, scaturita da una condivisione

di materiale senza il consenso dei soggetti tirati in causa; ed il secondo, strettamente legato al primo punto, che propone di porre sotto la lente dell'indagine, il genere sessuale dei soggetti conivolti nel fenomeno, considerando spesso la diade maschio-esecutore e femmina-vittima (Henry & Powell, 2015a; Henry & Powell, 2015b; Salter & Crofts, 2015).

Nelle loro ricerche, Henry e Powell (2015) sottolineano come, grazie all'uso della tecnologia, sia possibile compiere crimini con origini più antiche, come, ad esempio la violenza sessuale, sostenendo che il fenomeno del *Revenge Porn* non si inneschi solo a causa della fine di una relazione, ma che spesso questo venga utilizzato come mezzo per controllare e minacciare partner attuali o ex partner. Ciò innesca un continuum di forme di violenze intime, in cui l'utilizzo della tecnologia, diventa un alleato fondamentale per espandere i comportamenti minacciosi e offensivi contro la vittima.

Per quanto riguarda la seconda opinione qui proposta, Stroud (2014) confuta la teoria proposta basata sul genere sessuale portando dati a favore di vittime di *Revenge Porn*, di genere sia femminile che maschile.
Da qui, Angelides (2013), Karaian (2014), Lee e Crofts (2015) e altri autori hanno dunque evidenziato che, a prescindere dal genere sessuale della persona coinvolta in episodi di *Revenge Porn*, l'attenzione debba essere posta sul comportamento problematico del fenomeno, ovvero sulla problematica legata alla

possibilità di condividere nel mondo digitale il materiale con sfondo sessuale, senza aver ottenuto il consenso da parte delle persone protagoniste dell'atto.

Negli interventi attuati in merito al fenomeno del *Revenge Porn*, Van e colleghi (2014), hanno proposto di includere la condivisione di materiale con contenuto sessualmente esplicito, negli interventi di prevenzione al fenomeno del bullismo e, soprattutto, del cyberbullismo. Tali autori, pur concordando sul comportamento rischioso generato da episodi di sexting, sottolineano l'importanza della società e, soprattutto del ruolo della scuola, nell'adottare campagne preventive per cui, piuttosto che focalizzare l'attenzione sulla colpevolizzazione della vittima, ci si concentri sulla condivisione non consensuale come un vero e proprio atto di bullismo / cyberbullismo.

Inoltre, progetti di prevenzione, dovrebbero anche sensibilizzare l'attenzione dei giovani adulti, nel non condividere mai materiale a sfondo sessuale né nei confronti di soggetti con cui si ha un rapporto attuale, né nei confronti di sconosciuti.

2.2 Casi di cronaca

Focalizziamo ora l'attenzione su alcuni casi di cronaca che hanno ad oggetto il *Revenge Porn*, i quali, data la loro portata, hanno incentivato la creazione di leggi specifiche per arginare e contrastare questa problematica.

In primis, uno dei casi che analizzeremo riguarda la condotta incriminatrice commessa da D. Feltmayernel nell'anno 2007 in Missouri: egli distribuì alcuni DVD contenenti atti sessuali consumati da lui e dalla sua (ex) fidanzata, senza il suo consenso, mosso da un sentimento di vendetto scaturito dall'inaccettabilità nell'accettazione della fine della loro storia d'amore. Poichè, nel 2007, non era ancora presente nessuna normativa che prevedesse punizioni per gli autori di *Revenge Porn*, Feltmayer si trovò a dover scontare la misera pena di 3 mesi di reclusione e 30 ore di servizi per la comunità. Questo perché, la condanna fu inflitta non per l'atto di *Revenge Porn* in sé e le relative conseguenze causate alla vittima, ma per l'aver diffuso, attraverso dvd, degli atti osceni.
Tutto ciò, si aggrava maggiormente, poiché, nella fase processuale, non si dimostrò che i video fossero stati prodotti con il consenso di entrambi, cosa che andava ad aggravare ancor di più la posizione del carnefice.
Analogamente, in California, durante il periodo di tempo che va dal 2012 al 2014, si sono consumati episodi simili, basati dunque su sentimenti vendicativi avvertiti da ex partner: tali episodi riguardavano la sconcertante scoperta di alcune vittime nel trovare pubblicati in rete alcuni video che li ritraevano durante rapporti sessuali, resi pubblici e facilmente accessibili dai precedenti partner.

La cosa che più contraddistingue questi episodi era la possibilità che il sito, in cui erano stati pubblicati tali materiali, dava alle stesse vittime: offriva loro la facoltà di richiedere la rimozione di tutto il materiale che le riguardava, dietro pagamento di ingenti somme di denaro.

In Canada, invece, ciò che portò alla determinazione di adottare una norma incriminatrice del fenomeno del *Revenge Porn*, fu il triste caso di Amanda Todd. Amanda, una giovane adolescente di 15 anni, si tolse la vita, nel 2012, a seguito della pubblicazione e successiva diffusione di una sua foto di nudo,inviata a tutta la sua comitiva e ai suoi compagni di scuola. La foto in questione, fu inviata dalla stessa Amanda ad una persona conosciuta via chat che, da quel momento, iniziò a ricattare la ragazzina, obbligandola a mandare foto sempre più sessualmente esplicite, tenendola in pugno sotto ricatto di pubblicazione della prima foto a seno nudo.

Quando Amanda e la sua famiglia appresero dalla polizia che la foto incriminata era stata pubblicata in rete, ed era dunque di libero accesso a tutti, rimasero profondamente sconvolti tanto che Amanda iniziò a fare uso di alcool e sostanze stupefacenti come "soluzione" ai suoi problemi di ansia e depressione. Con l'aggravarsi della situazione, l'intera famiglia pensò di lasciare la cittadina e trasferirsi in una nuova città per crearsi una nuova vita, cosa che però, non accadde. Difatti, il carnefice di Amanda, creò un falso profilo sui social intestato alla stessa ragazzina, con i dati anagrafici e i contatti della nuova residenza; il fatto ancor più grave fu che, nello stesso profilo, pubblicò la foto a seno nudo di

Amanda, riportando a galla, con una sola foto, tutto ciò che la ragazzina avrebbe voluto lasciarsi alle spalle con il trasferimento. Il fatto che ormai anche in questa nuova città molte persone erano ormai a conoscenza di questo episodio, portò Amanda a subire aggressioni, fisiche e verbali, e pregiudizi in modo sempre più marcato che la portarono ad un tentativo di togliersi la vita.
Questo primo tentativo, purtroppo per lei, fu sventato da parte dei soccorritori.
Nonostante gli aiuti che la ragazza ricevette e i successivi trasferimenti familiari, la portarono a subire continui atti di bullismo e cyberbullismo che, nel settembre del 2012, la portarono al suicidio.
A seguito di questo tragico episodio, la polizia Canadese identificò il responsabile che fu condannato a dover scontare una pena per abuso sessuale minorile.
Questa vicenda è da considerarsi importante perchè da qui si decise di proporre l'adozione di una legge contro gli atti di cyberbullismo, con la successiva emanazione della legge contro il fenomeno del *Revenge Porn*.

In ambito extraeuropeo sono da menzionare anche casi di cronaca noti, in Israele e in Giappone. Nello specifico:

- lo studio del *Revenge Porn* è stato approfondito in Israele a seguito di un episodio di cronaca riguardante una minorenne: a seguito della fine della sua relazione con il fidanzato, quest'ultimo, mosso dai sentimenti di vendetta, ha riempito di telecamere nascoste l'appartamento dell'ex fidanzata, ovviamente, senza il suo consenso. Tra il materiale registrato dalle telecamere, che riprendevano ogni momento della sua giornata,

c'erano anche atti sessuali che la ragazza aveva avuto con il suo nuovo fidanzato. Tali atti, sono stati pubblicati in rete dall'ex fidanzato che, una volta incriminato di tali reati, è stato prontamente obbligato alla rimozione del materiale pubblicato sul web e a risarcire la vittima e la sua famiglia;

- In Giappone, invece, fu proprio il primo cittadino ad essere condannato per atti di *Revenge Porn* attuati nei confronti della sua ex compagna. Tuttavia, l'approvazione di una specifica legge, si ebbe dopo l'episodio di stalking e cyberstalking avvenuto nel 2013 a Tokyo: la vittima, per mesi, ha visto pubblicato materiale privato, a contenuto sessualmente esplicito, da parte del suo ex fidanzato, che ha poi "concluso" la sua vendetta, con l'omicio della vittima. A causa di tale episodio, la legge giapponese decise di approvare una legge a tutela della vittime di *revenge porn*, ma anche, a scopo preventivo, per arginare questo dilagante fenomeno.

Ovviamente, nel citare casi di cronaca con oggetto episodi di *Revenge Porn*, non possiamo non dedicare attenzione alla vicenda di Tiziana Cantone, celebre caso che ha colpito l'opinione pubblica italiana.

L'episodio, conclusosi con il suidicio della ragazza, ha posto molto in evidenza il cosiddetto "dark side" dei social network.

Il tutto risale al 2015, quando, durante un rapporto sessuale, Tiziana, acconsentì ad essere oggetto di riprese da parte del suo fidanzato.

Nello stesso anno, qualche mese dopo, questo stesso fidanzato iniziò a pubblicare in rete questi filmati, inviandoli prima attraverso l'app di messaggistica Whatsapp e, successivamente, anche attraverso l'utilizzo di Facebook.

Il potere di condivisione di queste piattaforme, rese in pochissimo tempo virali questi filmati, tanto da renderli poi dei veri e propri fenomeni mediatici. Difatti, una frase che fu pronunciata dalla stessa Tiziana durante la ripresa del video, iniziò ad essere condivisa attraverso meme e riproposta in modo "scherzoso" da parte anche di personaggi pubblici.

Dunque, tutto quello che le persone vedevano come un qualcosa di divertente e su cui poter ridere, era, ovviamente, vissuto in maniera ben diversa dalla giovane ragazza che, nel settembre dell'anno seguente, consapevole dell'impossibilità di liberarsi ormai di quell'immagine che le era stata attribuita, decise di suicidarsi.

Dal punto di vista giudiziario, dopo varie vicissitudini, il G.I.P., nel 2017, ha disposto l'archiviazione del caso.

Nei recenti anni, l'ormai ex fidanzato della vittima Cantone, è stato mandato a giudizio per i seguenti capi di imputazione: simulazione di reato, calunnia ed accesso abusivo a sistema informatico, poiché, sarebbe stato proprio lui a convincere l'allora fidanzata a presentare una denuncia per fasullo smarrimento del cellulare personale e ad imputare i suddetti reati, successivamente, ai 4 ragazzi con cui fu condiviso per primo il video.

Dunque, la speranza che questo terribile caso ha voluto accendere, è quella che con il 612 ter c.p., si possa portare all'integrazione di un utile strumento per contrastare e reprimere i futuri atti di *Revenge Porn*.
Nel paragrafo successivo, analizzeremo alcune normative vigenti, in Italia e nel resto del mondo.

2.3 Confronto tra normativa italiana e normative emergenti

In questo capitolo abbiamo dunque introdotto e spiegato, anche attraverso casi di cronaca nazionali e non, il fenomeno del *Revenge Porn*. Ci soffermeremo ora sulle normative vigenti in Italia e nel resto del mondo per contrastare ed arginare questo fenomeno.

In Italia, l'ordinamento giuridico, si è basato molto sulle norme internazionali, europee e non, create ad hoc per contrastare il *Revenge Porn*.
Dal 9 agosto del 2019, è entrato in vigore nell'ordinamento italiano l'art. 612 ter del codice penale, per cui il *Revenge Porn* è definito come un vero e proprio reato, punibile con la reclusione da 1 a 6 anni e una sanzione pecuniaria da 5.000 a 15.000 euro.
La legge 69/2019 ha effettuato delle modifiche al c.p. con lo scopo di tutelare le vittime di violenza, di genere e violenza domestica, grazie all'introduzione di 21 articoli che introducono nuove tipologie di reato nelle quali rientra, per l'appunto, il *revenge porn*.

E' doveroso, però, effettuare ora un excursus generale sulle normative vigenti nel mondo.

Le più antiche normative a livello mondiale risalgono al 2004, grazie allo stato federale del New Jersey: nello specifico, il New Jersey Statutes 2C, secs. 15-19 dispone che "l'autore commette un reato di terzo grado se, sapendo di non essere autorizzato a farlo, rileva qualsiasi fotografia, film, videocassetta, registrazione o qualsiasi altra riproduzione dell'immagine di un'altra persona le cui parti intime sono esposte o che è coinvolto in un atto di penetrazione sessuale o contatto sessuale, a meno che tale persona non abbia acconsentito a tale divulgazione. Ai fini della presente sottosezione, "rilevare" significa vendere, produrre, dare, fornire, prestare, commerciare, spedire, consegnare, trasferire, pubblicare, distribuire, far circolare, diffondere, presentare, esporre, pubblicizzare o offrire. Fermo restando quanto previsto dal comma b. di N.J.S.2C:43-3, "una multa non superiore a $ 30.000 può essere inflitta per una violazione di questa sottosezione"[5].

Quanto detto da tale normativa del New Jersey, chiarisce in modo preciso e puntuale cosa si intenda per "diffusione", con il proposito di poter meglio delineare i confini entro cui è possibile parlare di illecito, differentemente dall'art.612 ter c.p.. Difatti, il codice penale italiano non delinea quali siano le condotte attraverso le quali possa avvenire la divulgazione e condivisione di

[5] N.J. STAT. ANN. 2C:14-9(c) (2004).

immagini e video, consentendo di lasciare uno spiraglio aperto per i nuovi metodi di divulgazione di tali contenuti.
Inoltre, la norma statunitense qui citata, non prevede una sanzione detentiva ma solo pecuniaria.

Si deve alla California l'introduzione successiva di una norma incriminatrice del *Revenge Porn*, a partire dal 2014; essa, oggetto di critica poichè molto restrittiva, dato che si può imputare il crimine solo a chi avesse partecipato alla produzione del materiale sessuale, è stata oggetto di correzione, seppur in parte, estendendo la sua applicabilità. Tuttavia, nonostante ad oggi non ci sia ancora una legge che operi a livello federale, gli USA garantiscono protezioni e tutele per le vittime di questo triste fenomeno.

Sempre nel 2014, più specificamente a gennaio, anche in Israele è stata introdotta una pena di ben 5 anni di reclusione per chi attuasse casi di *Revenge Porn*, fenomeno che, in sostanza, è stato paragonato ed eguagliato agli illeciti commessi attraverso abusi sessuali.
La punizione con reclusione, è stata adottata anche dal Giappone nel 2014 che, a differenza dei 5 anni previsti dalla normativa israeliana, punisce con 3 anni di reclusione tutti coloro i quali inviino un'immagine con contenuto sessualmente esplicito ad un'altra persona, senza il consenso della persona cui si fa riferimento.

Tuttavia, nonostante queste sanzioni, ad oggi, il Giappone è ancora lo stato che fa segnare un elevato numero di episodi riconducibili al *revenge porn*[6].

Infine, chiudendo il quadro delle normative extra europee, l'Inghilterra, nel 2015, ha introdotto un'apposita normativa che ha come fine ultimo quello di punire le condotte di *revenge porn*, seguita nel 2016 dalla Scozia.
Anche in questi casi, a differenza dell'art.612 ter, è richiesta l'azione specifica di voler commettere atti pregiudizievoli nei confronti della vittima, cosa che, di fatto, limita di gran lunga la reale portata di applicazione della suddetta norma.

Analizziamo ora il fenomeno del *Revenge Porn* da un punto di vista delle normative europee.

Il primo paese europeo che per primo ha introdotto una normativa sul fenomeno del *revenge porn*, è stata la Germania, nel 2014, per cui sono previste pene più mitigate rispetto alla normativa italiana: difatti, nel massimo della sua pena, sono previsti 3 anni di reclusione. Inoltre, allo scopo di frenare il sentimento vendicativo che può attivarsi in un partner che è stato lasciato, nel 2014 la corte regionale della Coblenza, cittadina tedesca, tramite sentenza, ha reso obbligatorio alla fine di una relazione, la cancellazione di materiale intimo da parte degli ex partner.

[6] *Legal and Constitutional Affairs Committee, Phenomenon Colloquially Referred to as 'Revenge Porn' (Commonwealth of Australia, 2016)*

Circa un anno dopo, anche la Spagna, ha creato una normativa specifica per i reati di *revenge porn*, per cui, in base all'articolo 197.7360 del codice penale spagnolo, sono punibili tutti i soggetti che diffondono a persone terze immagini, video, o anche registrazioni di audio realizzati in luoghi non pubblici, compromettendo la privacy dell'autore di tali atti, poiché pubblicate senza il suo consenso. Nonostante la legge creata ad hoc, le sanzioni applicate a tali malfattori si rivelano davvero inadeguate, poiché prevedono una reclusione da 3 mesi a un anno o, in alternativa, il pagamento di una somma di denaro.

Successivamente, nel 2016, la Francia ha emanato una legge per contrastare il crimine cibernetico, riversatasi nell'articolo 226-2-1 del codice penale francese per cui si prevede che, qualora la pubblicazione di materiale sessualmente esplicito non sia consensuale, il soggetto sia condannato ad una pena di 2 anni di carcere e una sanzione economica fino a 60mila euro.

2.4 Rischi e conseguenze del *revenge porn*

La condivisione non consensuale di materiale a sfondo sessuale esplicito porta dietro di sé una scia di conseguenze molto significative.

Alcune ricerche hanno, infatti, evidenziato che le molestie online sono associate a livelli più alti di sintomi psichiatrici, come forme di ansia e depressione,

consenso a forme sessuali forzate, forme di stupro, aumento del numero di partner sessuali ed aumento di esposizione a materiale pornografico (Thompson & Morrison, 2013), aumento del consumo di alcol, droga e sigarette (Patrick et al., 2015) .

D'altra parte, sono invece associate a livelli più bassi di autostima (Priebe & Svedin, 2012).

Ovviamente, va sempre chiarito che le ricerche condotte su soggetti vittima di condivisione non consensuale o di *Revenge Porn* permettono di stilare un quadro generale sull'impatto di questi fenomeni che può essere abbastanza diverso da soggetto a soggetto, se analizzato nello specifico.

Nell'effettuare un'analisi sulle ricerche condotte, nello specifico su gruppi di soggetti in età universitaria, Reed e i suoi collaboratori, nel 2016, hanno evidenziato, la presenza di un legame tra le forme di abuso digitale e quello fisico, tra l'abuso psicologico e quello messo in atto in modo sessuale nelle forme offline (ad esempio, la vittimizzazione).

Allo stesso modo, Marganski and Melander (2015) hanno sottolineato come la cyber vittimizzazione possa avere come conseguenza l'Intimate Partner Violence (IPV): attraverso l'acronimo IPV, nello specifico, si fa riferimento a forme di violenza attuate in ambito domestico, sia da un punto di vista sessuale, sia fisico che psicologico, perpetrate all'interno di una relazione intima con il proprio partner (Toro-Alfonso & Rodriguez-Madera, 2004; WHO, 1997). Lo studio ha

quindi evidenziato che coloro che sono state vittime di cyber vittimizzazione da parte del partner intimo hanno una probabilità più alta di essere vittime di :

- IPV psicologica, di circa 28 volte;
- IPV fisica, di circa 52 volte;
- IPV sessuale, di circa 4 volte.

Nella ricerca condotta nel 2016 da Morelli, Bianchi, Baiocco, Pezzuti, e Chirumbolo, si è posto l'accento sulla condivisione di materiale sessuale senza il consenso del soggetto che poi impersonificherà la figura della vittima e la perpetrazione della violenza nelle relazioni di coppia (*dating violence*) tra giovani ed adolescenti. In tale ricerca, si è dimostrato che la dating violence, così come le forme di sessismo benevolo e ostile, siano associate alla condivisione non autorizzata di materiale sessuale.

Nello specifico, le due forme di sessismo menzionate, moderano la relazione esistente tra condivisione non consenziente e la violenza nelle relazioni di coppia. La prima forma di sessismo descritta, ossia quella benevola, potrebbe contribuire alla riduzione di tale relazione, svolgendo, addirittura, la funzione di fattore protettivo; mentre, quello ostile, al contrario, potrebbe contribuire ad aumentare tale relazione, alimentandola.

Ulteriori ricerche (Bond,2010) , inoltre, hanno evidenziato che anche i fattori come il genere e l'età anagrafica possono essere rilevanti nell'attuazione del *Revenge Porn*.

Il genere femminile, dalle analisi dei dati ottenuti dalle varie ricerche, si è mostrato essere meno propenso nella condivisione di materiale sessuale senza il consenso da parte dell'uomo che, differentemente, procede nella diffusione del materiale con contenuto sessuale esplicito, anche senza il consenso della donna. Inoltre, in riferimento all'età, è stato rilevato che tali episodi hanno una frequenza maggiore tra i giovani rispetto ai soggetti più adulti.

Si è mostrato invece non avere nessuna rilevanza, l'orientamento sessuale della persona (Bond,2010).

D'altra parte, analizzando il fenomeno della condivisione di materiale sessuale online, è anche emerso che, i soggetti che vivono in una relazione stabile, non percepiscono questo fenomeno come un qualcosa di problematico, anzi, la considerano spesso come una normalità della relazione. E' nodale, altresì, sottolineare che esistono anche prove a sostegno della dannosità e dei rischi che tali atteggiamenti possono portare.

A riprova di ciò, Bond (2010), ha effettuato degli studi per analizzare il legame dei giovani con il loro cellulare e i rischi che associano al suo utilizzo, nella loro vita quotidiana: da questi studi, è emerso come a molti soggetti oggetto d'indagine non fossero ben chiari i confini esistenti tra la vita pubblica e quella privata ma, soprattutto, quanto fosse facile che l'immagine di un corpo nudo o la

visione di un atto sessuale percepito come privato e dunque con valenza positiva, possa trasformarsi in materiale pubblico e quindi negativo, con estrema facilità "grazie" all'uso della tecnologia. Ciò, come detto anche da altri autori, avviene con maggiore frequenza soprattutto quando si verifica un cambiamento nella relazione, come ad esempio, dopo una rottura tra i soggetti in causa. Nello specifico,riportiamo la testimonianza di un soggetto donna partecipante alla ricerca: "ho inviato foto di nudo integrale al mio fidanzato, in maniera privata. Lui, dopo che ci siamo lasciati, le ha diffuse pubblicamente, senza il mio consenso"[7].

Una cosa che, purtroppo, accomuna le vittime del *Revenge Porn*, è la paura che aumenta notevolmente il rischio di violenze fisiche e di stalking, effettuate online o offline, che spesso porta tali soggetti all'eliminazione di ogni loro profilo su pagine social per impedire a chiunque di poterli trovare ed identificare.

I soggetti i cui materiali personali vengono pubblicati online, sono sempre più vittime di insulti e minacce, fino addirittura alle minacce di morte, che li fanno sentire sempre meno al sicuro, anche in quei posti, in cui normalmente un soggetto dovrebbe sentirsi protetto e al sicuro, come anche la propria abitazione. A riprova di quanto detto, alcune vittime sono costrette ad abbandonare le loro vite, le loro abitazioni e i loro affetti più cari, per trasferirsi in posti lontani, dove nessuno, in teoria, dovrebbe riconoscerle.

[7] Bond E., 2016, *Sexting*, *Criminology and Criminal Justice*, 2016

Altre volte, purtroppo, tale soluzione non si rivela essere efficace e definitiva, portando la vittima a sprofondare in un profondo stato di disperazione per cui il suicidio è visto come unica soluzione possibile.

Anche il contesto lavorativo, può risentire di effetti significativi: nello specifico, uno studio realizzato da Microsoft nel 2009, ha rivelato che più dell'80% dei datori di lavoro si documenta sulla reputazione dei propri candidati online, e la utilizza come una buona base per le assunzioni nella aziendali. Quello che è doveroso sottolineare è che il datore di lavoro, reperendo informazioni on line che fanno riferimento, fra i tanti, ad aspetti legati alla sessualità, non si preoccupa nemmeno di contattare il candidato per chiedere come mai quei momenti riservati siano finiti in rete, ma opta per un'esclusione diretta del candidato da una possibile assunzione.

Da un punto di vista delle ripercussioni sulla salute, le vittime di *Revenge Porn* hanno dichiarato in più ricerche di soffrire di disturbi di ansia e di soffrire di attacchi di panico; nello specifico, Bates (2017), in un suo studio qualitativo effettuato attraverso la somministrazione di interviste, ha cercato di capire le esperienze delle vittime, esaminando anche la loro salute mentale.
Nel suo studio ha intervistato 18 soggetti femminili, vittime di *revenge porn*, sia di un ristretto gruppo di persone sia di gruppi più vasti, scoprendo l'impatto negativo che esso ha sulla salute mentale delle vittime, le quali, possono sviluppare molti problemi, come problemi di fiducia, disturbi da stress post

traumatico, forme di ansia e depressione, perdita di autostima e perdita del controllo sulla propria vita. Per sopperire a queste problematiche mentali, si era registrato un notevole implemento nell'uso di alcol, droghe e isolamento sociale. D'altra parte, però, si registravano anche soggetti che erano ricorsi a percorsi di sostegno e aiuto psicologico.

Dunque, dai dati raccolti dagli studi effettuati e nello specifico, dai dati raccolti nelle ricerche dello stesso Bates, si è potuto affermare che le vittime di *revenge porn* sviluppano conseguenze mentali molto simili a quelle vittime di violenza sessuale.

CAPITOLO III

DEEPFAKE: LA NUOVA MINACCIA PER LA REPUTAZIONE

3.1 *Deepfake*: una minaccia crescente

Il termine *"Deepfake"* attiene a tutti quei contenuti multimediali, quali foto, video, audio e testi, dal contenuto potenzialmente ingannevole; ovviamente, tale terminologia, non è da intendersi solo in un'accezione prettamente negativa, anzi.

Come sappiamo, questo fenomeno può assumere molteplici forme: dall'immagine semplice al video più complesso e realistico che riesce a trarre in inganno anche l'occhio più esperto.

Le prime tecnologie *deepfake* furono introdotte nel settore della visione artificiale, poi nell'audio e infine nella generazione di testo: questi, solitamente, hanno come oggetto la manipolazione dei contenuti e, ad esempio, lo scambio di espressioni del volto o di parti del corpo, oppure, prendendo in considerazione soltanto l'audio, la riproduzione di vocali utilizzando la voce di diversi soggetti, dopo soli 5 secondi di ascolto.

Si deve a Radford e colleghi (2019)[8], la creazione di un modello linguistico (GPT-2) capace di produrre in maniera autonoma, senza la supervisione di personale, dei paragrafi di testo coerenti, molto simili a quelli che un normale essere umano potrebbe essere capace di produrre.

Sempre nel 2019, Zellers e colleghi[9] , hanno contribuito alla generazione di testo grazie alla creazione di un nuovo approccio, GROVER, per l'apprendimento e lasusseguente generazione di documenti multi-campo, come articoli di riviste.

Inoltre, Keskar et al.[10] (2019), hanno introdotto CTRL, ossia un modello linguistico condizionale che fa uso di codici di controllo per la produzione di testo con stile, contenuto e comportamento specifico per l'attività.

Dunque se negli anni precedenti, la tecnologia associata al *deepfake* era accessibile solo a personale esperto in ambito informatico o con competenze particolari, a partire dal 2018 c'è stato un grande sviluppo di app *deepfake*, scaricabili sul proprio smartphone e quindi di libero accesso e di facile utilizzo per gran parte della popolazione.

[8] Alec Radford, Jerey Wu, Rewon Child, David Luan, Dario Amodei, and Ilya Sutskever. Language models are unsupervised multitask learners". In: OpenAI Blog 1.8 (2019), p. 9.

[9] Rowan Zellers, Ari Holtzman, Hannah Rashkin, Yonatan Bisk, Ali Farhadi, Franziska Roesner, and Yejin Choi. \Defending Against Neural Fake News", (2019)

[10] Nitish Shirish Keskar, Bryan McCann, Lav R Varshney, Caiming Xiong, and Richard Socher. \Ctrl: A conditional transformer language model for controllable generation", 2019.

Esempi di tali applicazioni sono FakeApp[11], FaceSwap[12] e DeepFaceLab[13] che si basano sulla possibilità di creare dei video e scambiare i volti delle persone che lo interpretano.

Tuttavia, se l'obiettivo primario era quello di suscitare ilarità nelle le persone che utilizzano la tecnologia *deepfake*, è importante tenere presente che l'attenzione è anche da attribuirsi al suo cattivo utilizzo e al legame che esso ha con elementi riguardanti disinformazione, in generale, ma più nello specifico, applicazioni legate al mondo del porno on line.

Difatti, la creazione di molti software di editing, basati sull'algoritmo del deep learning, facilita la creazione di oggetti e *multimedia*, per l'appunto "*fake*": per deep learning, va chiarito che intendiamo quella classe di algoritmi di apprendimento automatico che utilizza livelli multipli per estrarre progressivamente caratteristiche di livello superiore dall'input grezzo.[14]
Al fine di contrastare tale utilizzo del deepfake, non è necessario solo un controllo umano, ma anche un rilevamento automatizzato che si dimostri idoneo e abile nel rilevare la veridicità o meno, del materiale proposto.

[11] Zhi Peng Liu. FakeApp: un caso di studio sull'impatto dell'intelligenza artificiale. (Accesso il 27/05/2020). Febbraio 2018
[12] deepfakes/faceswap: software Deepfakes per tutti. (Accesso il 27/05/2020). 2019. URL: https://github.com/deepfakes/faceswap.
[13] Ivan Petrov, Daiheng Gao, Nikolay Chervoniy, Kunlin Liu, Sugasa Marangonda, Chris Um´e, Jian Jiang, Luis RP, Sheng Zhang, Pingyu Wu, et al. "DeepFaceLab: un framework di scambio di volti semplice, flessibile ed estensibile".
[14] https://www.treccani.it/vocabolario/deep-learning_(Neologismi)

Ad esempio, il software XceptionNet, consente di rilevare ed aiutare l'utente a capire se l'immagine o il video che si sta guardando, sia reale o il contenuto sia stato alterato grazie ad un *deepfake*.

Inoltre, anche alcune piattaforme quali Amazon, Facebook e Microsoft, hanno creato una "D*eepfake* Detection Challenge"[15] (2019) al fine di proporre soluzioni nuove e maggiormente efficaci per riconoscere i video *fake*, oppure Google (2019) che ha invece condiviso un database composto da più filmati *deepfake*, per aiutare i soggetti terzi ad allenarsi nel riconoscimento di materiale contraffatto.

Dunque bisogna fare i conti anche con i risvolti negativi e casi in cui tutto il materiale creato viene utilizzato per arrecare danno: il semplice sistema delle recensioni rilasciate su un sito internet, per esempio, può essere completamente falsato, sovraccaricando il tutto di recensioni distorte e fasulle al solo scopo, ad esempio, di disinformare e ledere l'immagine e la reputazione di un marchio.

3.2 Conseguenze del cattivo utilizzo del *DEEPFAKE*: le due facce della medaglia

Come si è affermato finora, lo sviluppo tecnologico porta dietro di sé una scia di effetti sia positivi che negativi.

[15] Yuezun Li, Xin Yang, Pu Sun, H. Qi, Siwei Lyu, Celeb-DF: A New Dataset for DeepFake Forensics, 2019.

Nel caso del *Deepfake*, è possibile delineare in maniera abbastanza netta, le due facce della medaglia.

Come spiegato nel precedente paragrafo, i risvolti negativi sono da identificarsi soprattutto nel cattivo utilizzo del *deepfake* con l'obiettivo di umiliare, frodare e dare una cattiva informazione ma, nel suo utilizzo negativo più comune, nell'associarsi ad attività pornografiche. Tali attività, risultano primariamente rivolte alle celebrità, soprattutto di sesso femminile.

Un esempio di app che aiuta il proliferarsi del *deepfake* associato alla pornografia è sicuramente la DeepNudesApp[16] che tramite l'uso di una foto di una qualsiasi persona vestita, grazie ad un algoritmo, riesce a creare una nuova immagine della stessa, ma in versione completamente nuda. Tale app funziona solo sul genere femminile e consente anche la modifica di alcune parti del corpo.

E' doveroso dire che il creatore di tale app ha, in un secondo momento, scelto di rimuovere la sua stessa creazione dalle piattaforme digitali.

Un altro famoso episodio è quello che ha riguardato Rana Ayyub, una scrittrice e giornalista investigativa che, a causa di una campagna di disinformazione messa in atto per screditarla, ha visto associata la sua immagine a tweet falsi, video porno e diffusione di informazioni personali e private.

[16] Samantha Cole. L'orribile app DeepNude spoglia una foto di una donna con un solo clic - VICE. (Accesso il 27/05/2020). Luglio 2019. URL: https:// www.vice.com/en_us/article/kzm59x/deepnud e-app-creates-fake-nudes-ofany-woman

Tuttavia, è opportuno spiegare anche la fattispecie rinominata *Cheap-fake*, ossia la sostituzione nel testo attraverso l'utilizzo di sinonimi o l'utilizzo di video con una bassa risoluzione.

Un'immagine estrapolata dal suo contesto di appartenenza, un elementare ritocco effettuato attraverso il programma Photoshop o un file audio tagliato e, quindi, modificato, rappresentano tutti esempi del fenomeno chiamato *cheap-fake*. Ciò ci fa riflettere su quanto la manipolazione sia sempre stata utilizzata, anche quando la tecnologia non aveva ancora raggiunto i risultati odierni.

Un caso che sottolinea tale utilizzo negativo è un video del 2018, condiviso su whatsapp: attraverso un taglio di alcuni fotogrammi del video e un controllo sulla velocità di riproduzione, è stato alterato il messaggio che voleva essere condiviso. Il video voleva sensibilizzare il triste fenomeno del rapimento dei bambini in Pakistan; tuttavia l'effetto ottenuto fu quello di portare alla creazione di folle di vigilanti atti a proteggere i bambini da qualsiasi persona si avvicinasse loro, producendo come effetto, il linciaggio di circa 20 persone.

Altro episodio che ben ci aiuta a capire gli effetti di un *deepfak*e risale al 2019 e, a farne i danni, è stata un'azienda energetica britannica: nello specifico, una voce *fake* è stata utilizzata per ingannare un CEO, facendogli credere che a chiamarlo fosse il suo capo. Tale inganno ha portato alla circostanza per cui fossero trasferite grosse somme di denaro sul conto di un fornitore perché *"il capo così mi aveva ordinato"*.

Da quanto detto, risulta abbastanza evidente che l'utilizzo inadeguato del *deepfake*, porti a rischi e conseguenze importanti. Il mondo cybernetico, infatti, non è esente da criminali che possono, tramite la creazione di un video o di un audio o immagini con la tecnologia del *deepfake*, indurre soggetti terzi a compiere determinate azioni che possono trasformarsi in vere e proprie truffe.
Ovviamente, gli effetti negativi sono da intendersi anche legati all'ambito psicologico per cui le vittime di *deepfake* possono sviluppare sintomi di ansia e depressione e, al contempo, lo stesso sviluppo del d*eepfake* ha portato le persone a diffidare sempre più delle immagini reperite su internet e a confidare sempre meno nella veridicità di foto/video/audio condivisi da altri soggetti, attribuendogli spesso la presenza, anche non accertata, di almeno un elemento *fake*.

D'altra parte, è possibile identificare anche un lato positivo nell'utilizzo del *deepfake*, soprattutto nel campo dell'istruzione o in quello dell'intrattenimento.
Ad esempio, la CereProc, azienda scozzese, ha ricreato l'audio del discorso che J.F. Kennedy, avrebbe dovuto tenere il giorno in cui fu assassinato. Con questo esempio, è possibile riportare l'importanza dell'utilizzo del *deepfak*e anche con quei soggetti che hanno delle problematiche che non gli consentono di parlare, a causa, magari, di malattie o infortuni.

Un ulteriore utilizzo positivo inerisce al mondo dei documentari: infatti, si riesce a dare un volto alle popolazioni poco visibili e conosciute, pur celando la loro reale

identità. E' questo il caso di "Welcome to Chechnya", un famoso documentario profondo e, al contempo, di particolare impatto che narra delle persecuzioni attuate sulla comunità LGBT in Cecenia e degli audaci tentativi degli attivisti di permettere loro di scappare e, così, sottrarli al pericolo. Insomma, si è trovato un modo sicuro per documentare i fatti senza esporre nessuno a pericoli. Il suo regista, France, afferma che: " *I deepfake cambiano ciò che la gente dice e fa e questo non cambia nulla. Permette ai miei soggetti di raccontare le loro storie. E restituisce la loro umanità in un modo che non sarebbe stato possibile in altre circostanze".*[17]

E ancora, anche in ambito scolastico il *deepfake* può trovare la sua ragion d'essere: attraverso questo strumento, si possono infatti sensibilizzare gli studenti riguardo a temi particolarmente delicati come, ad esempio, l'Olocausto: l'Illinois Holocaust Museum and Education Center, tramite una commistione tra interviste registrate e tecnologia di riconoscimento vocale, permette a chi è sopravvisuto ad un evento così tragico come l'Olocausto di dare risposta ai quesiti dei visitatori tramite un discorso che li veda protagonisti.

Anche l'arte potrebbe ricavare vantaggi dal *deepfake*: qualora si visitasse il Dalì Museum a San Pietroburgo, a dare ospitalità sarebbe lo stesso Dalì che spiegherebbe in prima persona la sua arte e i suoi capolavori.

[17] Rothkopf J. 2020. Deepfake Technology Enters the Documentary World. The New York Times.

3.3 Il DEEPFAKE nell'ordinamento giuridico

Come sappiamo, la tecnologia, di per sè, non rappresenta affatto una fonte di pericolo: può diventare rischiosa attraverso un utilizzo distorto.
In base ad una ricerca del 2019 effettuata dalla società Sensity che si occupa di Cyber Security, è stato chiaro che i video *deepfake* caricati on line sono quasi tutti pornografici e che anche Telegram è ormai diventata un'applicazione utilizzata al sol fine di scambiarsi video per adulti.

Ad oggi, nel nostro Paese non è ancora presente una normativa specifica al riguardo, anche se grazie al cosiddetto "Codice Rosso", come poi vedremo, è stato compiuto un notevole passo in avanti. Il problema, però, è relativo alla circostanza per cui la norma non menziona contenuti artefatti: in base al principio di tassatività vigente in ambito penale, la legge deve indicare precisamente gli estremi costituenti il reato; la mancanza, poi, di giurisprudenza in materia ha reso la gestione del problema ancor più complessa.

La domanda che sorge spontanea, quindi, è relativa al modo in cui ci si può tutelare.
In primis, si potrebbe presentare denuncia per diffamazione, ex art. 595 del codice penale: *"Chiunque, comunicando con più persone, offende l'altrui*

reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro.

Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a duemilasessantacinque euro.

Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a cinquecentosedici euro.
Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio , le pene sono aumentate."[18]

Qualora, invece, fossimo di fronte ad una situazione per cui i contenuti fossero stati creati con lo scopo di minacciare o con il fine di estorcere del denaro dalla vittima in cambio dell'eliminazione dello stesso contenuto o della sua mancata pubblicazione, può integrarsi il reato di estorsione, ex art 629 del codice penale:
"Chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 a euro 4.000.

[18] art. 595 codice penale

La pena è della reclusione da sette a venti anni e della multa da da euro 5.000 a euro 15.000, se concorre taluna delle circostanze indicate nell'ultimo capoverso dell'articolo precedente."[19]

In aggiunta, potrebbero configurarsi anche altri due reati: lo stalking, nel tentativo di recuperare innumerevoli video e immagini relativi alla vittima e il reato di trattamento illecito di dati personali ex art. 167 del Codice della Privacy , oltre che il furto di identità ex art. 494 del codice penale in base viene dettato quanto segue.

" *Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno."*[20]

Per quanto attiene, invece, ai paesi stranieri, possiamo fare riferimento agli Stati Uniti.

Tra il 2018 e il 2019 sono stati introdotti il *"Malicious deepfake Prohibition Act of 2018"* e il *"deepfake Accountability"*.

[19] art. 629 codice penale
[20] art. 494 codice penale

Il governo statunitense e, in prima persona il senatore Ben Sasse, hanno firmato il "*Malicious deepfake Prohibition"*: quest'atto contiene in sé la disciplina delle conseguenze e delle responsabilità giuridiche collegate al dar vita e a condividere contenuti multimediali artefatti.

Grazie ,soprattutto, a provvedimenti della medesima tipologia, le Agenzie di sicurezza americane hanno messo in atto specifici controlli per cercare di epurare il mondo di internet da contenuti fasulli, disinformanti e offensivi: il loro fine è quello di rendere la vita dei potenziali carnefici particolarmente complicata.

Il *"deepfake Accountability"*, invece, è un atto di circa 25 pagine che si basa su due nozioni fondamentali: l'obbligo per chi dà vita ad un deepfake di fare una dichiarazione in cui ammette che il video è stato oggetto di alterazione, altrimenti verrà integrato un reato federale; la possibilità della persona danneggiata di poter far causa alla persona che ha creato video o immagini incriminati.

Un ulteriore esempio potrebbe esserci fornito dalla Cina.

Quasi alla fine dell'anno 2019, la Cina ha dichiarato che, dall'anno successivo, i *deepfake* dovevano essere forniti di un *watermark* o, in ogni caso, di qualcosa che renda immediatamente palese che si è di fronte ad un contenuto, appunto, *fake,* altrimenti si commette un crimine. L'esecutivo cinese, inoltre, ha anche chiarito che avrebbe cominciato a perseguire e punire alacremente tutti coloro i quali, nel mondo cibernetico, non dimostravano di rispettare suddette norme.

3.4 *DEEPFAKE* E *REVENGE PORN*: punti contatto

La circostanza per cui, nel corso del tempo, sia stata utilizzata in misura sempre maggiore la tecnologia, anche al fine di porre in essere fattispecie criminose, ci obbliga, in una maniera o nell'altra, a fare i conti con crimini di nuova generazioni, non ancora normati. Tutto ciò, ad oggi,è diventato imprescindibile a causa della propagazione dei suddetti reati e della loro correlata potenzialità di offesa.

In base al Report "The State of deepfakes" del progetto Sensity per indagare e identificare il fenomeno del *deepfake*, alla fine dell'anno 2019 i casi erano quasi il doppio dell'anno precedente, davvero troppi: all'incirca 15.0000.
A rendere tutto ciò una fonte di preoccupazione ancor più crescente è che quasi il 95% dei video in questione erano pornografici; soltanto una minima percentuale, pari a meno del 5%, erano di altro tipo. Questo vuol dire che, nella gran parte della casistica, il *deepfake* viene utilizzato in circostanze patologiche e in contesti disturbanti che rendono internet un utensile di cui ci si serve al fine di integrare un reato: difatti, un'ulteriore fattispecie criminosa a cui è connesso è rappresentato dal *revenge porn*.
L'art 612 ter c.p., che si riferisce alla "Diffusione illeciti di immagini o video sessualmente espliciti", lo sanziona direttamente ed è stato inserito all'interno del codice penale italiano grazie al provvedimento legislativo noto come Codice Rosso (L. 69/2009). La disposizione in oggetto è stata inclusa proprio perché il fenomeno si è esteso più che mai, diventando a dir poco incontrollabile :

diffondere video e immagini, a sfondo sessuale, senza che la vittima avesse prestato il suo consenso o sottraendoglieli fraudolentemente, è purtroppo diventata una consuetudine e ne sentiamo notizie quasi quotidianamente. Va inoltre sottolineato che, prima che intervenisse la suddetta riforma, le leggi presenti non si erano dimostrate sufficienti ad arginare il problema né ad interrompere la fattispecie criminosa attraverso la minaccia di una sanzione severa e consona.

Entrando nel merito dell'art 612 ter del codice penale italiano, la norma sanziona tutti i comportamenti che consistono nell'inoltrare, consegnare o pubblicare, quindi diffondere, "immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate".

Ciò che distingue l'articolo è, nello specifico, la pluralità delle persone a cui è destinato: non vuol soltanto punire chi abbia realizzato e contribuito alla diffusione dei contenuti, che abbiamo poc'anzi citato, ma anche tutte quelle persone che, anche se non hanno partecipato attivamente a produrre o a sottrarre video e foto, abbiano in qualche misura preso parte alla loro diffusione. Suddetti soggetti saranno puniti con la reclusione da uno a sei anni e con una multa da 5.000 a 15.000 euro: *condicio sine qua non* affinché venga applicato l'articolo di cui stiamo parlando è che manchi il consenso della "vittima". Più nello specifico, deve essere assente una manifestazione di volontà esplicita e positiva: non si può desumere.

Dall'art 612, infine, ai commi 3 e 4, viene previsto che le sanzioni vengano inasprite qualora il reato venga integrato il reato in circostanze maggiormente

gravose, come un rapporto affettivo tra il colpevole e la vittima o nel caso in cui la stessa persona perseguitata versi in uno stato di inferiorità psichica o fisica.

Dopo la disamina di ambo i reati, può risultare fondamentale comprendere il modo in cui riescono a mettersi in contatto in una singola condotta dannosa e pregiudizievole: si può rispondere a questa domanda utilizzando termini di nuova generazione come "*deepnude*" e "porno *deepfake*", facenti riferimento tutti e due a comportamenti che consistono nell'uso, appunto, di *deepfak*e al fine di dar vita a fasulli contenuti con sfondo e intento pornografici. Filmati e immagini vengono create attraverso la sovrapposizione dell'immagine raffigurante una persona su una foto o un video che risultano sessualmente espliciti: la stessa persona che si ritrova ad essere vittima di questa situazione si vede protagonista di una scena mai realmente accaduta, in coppia con persone che neanche conosce. E' altresì possibile denudare digitalmente una persona, pur partendo da una foto in cui risulta vestita.

Sintetizzando quanto appena detto, il carnefice, dato che non possiede oggetto tramite cui ricattare la sua vittima, li crea dal nulla pur di commettere un comportamento che integra il reato di *revenge porn.*

Una volta individuato il punto di raccordo che sussiste tra l'utilizzo di internet per scopi illeciti e la divulgazione di pornografia, tuttavia, rimane l'interrogativo sul modo in cui si può collegare il porno *deepfake* alla macroare del *revenge porn*, dato che non esiste tuttoggi una normativa determinata e specifica che ne parli e che nemmeno la giurisprudenza se ne è occupata.

Proprio perché la norma inquadrata dall'art 612 ter c.p. fa riferimento a contenuti sessualmente espliciti che siano stati prodotti, sottratti, ricevuti o altrimenti acquisiti, non parla in modo chiaro e preciso di oggetti che siano nati grazie all'utilizzo della tecnologia e, quindi, non veritieri.

Sulla base del principio di tassatività della suddetta norma e del divieto di analogia, entrambi fondamenti del diritto penale stabiliti costituzionalmente (art 25 costituzione), dall'art 1 del codice penale e dall'art. 14 delle Preleggi, appare arduo ricondurre il porno *deepfake* nel reato noto come *revenge porn.*

Altra situazione si presenterebbe, se le immagini riguardanti i porno *deepfake* riguardassero soggetti che non ancora abbiano compiuto 18 anni: secondo quanto stabilito dall'art. 600 quater 1 del codice penale, che si occupa del crimine di pornografia virtuale, viene integrato il reato di pornografia minorile (art 600 ter) e il reato di detenzione di materiale pornografico (art 600 quater c.p.) anche qualora foto e video fossero virtuali ossia "realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali".

Suddetta normativa, quindi, si riferisce a ciò che viene creato tramite internet e intelligenza artificiale.

CAPITOLO IV

MISURE DI PREVENZIONE E DI CONTRASTO

4.1 Misure di prevenzione e di contrasto al *cyberstalking*

Ormai quotidianamente, i giudici hanno dovuto porsi interrogativi circa la possibilità di integrare il reato noto come stalking perpetrato in rete.
Anche la Suprema Corte ha, in numerose sentenze, dato applicazione alla disciplina di cui all'art. 612-bis per i casi in cui si è perfezionato il cyberstalking, andando di fatto ad anticipare, e di certo ad incoraggiare, l'iniziativa successiva del legislatore che ha condotto all'integrazione del comma 2.

La Suprema Corte, con la V sezione penale e attraverso la Sentenza nr. 25488/2011 del 24 giugno, ha confermato quanto sia rilevante la fattispecie criminosa nota come cyberstalking, ribadendo nei riguardi di un uomo il "divieto di avvicinamento" agli ambienti e ai luoghi frequentati in maniera abituale dalla sua ormai ex ragazza con cui, tra l'altro, aveva anche convissuto.

Il reo, in un secondo momento all'interruzione della convivenza decisa dalla vittima, le aveva inoltrato messaggi contenenti minacce e offese gratuite in maniera reiterata e costante tramite il social network noto come Facebook.

Non pago delle sue malefatte, si era intrufolato nella dimora della sua ex fidanzata e le aveva causato numerose lesioni con un'aggressione fisica e violenta.
Il Tribunale Supremo, relativamente all'episodio specifico, aveva statuito che la messaggistica scambiata tramite Facebook poteva integrare la fattispecie del cyberstalking: grazie a questa pronuncia, ci rendiamo conto di quanto siano stati essenziali gli interventi della Cassazione.
La riportiamo di seguito.

SUPREMA CORTE DI CASSAZIONE

SEZIONE V PENALE

Sentenza 15 aprile - 24 giugno 2011, n. 25488

(Presidente Calabrese – Relatore Zaza)

"Ritenuto in fatto

Con il provvedimento impugnato veniva parzialmente confermata l'ordinanza del Giudice per le indagini preliminari presso il Tribunale di Salerno in data 6.12.2010 laddove con la stessa veniva applicata nei confronti di C. M. la misura cautelare del divieto di avvicinamento ai luoghi frequentati dalla persona offesa per i reati di cui agli artt. 612 bis, 582 e 614 c.p., ed in particolare per aver violato il domicilio

in Salerno di P. D. il 17.5.2010, per aver costantemente minacciato la P. dopo che la stessa aveva interrotto la convivenza con l'indagato, con messaggi inviati tramite il sito internet Facebook dal 3.9.2010 al 16.11.2010, e per aver infine in quest'ultima data percosso la P. cagionandole lesioni.

La sussistenza dei gravi indizi a carico del C. era ritenuta in base alle dichiarazioni della persona offesa e agli ulteriori elementi individuati a riscontro delle stesse.

Il ricorrente deduce violazione di legge, lamentando l'assunzione quali riscontri di certificati medici che per la maggior parte riportavano patologie riferite dalla stessa P., e all'inclusione fra gli stessi di un referto in data 29.5.2010 non esistente agli atti e relativo ad un periodo non contestato.

Considerato in diritto

Il ricorso è infondato.

L'ordinanza impugnata motivava invero in tema di gravità indiziaria ritenendo la parte offesa attendibile non solo per la conferma derivante da più certificati medici diversi da quello di cui il ricorrente lamenta l'irrilevanza, ma anche per gli apporti provenienti dalle dichiarazioni della madre della P., B. R. M., sui messaggi telefonici ricevuti dalla figlia e sulla manifestata paura della stessa di uscire dall'abitazione, e da quelle di C. L. sulla constatazione delle lesioni prodotte il

2.9.2010 e sull'atteggiamento aggressivo del C. nei confronti della P. nell'episodio del 27.9.2010. Detta motivazione, per la pluralità e la significatività degli elementi valutati, è logicamente inattaccabile dalle censure del ricorrente, indirizzate unicamente sui riscontri documentali, per i quali si propone peraltro una mera lettura in chiave difensiva dei relativi contenuti, e prive di specifiche doglianze sulla credibilità intrinseca della parte offesa.

Il ricorso deve pertanto essere rigettato, seguendone la condanna del ricorrente al pagamento delle spese processuali.

P.Q.M.

Rigetta il ricorso e condanna il ricorrente al pagamento delle spese."

In realtà, già in precedenza, nello specifico un anno prima, attraverso il provvedimento 32404/2010, la Cassazione con la VI sezione penale aveva stabilito che *"gli atti di molestia reiterati e idonei a configurare il delitto di stalking ex art. 612 bis c.p., possono concretarsi non solo in telefonate, invii di buste, sms, e-mail, nonché di messaggi tramite internet, anche nell'ufficio dove la persona offesa prestava il suo lavoro, ma possono consistere anche nella trasmissione da parte dell'indagato, tramite Facebook, di un filmato che ritraeva un rapporto sessuale tra lui e la donna".*

Difatti, nel caso specifico, i giudici avevano analizzato condotte che avevano causato nel soggetto-vittima una condizione di apprensione-agitazione e una sensazione di vergogna, condizione e sensazioni talmente gravi da portare, in qualche modo, alle dimissioni la persona che aveva subito violenza.

Grazie ad una decisione susseguente, la Suprema Corte ha chiarito che offendere, ingiuriare e inoltrati messaggi di minaccia attraverso Facebook può perfezionare la fattispecie criminosa dello stalking e non il reato noto come diffamazione, se i comportamenti messi in atto dal reo generano nelle vittime "uno stato di ansia e di paura".

Ciò ha tratto origine da un episodio in particolare: un uomo, che aveva perso la custodia dei suoi figli a seguito della separazione dalla coniuge, aveva messo in atto vere e proprie persecuzioni ai danni degli, ormai, ex suoceri, utilizzando anche Facebook come strumento per perpetrare le sue malefatte.

I suoceri avevano cominciato a vivere in un perenne stato di timore profondo e di ansia crescente, temendo realmente per la loro stessa incolumità: fu questo a dare vita alla sentenza nr. 21407/2016 del 23 maggio.

Grazie a questa pronuncia, si è reso pacifico quanto segue: anche una condotta, che consti nella pubblicazione di un commento offensivo sui social e diretta ad un soggetto, se presa in considerazione singolarmente, potrebbe perfezionare il reato noto come diffamazione o minaccia (ex art. 595 del codice penale ed ex art. 612 del codice penale); se venisse perpetrata nel corso del tempo in modo continuativo, potrebbe integrare il reato di stalking.

La sezione V del Tribunale Supremo, coerentemente rispetto a quanto era stato statuito dalla giurisprudenza di legittimità, dopo aver statuito che: "*I messaggi o filmati postati sui social network integrano l'elemento oggettivo del delitto di atti persecutori"*, ha altresì precisato che: *"L'attitudine dannosa di tali condotte non è tanto quella di costringere la vittima a subire offese o minacce per via telematica, quanto quella di diffondere fra gli utenti della rete dati, veri o falsi, fortemente dannosi e fonte di inquietudine per la parte offesa".*

Le pronunce a cui stiamo facendo riferimento prendono origine dalla circostanza per cui venne creato un profilo sul social network Facebook denominato "LAPIDIAMO LA ROVINA FAMIGLIE" all'interno del quale giravano filmati, commenti e foto riferiti alla ragazza che ormai era diventata la sua ex amante, resasi rea di aver rivelato alla moglie dell'uomo la loro relazione.

Considerando la questione nella sua interezza, i giudici avevano affermato che la circostanza per cui foto e video ritenuti offensivi potevano essere, in qualche modo, ignorati fosse irrilevante: il danno era collegato alla circostanza per cui gli stessi contenuti offensivi fossero pubblicati e non alla circostanza per cui la donna potesse o meno vederli.

In ultima analisi, a definire la questione in modo definitivo è stata la CEDU attraverso la sentenza nr. 56867/2015 dell'11 febbraio 2020: la Corte, all'unanimità ha statuito che, in osservanza dell'articolo 3 circa il divieto di trattamenti inumani e degradanti e dell'articolo 8 che riguarda il diritto al rispetto

della vita privata (includendo anche la riservatezza della corrispondenza) : "*La cosiddetta cyberviolenza deve essere considerata a tutti gli effetti come violenza contro le donne e che, di conseguenza, le autorità nazionali non possono trattare episodi quali lo stalking via web, l'utilizzo abusivo degli account informatici di una donna da parte dell'ex marito o l'acquisizione di immagini e dati alla stregua di casi di violenza "comune", ma devono prevedere l'applicazione delle regole più stringenti".*

Alla Corte europea, nel caso a cui si faceva riferimento, si era riferita una donna rumena: l'ex marito era stato denunciato per i suoi comportamenti reiterati che integravano il reato noto come violenza domestica e anche per l'uso non consensuale dei social network della vittima, dato che era entrato impropriamente anche all'interno del personale account di Facebook della donna acquisendo foto e dati sensibili.

Il P.M. aveva disposto l'archiviazione della questione in quanto le condotte poste in essere dall'uomo non erano state considerate così gravi da determinare un intervento dell'autorità giudiziaria.

Il diffondersi della tecnologia, insieme alla diffusione di mezzi e strumenti digitali, hanno, in realtà, operato un ridimensionamento del diritto penale vigente. Basti pensare, per esempio, ad un'ordinanza restrittiva che difenda la vittima dall'essere pedinata e aggredita; ovviamente, non impedirebbe l'integrazione del reato di cyberstalking. Come ci ha chiarito, infatti, anche la Corte Europea dei diritti dell'uomo, se vogliamo fare realmente un passo in avanti, dobbiamo

imparare a distinguere tra violenza e cyberviolenza, così come tra atti persecutori, per così dire, comuni e la nuova fattispecie di cyberstalking.

4.2 Come combattere e prevenire il *revenge porn*

Il fenomeno del revenge porn, come già detto, in qualche modo, riflette l'attuale società, fortemente caratterizzata da una pregnante diseguaglianza di genere: è come se l'universo maschile volesse trovare nuovi modi per punire le ex partner, danneggiando la loro reputazione e ricercando strumenti per umiliarle.

Come se le donne dovessero subire una punizione, dopo essersi macchiate del peccato di aver desiderato troncare, in modo volontario, la relazione sentimentale.

Allo stesso modo, tutto ciò che è conseguente a questo reato sembrerebbe danneggiare maggiormente le donne proprio a causa del retaggio maschilista che riflette i pensieri non solo del sesso maschile, ma anche dello stesso gentil sesso.

Colpevolizzare una vittima di stupro per l'abbigliamento indossato mentre si verificava la fattispecie criminosa è come, quindi, dare giustificazione ai contenuti sessualmente espliciti prodotti senza il consenso della persona perseguitata.

Sono due facce della medesima medaglia, la violenza di genere: una questione culturale e profondamente radicata.

Come già riportato all'interno dell'elaborato, l'art 612 ter comincia con la clausola " *Salvo che il fatto costituisca più grave reato"* : tale precisazione appare d'obbligo, dato che il comportamento descritto nelle ipotesi, per così dire,

ordinarie si intersecano con altri reati. Anzitutto, quindi, potrebbe risultare utile operare delle precisazioni sul modo in cui viene data applicazione alla clausola citata poc'anzi.

Come sappiamo, è stata la legge 69 del 2019 ad introdurre questo nuovo comma per cercare di fornire un'adeguata e reale protezione a chi è costretto a subire, ormai quasi quotidianamente, la diffusione di contenuti sessualmente espliciti: prima del 2019, purtroppo, non vi era una risposta normativa a quella che ormai è divenuta una piaga sociale a tutti gli effetti.

Però, va operata una riflessione: quanto sarebbe utile, piuttosto che combatterlo, cerca di prevenirlo a monte?

Sarebbe proficuo, anzitutto, cercare di evitare, per quanto possibile, la condivisione di contenuti sessualmente espliciti, o comunque, intimi.

Il miglior metodo per proteggersi da questi tipi di atteggiamenti e di offese è evitare di pubblicare sul web foto e video intime: anche qualora ci fosse un rapporto solido di fiducia, inoltrare contenuti di questo tipo equivale ad esporsi ad un rischio non indifferente, soprattutto a causa della presenza di hacker che potrebbe sottrarre filmati e fotografie senza alcun consenso.

In un mondo utopistico, ci si potrebbe affidare in modo incondizionato al proprio compagno o ai propri amici: la verità, nuda e cruda, è che troppo spesso chi si rende reo della fattispecie criminosa in esame è proprio la persona con cui si intrattiene una relazione.

Per avere una protezione ancor più certa, in realtà, sarebbe veramente vantaggioso evitare di possedere sui propri *device* e *personal computer* filmati e

fotografie intime, proprio per i motivi citati poc'anzi: potrebbe finire in possesso di qualcuno che li utilizza in modo illecito e improprio.

Basti pensare a quello che è accaduto a moltissime celebrità nel corso del tempo: si sono spesso ritrovate a dover dover affrontare situazioni veramente paradossali perché hacker esperti avevano violato i loro dispositivi e avevano avuto accesso a dati personali.

L'unico mezzo, però, realmente proficuo al fine di combattere e prevenire il revenge porn è il seguente: essere minacciati dalla pena, affiancando il tutto a strumenti che provengono dalla disciplina civilistica, aventi carattere inibitorio e a iniziative sociali che provengano da associazioni o famiglie, ad esempio.

La circostanza per cui, una volta pubblicati i contenuti, ne rimane sempre traccia sul web causa un danno a livello d'immagine, ma anche un danno di tipo psicologico particolarmente rilevante: per questi motivi, l'intervento da mettere in atto dev'essere anzitutto di carattere penale.

Gli strumenti amministrativi, così come quelli civili, se utilizzati da soli, risultano inadeguati: un'ingiunzione deliberata dal giudice civile può sì portare alla rimozione del contenuto sessualmente esplicito da un particolare sito internet, come dimostrato nel caso di *Tiziana Cantone*, ma non si dimostra capace di contrastare che lo stesso contenuto possa essere pubblicato su un altro sito, anche da un utente diverso, non ancora punito. Anche cercare di aumentare, in sede amministrativa, la collaborazione e la cooperazione con i *providers* potrebbe rivelarsi un rimedio poco pratico.

4.3 Contrastare i risvolti negativi del *deepfake*

Abbiamo precedentemente descritto, nel capitolo dedicato al *deepfake*, alcuni degli effetti negativi che potrebbero derivare da un suo utilizzo errato.
Proprio sugli effetti negativi che possono scaturire, alcuni autori, hanno espresso profonda preoccupazione.
Ad esempio, un Professore universitario della California, Hany F., ha espresso la sua perplessità nei confronti del lavoro svolto da molti ricercati, i quali, dovrebbero prestare una maggiore attenzione riguardo la veridicità dei dati analizzati per la futura pubblicazione di ricerche accademiche.

A tal proposito, lo stesso professore si è attivato in prima persona per la creazione di metodologie atte ad individuare e contrastare l'uso del *deepfake*. Tuttavia, sottolinea come non solo sia difficile riuscire ad individuare una situazione *fake*, ma il problema si acuisce anche a causa della velocità dello sviluppo tecnologico e dei cambiamenti che avvengono nella vita sociale.

Questa situazione porta conseguenzialmente a due possibili strade: le persone saranno portate a credere a tutto il materiale condiviso, *fake* o meno, oppure, si potrebbe verificare lo scenario opposto. A tale fenomenologia, la ricercatrice Ovadya , ha dato il nome di "apatia della realtà", andando a sottolineare che la minaccia maggiore non è quella proveniente dai soggetti vittima di informazioni

fake ,ma da coloro che considerano tutte le informazioni provenienti da qualsiasi fonte (anche da fonti istituzionali), come informazioni non veritiere.

Anche Danielle Citron, docente di diritto della Boston University, si è occupata fin da subito del fenomeno del *deepfake* e dei conseguenti rischi negativi sulla società, sia da un punto di vista politico, sia, in maniera maggiore, da un punto di vista della violazione dei diritti delle donne a causa del *deepfake*, affermando che "*Quando nulla è vero, la persona disonesta prospererà dicendo che ciò che è vero è falso*".

Nello specifico, la minaccia del *deepfake* è ancora maggiore poiché è ancora più difficile riuscire a riconoscerli, rispetto alla *fake* news. I primi ad essere messi sotto indagine sono i giornalisti che, non solo devono *in primis* effettuare un processo di selezione dei documenti reali da quelli fasulli, ma devono anche fare i conti con la scarsa fiducia che i cittadini ormai hanno verso il materiale pubblicato.

Un altro settore che risente della minaccia derivante da un uso negativo del *deepfake*, è sicuramente il campo della sicurezza informatica e le relative frodi fiscali a cui può andare incontro. Ad esempio, si potrebbero creare falsi video o audio, per sabotare qualcuno dell'azienda, ricattarlo o per carpire informazioni private e non condivisibili.

Di recente è stato anche scoperto un sito web che, attraverso l'uso di *deepfake*, cerca di sottrarre criptovalute alla vittima.

Inoltre, anche i personaggi famosi, possono essere vittima del *deepfake* con l'obiettivo di usare la loro immagine per finalità politiche. Ne è un esempio quanto avvenne nel 2019, quando fu pubblicato in rete un falso video di due artisti britannici in compagnia di Mark Zuckerberg, *Chief Executive Officer* di Facebook e altre piattaforme digitali, nel quale il CEO dichiarava di aver messo in piedi un'organizzazione in grado di prendere il controllo di una miriade di dati di milioni di utenti nel mondo, con finalità manipolative, soprattutto in prospettive future[21].

Da un punto di vista politico, infatti i *deepfake* sono definiti come "una grave minaccia per la nostra società, il sistema politico e le imprese"[22] a causa dei loro risvolti negativi su molteplici fronti. Un esempio di *deepfake* che ha colpito la politica italiana risale al 2019, quando in rete venne pubblicato un video di Matteo Renzi atto a prendersi burla di alcuni membri della politica italiana.
Proprio in quello stesso anno, anche il Senato della Repubblica, ha affrontato il tema delle minacce derivanti da un uso improprio del *deepfake* e ha cercato delle metodologie atte a fronteggiarle:

[21] Arcangelo Rociola, Il finto video in cui Zuckerberg dice di avere il controllo delle nostre vite, AGI-Agenzia Italia, giugno 2019
[22] Westerlund M., The emergence of deepfake technology: a review, Technology Innovation Management Review, 9(11) : 40-53, 2019

"I deepfake, cui è dedicato appunto questo convegno, altro non sono se non il prodotto finale della contaminazione tra Intelligenza Artificiale e dati sensibili utilizzata a fini illeciti. Una nuova e assai temibile minaccia che, nel prossimo futuro, rischia di trasformare l'ecosistema digitale in un mondo nel quale riuscire a distinguere ciò che è vero da ciò che è falso risulterà sempre più arduo. Manipolare al computer, partendo da semplici fotografie e video, i volti, la voce e i movimenti delle persone per creare narrazioni visive molto realistiche con un'aderenza totale delle parole al labiale: le possibili conseguenze di un uso illegittimo della tecnologia deepfake sono angosciose, se pensiamo alla possibilità - già in effetti sperimentata - di creare falsi video in cui politici o personaggi pubblici fanno delle affermazioni in grado di cagionare conseguenze di un certo peso"[23]

Da qui, si è evidenziata la necessità di regolamentare da un punto di vista della legge, e la conseguente necessità di educare, soprattutto i nativi digitali, ad un uso responsabile di internet e del materiale in esso contenuto.

Quanto detto, ci consente di affermare che vengono attuate almeno quattro modalità per fronteggiare il d*eepfake*:

[23] La minaccia del deepfake: come affrontarla in Italia? Discorso pronunciato nella Sala Koch di Palazzo Madama il 9 dicembre 2019

- da un punto di vista legislativo, con l'attuazione di legislazioni specifiche;
- da un punto di vista aziendale, grazie alla creazione di politiche aziendali adatte;
- attraverso un lavoro di prevenzione e responsabilizzazione, rivolta, soprattutto ai giovani;
- attraverso la creazione di software anti *deepfake*.

Proprio in merito all'ultimo ambito descritto, un esempio, può essere il lavoro svolto da un centro Faculty di Londra, che si sta impegnando al fine di creare una vasta gamma di dati per elaborare poi un software automatico, in grado di riconoscere la veridicità o meno di un video.

Inoltre, anche Microsoft sta lavorando ad uno strumento che consenta di generare in maniera percentuale, il livello di autenticità di qualsiasi video caricato: tale strumento, però, non appare del tutto affidabile.

Anche i ricercatori dell'università di Buffalo[24], hanno elaborato uno strumento informatico in grado di aiutare a riconoscere i *deepfake*: tale software si basa sull'analisi dei riflessi di luce che si producono negli occhi dei soggetti. Questo perché, quando osserviamo qualcosa, nei nostri occhi si produce un riflesso dello stesso oggetto, cosa che invece non accade nel caso delle immagini generate da intelligenza artificiale. Tuttavia, uno dei principali limiti di tale sistema è che esso

[24] Bankead M., How to spot deepfakes? Look at light reflection in the eyes, University at Buffalo, 2021

funziona solo in presenza di una notevole quantità di luce, necessaria per produrre un riflesso nella cornea, e che siano ben visibili entrambi gli occhi.

In ambito italiano, i ricercatori accademici stanno lavorando anche loro al fine di progettare una strumentazione adeguata a combattere il fenomeno del *deepfake.* Nello specifico, le università di Trento e Firenze, collaborano, da ottobre 2020, al progetto Unchained[25] , finanziato dal Dipartimento della Difesa degli Stati Uniti. Le università italiane si occupano di due ambiti differenti: difatti, mentre quella di Firenze si focalizza di più sull'analisi del formato, quella di Trento analizza in modo più specifico il contenuto del materiale. Come riportato all'Ansa[26], la ricerca di Trento, guidata da Giulia Boato *"consiste nello sviluppare algoritmi, basati sia su analisi statistiche sia su paradigmi di deep-learning, adatti a scandagliare e ripercorrere tutta la catena del dato multimediale. L'investigazione forense ha bisogno della ricostruzione complessiva. Solo così possiamo dare un supporto ai servizi di intelligence, per la polizia postale e per tutti gli attori preposti a tracciare contenuti falsi e malevoli".*

Altri ricercatori e docenti italiani impiegati soprattutto nell'ambito dell'ingegneria dell'informazione, si sono trovati concordi nell'affermare che, se ripensiamo al fenomeno del *deepfake* di 10 anni fa, ci sono stati numerosi cambiamenti, come,

[25] Le Università di Trento e Firenze contro il deepfake. Rilevare in rete contenuti multimediali manipolati e diffamatori, redazione ANSA, 2020
[26]https://www.ansa.it/toscana/notizie/2020/10/27/le-universita-di-trento-e-di-firenze-contro-il-deep-fake_e5f7aea9-a0ca-4472-9b16-9170ee5310a8.html

ad esempio, il fatto che esso non riguardi più solo le immagini, ma anche i video siano oggetto di materiale *deepfake*.

Appare quindi necessario, cercare di creare software in grado di aiutare le persone a riconoscere ciò che esiste di veritiero da ciò che invece è frutto della realtà digitale.

In attesa di un supporto tecnologico affidabile, sarebbe opportuno avere un approccio più critico verso il materiale proposto, ma, è importante, non avere un approccio marcatamente critico.

Per fronteggiare tale ulteriore problematica che potrebbe generarsi come una reazione a catena, è necessario, come detto, dare più importanza ai progetti di prevenzione e sensibilizzazione.

Al momento, sostanzialmente, si può dire che i *deepfake* sono una minaccia alla libertà di informazione e condivisione di materiale online.

CONCLUSIONI

Il presente elaborato di tesi si è focalizzato sullo sviluppo del fenomeno dello stalking, nel mondo telematico.

La scelta di affrontare questa tematica è stata dovuta al periodo storico che in questi due anni ha colpito il mondo intero: la pandemia da Covid-19.

Durante questo periodo, ho avuto modo di restare disconnesso dal mondo reale a favore di un aumento esponenziale del mio tempo passato nel mondo online, che ha portato ad imbattermi in storie e racconti di abusi e violenze, condivisi in rete, avvenuti sia nel mondo reale, sia in quello cybernetico.

L'imposizione dei lock-down ha portato ingenti conseguenze anche nella casistica degli episodi di abuso: infatti, prendendo in esame alcuni studi condotti nella prima fase della pandemia, ossia da marzo a giugno del 2020, sono stati rilevati aumenti nei numeri degli episodi di abuso domestico e, purtroppo, sono state registrate 58 vittime di omicidio in ambito familiare.

Tutto ciò, mi ha incentivato nel voler approfondire tali tematiche sotto più sfaccettature, in quanto si avvicinavano molto anche al mio percorso di studio.

Il normale svolgimento della vita quotidiana può essere alterato dall'essere vittima di azioni di stalking e, l'enorme sviluppo della tecnologia, non ha fatto altro che aumentare la diffusione di questa vicenda, portando anche alla creazione di nuove sottocategorie attuabili online.

Spetterebbe all'ambito giuridico attivarsi in maniera maggiore non solo nel sanzionare i carnefici di questi reati, ma nell'attuazione di norme più dure al fine di prevenire anche lo svilupparsi dello stalking, online e offline.

La prima considerazione da fare è che la fattispecie criminosa rappresenta un tema articolato molto diversamente a seconda dell'ordinamento di appartenenza: si passa da Paesi che non ne fanno menzione a Stati che lo disciplinano in larga misura e dettagliatamente.

Inoltre, una grande attenzione, andrebbe posta sui nativi digitali e dunque sarebbe opportuno portare alla creazione di progetti negli ambienti scolastici per promuovere un processo di sensibilizzazione.

Dunque, i rischi a cui, però, potremmo essere esposti sono i seguenti:

- un'eccessiva demonizzazione delle tecnologie, dato il loro utilizzo indebito e illecito;
- la redazione di norme già obsolete in partenza a causa dell'evoluzione costante e progressiva della tecnologia.

Quindi, in conclusione, potremmo dire che la tecnologia ha i suoi risvolti positivi così come quelli negativi: prendendo in prestito le parole del filosofo Aristotele, *in medio stat virtus*.

RINGRAZIAMENTI

Desidero ringraziare il prof. Armando PALMEGIANI, relatore di questa tesi, per la grande disponibilità e cortesia dimostratami, apprezzando sin da subito il progetto proposto.

Grazie ai miei genitori, per essere stati un costante sostegno durante il mio percorso di studi e per come mi avete educato e sorretto in ogni momento. Grazie per non avermi permesso di arrendermi.

Ringrazio Lucia, la mia dolce metà, che ha sempre creduto in me e non mi ha mai posto vincoli di alcun tipo, lasciandomi la responsabilità delle mie scelte.

Desidero infine ringraziare i miei piccoli Giovanni e Nathan, stabili spettatori dei miei sacrifici, senza mai lamentare il tempo a loro sottratto. Spero almeno un giorno di poter dare proprio a voi lo stesso dolce ed instancabile sostegno, perché possiate crescere e raggiungere quanto prima questo meraviglioso traguardo.

BIBLIOGRAFIA

- Radford A., Wu J., Child R., Luan D., Amodei D. , Sutskever I., Language models are unsupervised multitask learners". In: OpenAI Blog 1.8, 2019.
- Angelides, S., 'Technology, hormones, and stupidity': The affective politics of teenage sexting. Sexualities, 16, 665-689, 2013
- Argyriou E, Um M, Wu W, Cyders MA. Measurement Invariance of the UPPS-P Impulsive Behavior Scale Across Age and Sex Across the Adult Life Span. Assessment. 2020
- Attrill-Smith e Wesson, The Psychology of Cybercrime, The Palgrave Handbook of International Cybercrime and Cyberdeviance, pp 653-678, 2020
- Bates, S., Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. Feminist Criminology, 12(1), 22-42, 2017
- Bergonzi Perrone, Marcello, La nuova figura del cyberstalking, Stem Mucchi Editore, 2010
- Bond E., 2016, Sexting, Criminology and Criminal Justice, 2016
- Bond, E. , The mobile phone = bike shed? Children, sex and mobile phones. New Media & Society, 13, 587-604.2010
- Brenner, M. E. . Interviewing in Educational Research. In J. Green, G. Camilli, & P. B. Elmore (Eds.). Handbook of Complementary Methods in Education Research (pp. 357-370). Washington DC: American Educational Research Association, 2006

- Buckels et al., The Nexus of the Dark Triad Personality Traits With Cyberbullying, Empathy, and Emotional Intelligence: A Structural-Equation Modeling Approach,Front Psychol, 2021
- Cavezza C., McEwan Troy E., Cyberstalking versus off-line stalking in a forensic sample, Psychology, Crime & Law, Volume 20, Number 10, pp. 955-970, p. 958, 2014
- Citron, D. K., & Franks, M. A. Criminalizing revenge porn. Wake Forest Law Review, 45, 101-140, 2014
- Citron, Danielle Keats and Franks, Mary Anne, Criminalizing Revenge Porn (May 19, 2014). Wake Forest Law Review, Vol. 49, 2014, p. 345+, U of Maryland Legal Studies Research Paper No. 2014-1
- Clare McGlynn, Erika Rackley, Image-Based Sexual Abuse, Oxford Journal of Legal Studies, Volume 37, Issue 3, Autumn 2017, Pages 534–561
- Cupach William R., Spitzberg Brian H., Attrazione, ossessione e stalking, Astrolabio Ubaldini Editore, 2011.
- Cupach, W.R., & Spitzberg, B.H., The dark side of relationship pursuit. From attraction to obsession and stalking. Mahwah (NJ): Lawrence Erlbaum Associates, 2004
- DeKeseredy WS, Schwartz MD. Thinking Sociologically About Image-Based Sexual Abuse: The Contribution of Male Peer Support Theory. Sexualization, Media, & Society. December 2016
- Diaz R., Garofano L., I labirinti del male, Infinito Edizioni, 2013, p. 66.
- Döring, N., Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting? Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8(1), Article 9, 2014

- G.M. Galeazzi, P. Curci, The tormenting harasser syndrome (stalking): a review, 2001
- Giangrande A., Anno 2021, La Giustizia Prima parte, Volume 232 di L'Italia del Trucco, l'Italia che siamo, Giangrande, 2021
- Glenn, M. Sellbom, Theoretical and empirical concerns regarding the dark triad as a construct, Psychology Journal of personality disorders, 2015.
- Hayes et al., Criminal Justice in America. Third Edition. Teacher's Guide, 2000.
- Hutchings, A., & Hayes, H. . Routine activity theory and phishing victimisation: who gets caught in the 'net'?. Current Issues in Criminal Justice, 20(3), 433-452., 2009
- Kalaitzaki, Argyroula. "Cyberstalking Victimization and Perpetration Among Young Adults: Prevalence and Correlates." Recent Advances in Digital Media Impacts on Identity, Sexuality, and Relationships, edited by Michelle F. Wright, IGI Global, 2020, pp. 22-38.
- Karaian, L. , Policing 'sexting': Responsibilization, respectability and sexual subjectivity in child protection/crime prevention responses to teenagers' digital sexual expression. Theoretical Criminology, 18, 282-299, 2014
- Kate Walker, Emma Sleath, A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media, Aggression and Violent Behavior, Volume 36, 2017
- Kircaburun, K., Jonason, P.K. & Griffiths, M.D.. The Dark Tetrad traits and problematic social media use: The mediating role of cyberbullying and cyberstalking. Personality and Individual Differences, 135, 264-269, 2018

- Lee, M., & Crofts, T., . Gender, pressure, coercion and pleasure: Untangling motivations for sexting between young people. British Journal of Criminology, 55, 454- 473, 2015
- Marganski, A., & Melander, L., Intimate partner violence victimization in the cyber and real world: Examining the extent of cyber aggression experiences and its association with in-person dating violence. Journal of Interpersonal Violence, 2015
- Ménard, Kim S., and Aaron L. Pincus. "Predicting overt and cyber stalking perpetration by male and female college students." Journal of Interpersonal Violence 27.11 : 2183-2207, 2012
- Minnella C., Lo stalking tra criminologia, giurisprudenza e recenti modifiche normative, Rassegna
- Morelli, M., Bianchi, D., Baiocco, R., Pezzuti, L., & Chirumbolo, A.. Not-allowed sharing of sexts and dating violence from the perpetrator's perspective: The moderation role of sexism. Computers in Human Behavior, 2016 a
- Nitish Shirish Keskar, Bryan McCann, Lav R Varshney, Caiming Xiong, and Richard Socher. \Ctrl: A conditional transformer language model for controllable generation", 2019.
- Pathè M., Mullen P. E. , The impact of stalkers on their victims, 2018
- Patrick, K., Heywood, W., Pitts, M. K., & Mitchell, A., Demographic and behavioral correlates of six sexting behaviors among Australian secondary school students. Sexual Health, 12, 480-487, 2015
- penitenziaria e criminologica, 2013

- Priebe, G., & Svedin, C., Online or off-line victimization and psychological wellbeing: A comparison of sexual-minority and heterosexual youth. European Child & Adolescent Psychiatry, 21, 569-582, 2012
- Reed, L. A., Tolman, R. M., & Ward, L. M,. Snooping and sexting: Digital media as a context for dating aggression and abuse among college students. Violence Against Women, 2016
- Rothkopf J., Deepfake Technology Enters the Documentary World. The New York Times, 2020
- Rowan Zellers, Ari Holtzman, Hannah Rashkin, Yonatan Bisk, Ali Farhadi, Franziska Roesner, and Yejin Choi. \Defending Against Neural Fake News", 2019
- Scott R. Stroud, The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn, Journal of Mass Media Ethics, 29:3, 168-183,2014
- Smoker, M., & March, E., Predicting perpetration of intimate partner cyberstalking: Gender and the Dark Tetrad. Computers in Human Behavior, 72, 390–396, 2017
- Smoker, M., & March, E., Predicting perpetration of intimate partner cyberstalking: Gender and the Dark Tetrad. Computers in Human Behavior, 72, 390–396, 2017
- Thompson, M. P., & Morrison, D. J., Prospective predictors of technology-based sexual coercion by college males. Psychology of Violence, 3, 233-246, 2013
- Van Ouytsel, J., Walrave, M., & Van Gool, E,. Sexting: Between thrill and Fear - How schools can respond. Clearing House, 87, 204-212, 2014

- Yar M., The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory, European Journal of Criminology, 2005
- Ziccardi G., Cyberstalking e molestie portate con strumenti elettronici: aspetti informatico-giuridici, Rassegna Italiana di Criminologia, 2011

SITOGRAFIA

- https://www.researchgate.net/figure/Baccarella-et-al-2018s-dark-side-of-social-media-functionality-theory_fig4_330938206
- https://link.springer.com/article/10.1007/s10611-007-9063-7
- https://www.researchgate.net/publication/238433587_The_Novelty_of_'Cybercrime'An_Assessment_in_Light_of_Routine_Activity_Theory
- https://www.buffalo.edu/news/releases/2021/03/010.html
- https://www.theguardian.com/technology/2014/may/22/revenge-porn-victims-boost-german-court-ruling
- https://www.ansa.it/toscana/notizie/2020/10/27/le-universita-di-trento-e-di-firenze-contro-il-deep-fake_e5f7aea9-a0ca-4472-9b16-9170ee5310a8.html