

INDICE SOMMARIO

Introduzione.....	4
-------------------	---

CAPITOLO I:

IL REATO DI REVENGE PORNOGRAPHY - UN FENOMENO IN PROGRESSIVA ESPANSIONE NELLA SOCIETA' ATTUALE

1. Il ruolo della rete nel contesto attuale: un mezzo di commissione dei reati.....	9
1.1 La responsabilità del <i>Provider</i> del servizio <i>Internet</i> : Teorie e nuovi risvolti.....	12
1.2 L'utilizzo dei <i>Social Network</i> per finalità illecite.....	16
2. Da dove deriva il termine "Revenge Porn"? Analisi terminologica e concettuale della fattispecie.....	21
3. La mancanza del consenso e gli effetti sulla vittima di <i>Revenge Porn</i>	24
3.1 Il caso di Tiziana Cantone.....	32
3.2 Internet e Revenge Porn: pericoli e insidie per i minori.....	39
3.3 Le nuove sottocategorie di Revenge Porn e i fenomeni ad esso associati...	45
4. Le figure di reato che venivano applicate prima della Riforma del Codice Rosso.....	53
4.1 Il reato di Diffamazione.....	54
4.2 art. 167 d.lgs. 196/2003.....	58
4.3 Atti persecutori.....	62
4.4 Sostituzione di persona.....	65
4.5 Violenza sessuale.....	66
4.6 Diffusione di riprese e registrazioni fraudolente.....	69
5. Iter legislativo anteriforma del 2019.....	71
5.1 La prima Proposta di legge di Revenge Porn.....	73
5.2 La seconda e la terza Proposta di legge.....	75

CAPITOLO II

IL CODICE ROSSO E L'INTRODUZIONE DELL'ART. 612 TER

1. Riforma del 2019 - il Codice Rosso e le novità di recente introduzione.....	78
--	----

1.1 Modifiche e novità introdotte dalla riforma del Codice Rosso, dal punto di vista procedurale.....	82
2. L'articolo 612ter, il delitto di diffusione illecita di immagini o video sessualmente espliciti.....	88
2.1 La clausola di salvaguardia ed il concorso di reati.....	91
2.2 La pluralità di condotte incriminate nell'articolo di diffusione illecita di immagini sessualmente esplicite.....	92
2.3 L'oggetto della condotta dell'articolo 612ter - cosa si intende per 'immagini a contenuto sessualmente esplicito'?.....	96
2.4 Il concetto di "Nocumento" nel reato di <i>Revenge porn</i>	98
2.5 Le circostanze aggravanti e il maggior disvalore penalistico in base alla qualità della persona offesa.....	101
2.6 Il regime di procedibilità.....	104
2.7 <i>Revenge porn</i> - una disciplina volta alla tutela dei diritti fondamentali della persona.....	107
3. Casi Giurisprudenziali - risoluzione degli episodi di <i>Revenge porn</i> nella prassi.....	116
4. La fattispecie negli ordinamenti stranieri - Come viene regolamentato il <i>Revenge Porn</i> all'estero?.....	121
4.1 La criminalizzazione negli Stati Uniti.....	124
4.2 La criminalizzazione in Germania e Francia: i casi più rilevanti.....	129
4.3 Come viene trattato il <i>Revenge porn</i> in Spagna? Evoluzione normativa ed esperienze giurisprudenziali.....	131
4.4 La criminalizzazione in Giappone.....	133

CAPITOLO III

COME L'INTELLIGENZA ARTIFICIALE PUO' INSINUARSI NEL REATO DI REVENGE PORNOGRAPHY – NUOVE PROSPETTIVE APPLICATIVE DI PREVENZIONE E MODALITA' DI COMMISSIONE DEI REATI

1. Intelligenza Artificiale – nozioni generali e normative applicabili.....	135
1.1 L'Intelligenza Artificiale: uno strumento in rapida ascesa.....	136
1.2 Come nasce l'Intelligenza Artificiale?.....	143
1.3 L' <i>AI Act</i> : Il primo regolamento al mondo sull'Intelligenza artificiale.....	146
1.4 GDPR e <i>AI act</i> : la tutela dei dati personali, chi se ne occupa?.....	151
1.5 L'Intelligenza Artificiale e i rischi per i Diritti fondamentali, innovazione o pericolo?.....	155

2. AI come mezzo di prevenzione e repressione dei reati - Applicabilità al <i>Revenge porn</i>	159
2.1 La funzione preventiva dei reati – la teoria della pena.....	160
2.2 Il fenomeno del <i>Revenge porn</i> , come le piattaforme <i>online</i> vogliono utilizzare l'Intelligenza Artificiale in chiave preventiva.....	162
3. Intelligenza Artificiale come mezzo di commissione dei reati.....	173
3.1 Come è nato il termine Deepfake? Storia, funzionamento ed evoluzione giuridica.....	175
3.2 Il <i>Deepnude o porno deepfake</i> – criminalizzazione e punti di contatto con la fattispecie del <i>Revenge porn</i>	182
3.3 responsabilità penale dei reati - uomo o macchina?.....	190
3.4 Deepfake: come proteggersi? Strumenti utili per il rilevamento, prevenzione e contrasto a questo fenomeno.....	193
 Considerazioni finali– <i>Revenge Porn</i> e Intelligenza Artificiale.....	 196
BIBLIOGRAFIA.....	211
INDICE GIURISPRUDENZA.....	224

INTRODUZIONE

Il presente elaborato ha come obiettivo quello di indagare e approfondire il reato del Diffusione illecita di immagini o video sessualmente espliciti, articolo 612ter, collocato nel libro secondo, titolo XII incentrato sui delitti contro la persona, capo III («Dei delitti contro la libertà individuale»), sezione III, dedicata ai delitti contro la libertà morale, del Codice penale.

Il fine di questa analisi è quello di mettere in relazione questa fattispecie all'utilizzo dell'Intelligenza Artificiale, come metodologia di attuazione del reato, ma anche come strumento di prevenzione utile per il legislatore.

Inizialmente, verrà effettuata una digressione generale al fine di capire al meglio tutti gli elementi circostanziali al reato di diffusione illecita di immagini sessualmente esplicite, per arrivare poi a descrivere nei capitoli successivi la fattispecie oggetto d'esame.

Definiremo, dunque, in che modo la tecnologia si è sviluppata come uno strumento, nel corso degli anni, sempre più imprescindibile nel vivere quotidiano di ogni persona, e come quest'ultima possa essere uno strumento molto pericoloso di commissione dei reati.

Infatti, sebbene il diritto alla circolazione in rete venga visto come fondamentale per l'individuo, sottolinea la Dichiarazione dei diritti di *Internet*, il legislatore deve comunque assicurare una gestione e un bilanciamento della libertà di navigazione con i diritti che riguardano l'immagine, la privacy ecc, in modo tale da rendere la rete un "luogo" sicuro per il cittadino.

Affinché possa vigere il rispetto dei diritti e della dignità *online* è necessario evidenziare, in caso di reati commessi con l'utilizzo della rete, la responsabilità dei gestori dei più importanti siti internet, considerando le varie teorie di Dottrina e Giurisprudenza sui cosiddetti "*provider*" dei servizi.

Ai fini di una più corretta analisi, va ricordato l'importante ruolo che occupa in materia la legislazione europea, come la direttiva *e-commerce*, ma anche i casi di spicco che hanno aiutato al consolidamento della disciplina, per esempio *Google vs. Vividown*.

In seguito, ci concentreremo sul ruolo che i *social network* hanno avuto nella commissione dei reati contro la persona, come anche il reato oggetto di studio, la diffusione illecita di immagini o video sessualmente espliciti: primariamente i siti più utilizzati sono *Facebook*, *Instagram*, *X*, *Telegram*, ma anche molti altri.

Questi, col tempo si sono adattati a nuove metodologie sempre più avanzate per la tutela dei diritti del cittadino; Meta, che ha istituito, anche grazie all'aiuto dell'Intelligenza Artificiale, piattaforme apposite di segnalazione dei reati, ai fini di una più rapida rimozione dei contenuti illeciti.

Successivamente, verrà dato ampio spazio alla definizione formale e alla nascita della fattispecie di reato di diffusione illecita di immagini sessualmente esplicite,

analizzandone l'uso terminologico, le caratteristiche sia normative che le evoluzioni sviluppatasi grazie all'avanzare tecnologico, analizzando il *quomodo* della opinione giurisprudenziale.

Nel corso dell'analisi verranno eseguiti paragoni con gli ordinamenti esteri in modo tale da avere una visione più ampia del reato e al fine di comprendere in toto il *quid* che ha portato allo sviluppo della Riforma del Codice Rosso, introdotta nel 2019.

In particolare, verrà trattata la disciplina inglese, come punto di partenza dal quale verrà condotta l'approfondimento sul *Revenge porn*, poiché è proprio lì che per la prima volta viene utilizzato questo neologismo.

Ci occuperemo di confrontare le due fattispecie, sia a livello terminologico che sul piano normativo, evidenziando le differenze principali e i punti di contatto con l'articolo 612ter, oggetto del mio studio.

Verrà descritto in particolare il reato di *Revenge porn* nel nostro codice penale, considerando anche i suoi elementi fondanti: tra questi, la mancanza di accettazione della vittima alla diffusione del contenuto sessualmente esplicito e i potenziali effetti, anche di carattere psicologico, lavorativo e relazionale che può provocare un evento dalla portata diffusiva così potenzialmente ampia.

Oltre a citare episodi Giurisprudenza nazionale ed estera, verranno trattati anche avvenimenti realmente accaduti e interviste rilasciate dalle vittime stesse.

Passeremo poi a descrivere alcuni dei casi fondamentali, che hanno necessariamente portato il legislatore a legiferare in materia il più celermente possibile: il caso di Giulia Sarti e il caso di Tiziana Cantone.

Due episodi, in particolare quello di Tiziana Cantone, che hanno segnato l'Italia e che hanno portato al bisogno urgente di una legge che criminalizzasse la condotta di diffusione non autorizzata di contenuti sessualmente espliciti, facendo sì che il nostro ordinamento si adeguasse agli standard di tutela degli altri Paesi.

Dopo di che, ci soffermeremo sui danni che *internet* e i *social network* potrebbero provocare nei confronti dei minori, se non adeguatamente controllati, e il crescente utilizzo dei *social*, da parte di questi ultimi, per commettere reati contro la persona, il più delle volte, reati di carattere sessuale: *Revenge Porn*, abusi sessuali che vengono ripresi e caricati online, *cyberstalking*, *cyberbullismo*, concentrandomi anche sulle modalità di prevenzione dei suddetti.

Illustreremo anche tutte le fattispecie che oggi vengono associate al *Revenge porn* e che ne costituiscono una sottospecie: come il *sexting*, il *doxing*, il *sextorsion*.

Tutte condotte altamente diffuse soprattutto tra i giovani, che il legislatore non ha ancora regolamentato in via esclusiva, ma che si possono collegare ad altre fattispecie di reato, e per il quale si auspica al più presto un intervento in materia.

Nel quarto paragrafo, saranno presentate tutte le fattispecie di reato che venivano applicate e accostate a questo reato, precedentemente all'entrata in vigore dell'articolo 612 ter, e della riforma del Codice Rosso.

Saranno trattati in particolare, il reato di Diffamazione articolo 595 c.p., il reato di illecito trattamento dei dati personali all'articolo 167 d.lgs. 196/2003 (GDPR), la

disciplina di atti persecutori articolo 612 bis, la sostituzione di persona articolo 494 c.p., il reato di violenza sessuale articolo 609 c.p., la diffusione di riprese e registrazioni fraudolente articolo 617 septies c.p.

In seguito, descriveremo, passo a passo, l'iter legislativo che ha portato alla nascita della Riforma, andando nel dettaglio delle prime proposte e delle reazioni del Parlamento a queste ultime, citando anche alcuni interventi di spicco.

Nel secondo capitolo invece, sarà introdotta la riforma del Codice Rosso e le novità di carattere procedurale, le nuove funzioni degli organi più rilevanti del sistema, passando anche a elencare tutte le fattispecie innovative che sono entrate a far parte nel nostro ordinamento, riferendomi al panorama Europeo.

Andremo anche a descrivere la disciplina di recente introduzione, di diffusione illecita di immagini o video sessualmente esplicite, l'articolo 612 ter.

Esamineremo l'articolo passando dalle circostanze aggravanti, l'oggetto, il dolo generico o specifico, la clausola di salvaguardia, fino alla pluralità delle condotte incriminate, ma anche, dal concetto di nocumento al regime di procedibilità.

In seguito, si farà riferimento a tutti quei diritti fondamentali dell'individuo che vengono, in qualche modo, "toccati" dalla disciplina oggetto d'esame: Il diritto alla riservatezza e alla privacy, il diritto all'immagine, il diritto all'oblio e alla libertà sessuale.

Il terzo paragrafo tratterà invece di altri casi giurisprudenziali che vengono ritenuti particolarmente interessanti e meritevoli di ulteriore attenzione e analisi, al fine di mettere in luce sia i tratti positivi della normativa di recente introduzione, sia i vuoti di tutela che ancora oggi permangono e per i quali si auspica un intervento tempestivo del legislatore.

Pare anche opportuno trattare delle discipline estere e di come il *Revenge Porn* viene visto, sia al di fuori dell'Unione Europea che nei Paesi che ne fanno parte: in particolare, Francia, Germania, Spagna, ma anche negli Stati Uniti e in Giappone, citando anche "successi" normativi, come l'introduzione di una disciplina simile all'articolo 612ter, per piccoli Stati, come la Repubblica di San Marino.

Ciò proprio per sottolineare l'importanza di una tutela generale contro questo tipo di comportamenti, che possono ledere profondamente sia l'aspetto psicologico che lavorativo, ma anche sociale della persona offesa.

Nei successivi capitoli, verrà affrontato l'argomento dell'Intelligenza Artificiale, partendo dalla sua nascita e dalla sua matrice storica.

Faremo particolare riferimento all'utilizzo e agli effetti che quest'ultima potrebbe avere sulla società e sui diritti fondamentali, ricercandone al contempo gli aspetti positivi e gli eventuali possibili utilizzi in tutti gli ambiti della vita quotidiana, ma anche dal punto di vista della prevenzione e della repressione dei reati.

Citeremo le definizioni che vengono fornite da vari studiosi, esperti in materia, e dalle fonti ufficiali, come vari decreti-legge di recente introduzione, ma anche Regolamenti Europei.

Si farà riferimento alle anticipazioni di grandi autori della letteratura, che con il loro essere all'avanguardia e con un occhio sempre puntato all'avvenire, hanno previsto un futuro permeato dalla tecnologia, come Italo Calvino e Steven Hawking, che si sono interrogati sui possibili esiti di un modo di vivere “condiviso” con le macchine.

Infatti, l'IA sta talmente prendendo piede nell'uso comune che il Considerando della Risoluzione del Parlamento Europeo sulla robotica afferma che «è possibile che a lungo termine l'intelligenza artificiale superi la capacità intellettuale umana»¹.

Verrà citata giurisprudenza e Dottrina sia nazionale che internazionale, al fine di dare un quadro più completo sul futuro di questa materia, descrivendo come gli Stati si stanno attivando al fine di ordinare questi nuovi strumenti digitali.

Di spicco sono i due Regolamenti volti a tutelare i diritti personali: il Regolamento Generale sulla Protezione dei Dati (GDPR) e il Regolamento sull'Intelligenza Artificiale (AI act), vedremo infatti, come questi atti si intersecano tra loro, per fornire una tutela dei diritti fondamentali del cittadino a 360°.

Tratteremo inoltre, l'impatto negativo che potrebbe avere l'Intelligenza Artificiale sulla società, mettendo alla luce il rischio che questa possa essere utilizzata, come effettivamente sta avvenendo in tempi recenti, come metodologia di attuazione di svariati reati.

Si tratta, sia di reati contro la persona, ma anche contro enti pubblici e privati, e reati contro il patrimonio.

Sarà affrontato anche il modo in cui il *Revenge Porn* si è “evoluto” grazie a questi nuovi metodi di commissione di crimini *online*, descrivendo il fenomeno del “*deepfake*” e di come questo possa essere utilizzato ai fini della diffusione di immagini o video sessualmente espliciti, in particolare mi occuperò della crescente preoccupazione in merito al *deepnude* o *deep fake porn*.

Analizzeremo le risposte legislative, le proposte, i regolamenti, ma anche il comportamento dei *social network* più utilizzati per commettere questo tipo di reati.

Infine, si farà riferimento al *quomodo* dell'utilizzo dell'Intelligenza Artificiale come strumento utile per mettere in atto campagne nelle scuole, con la finalità di prevenire il reato di *Revenge porn*.

Concluderemo con le considerazioni in materia, facendo sicuramente affidamento sul fatto che il legislatore possa tenere il passo con l'innovazione tecnologica, non soccombendo, davanti a quella che viene definita una vera e propria “rivoluzione”².

Verranno presi in considerazione i notevoli sviluppi, sia dal punto di vista normativo, a livello nazionale, ma anche le più recenti novità introdotte sulla scena Europea.

¹ Risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

² M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. Pizzetti (a cura di), *Intelligenza artificiale*

CAPITOLO I - IL REATO DI REVENGE PORNOGRAPHY - UN FENOMENO IN PROGRESSIVA ESPANSIONE NELLA SOCIETA' ATTUALE

SOMMARIO

1. Il ruolo della rete nel contesto attuale – un mezzo di commissione dei reati 2. Da dove deriva il termine “*Revenge porn*”? Analisi terminologica e concettuale della fattispecie 3. La mancanza del consenso e gli effetti sulla vittima di *Revenge Porn* 4. Le figure di reato che venivano applicate prima della riforma del Codice Rosso 5. Iter legislativo anteriforma del 2019

Una premessa sui temi trattati nel primo capitolo

Il primo capitolo, come precedentemente descritto nella introduzione, parlerà di tutti quegli argomenti che, a mio parere, è necessario trattare, prima di far riferimento alla fattispecie di diffusione illecita di immagini o video sessualmente espliciti.

Innanzitutto, mi occuperò di tutte quelle normative a livello europeo che hanno regolamentato la commissione di reati mediante *internet*, come la Convenzione di Budapest, ma citerò anche fonti non vincolanti come la Dichiarazione dei Diritti di *Internet*.

Proseguirò poi a dare definizioni a titolo informativo, su alcuni termini fondamentali per comprendere appieno la fattispecie che andrò a trattare durante la mia analisi; infatti, lo scopo ultimo di questo capitolo è di carattere analitico-informativo.

Approfondirò varie normative, linee guida, Regolamenti Europei, che hanno portato alla costituzione di normative nazionali, come la NIS 1 (direttiva n. 1148/2016) e NIS 2 (direttiva n. 2555/2022, recepita con il d.lgs. n.138/2024).

In seguito, proseguirò citando la direttiva “E-Commerce” 2000/31, che all’articolo 14 si occupa della responsabilità dei prestatori dei servizi, i cosiddetti “*provider*”.

In questo capitolo, infatti, parlerò delle differenze tra i vari tipi di fornitori dei servizi ma anche delle due teorie che girano intorno alla loro responsabilità, soffermandomi sull’effettiva soluzione che in conclusione è stata utilizzata.

Durante la mia analisi, metterò in luce alcuni dati per comprendere appieno il livello di pericolosità che caratterizza *internet* e i *social media*, ai fini della commissione dei reati *online*, facendo riferimento ai social più utilizzati: Facebook, Whatsapp, Instagram, Telegram ecc.

Ma gli elementi fondamentali su cui si baserà il mio studio sono anche gli approfondimenti di varie sentenze che hanno posto le basi della Giurisprudenza recente, in materia di reati contro la persona commessi sul *web*; queste ultime saranno necessarie in seguito per comprendere come si è arrivati a una disciplina così necessaria e sofferta come la diffusione illecita di immagini sessualmente esplicite, all’articolo 612ter.

Analizzerò le fasi storiche di questo reato, da dove è nato e come si è evoluto, ma anche da dove deriva la terminologia comune “*Revenge porn*” e tutte le teorie e i dubbi ad essa connessi, ponendo particolare attenzione agli effetti (sia psicologici che lavorativi e patrimoniali, ma anche quelli che potrebbero verificarsi sui minori) e alla mancanza di consenso, che vengono considerati come elementi fondanti di questo reato.

Citerò il caso di Tiziana Cantone spiegando come, da questo episodio, si è arrivati alla discussione in merito alla normativa articolo 612 ter e alla sua introduzione come uno dei reati cardine della riforma del Codice Rosso, raccontando passo a passo l’iter legislativo, mettendo in luce anche la sostanziale inadeguatezza delle normative precedenti per la risoluzione di questi casi, che si stavano diffondendo a macchia d’olio.

1.0 (segue): Il ruolo della rete nel contesto attuale - un mezzo di commissione dei reati

A seguito dell’incremento significativo dell’utilizzo della tecnologia nelle relazioni economiche e sociali, sono aumentati esponenzialmente i reati perpetrati attraverso l’uso di *internet*, grazie alla rapidità con cui le informazioni vengono divulgate.

Oggi è possibile ottenere dati in tempo reale, sebbene questo da un lato sia conveniente, dall’altro potrebbe portare ad abusi.

Ciò ha generato nuove ipotesi di reato sanzionabili dal Codice penale, i cui effetti potrebbero essere ancora più devastanti per la vittima.

Per questo motivo la rete viene considerata un mezzo principale di commissione di reati, in vari settori, come i delitti contro il patrimonio e, seppur in misura minore, contro la persona.

Infatti, sono venuti ad esistenza reati “nuovi” perpetrati tramite *internet* (reati informatici in senso stretto, come il *Revenge Porn*, oggetto del nostro studio) che sono stati introdotti nel Codice penale, come l’accesso abusivo a sistema informatico, e reati che già erano criminalizzati, ma che *in rerum natura* possono anche essere commessi *online* (diffamazione, *stalking*, bullismo...) in questo caso il reato comune viene posto in essere mediante un *computer*.

A causa del carattere transnazionale dei crimini informatici, il Consiglio d’Europa nel 2001 ha deciso di dotarsi di una convenzione, di cui l’Italia si è resa firmataria nel 2008³: La Convenzione di Budapest.

Quest’ultima, come sottolinea Alexander Seger, Capo della Divisione della Criminalità informatica del Consiglio d’Europa, serve per tutelare i cittadini europei durante la loro navigazione su *Internet*, e proteggerli dai reati informatici «La Convenzione di Budapest è sinonimo di una visione di un *Internet* libero, dove le informazioni possono fluire liberamente, essere consultate e condivise, dove le restrizioni sono definite in

³ legge 18 marzo 2008 n.48

modo restrittivo per contrastare l'uso improprio e dove vengono indagati e perseguiti solo reati specifici, fatte salve le necessarie garanzie»⁴.

Obiettivi principali della Convenzione, sono una cooperazione internazionale adeguata, ma anche la criminalizzazione di condotte come, per esempio, l'accesso abusivo o la pornografia infantile, la frode informatica ecc., fornire strumenti di diritto processuale per poter contrastare la criminalità informatica e assicurare la ricerca corretta di prove digitali⁵.

All'articolo uno vengono fornite delle definizioni generali, delle quali citerò le più rilevanti per la nostra analisi: per "Service Provider" (fornitore di servizi) si intende «qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico; qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio».

"Sistema informatico" invece indica (*Infra*, § cap. 2 par. 2.3) «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati».

Nel 1996 I giudici della Corte Federale degli Stati Uniti affermavano che «il contenuto di *Internet* è vario quanto il pensiero dell'uomo»⁶ per questa ragione, vista la grande capacità di ogni persona di immettere nel sistema vari tipi di contenuti, incombeva anche a livello nazionale la necessità di tutela sia dei diritti primari dei cittadini (*infra*, § cap. 2 par. 2.2), come la libertà personale, la reputazione, libertà morale e di autodeterminazione, la libertà sessuale ecc., ma d'altro canto, anche la tutela della libertà di espressione prevista all'art 21 della Costituzione.

Per quanto concerne le fonti, di particolare rilievo in Italia è stata l'introduzione nel 2015 della cosiddetta "*Internet Bill of Rights*" una vera e propria "Dichiarazione dei Diritti di Internet", istituita presso la Camera dei deputati e pubblicata nel luglio 2015, la quale ha come obiettivo quello di definire generalmente l'uso della rete mediante linee guida, le quali, però, non hanno carattere vincolante.

Quest'ultima prevede all'articolo uno, il rispetto dei diritti fondamentali della persona (riconosciuti anche dalla Dichiarazione Universale dei diritti umani delle Nazioni Unite e dalla Carta dei diritti fondamentali dell'Unione Europea).

Considera l'articolo in esame, che questi diritti devono essere rispettati in modo tale da assicurarne l'effettivo esercizio sulla rete, al comma terzo la norma prevede che il riconoscimento dei diritti in *Internet* deve essere fondato sul pieno rispetto della

⁴ Crio Papers n. 59, Arena Marilena, La Convenzione di Budapest del Consiglio d'Europa sulla Repressione della criminalità informatica, 2021 (a cura di) Rosario Sapienza

⁵ ILARDA G., E G. MARULLO, *Cybercrime: Conferenza Internazionale. La convenzione del consiglio d'Europa sulla criminalità informatica*, Milano, 2004

⁶ US supreme Federal Court, Eastern District of Pennsylvania, 11 giugno 1996, in *Diritto dell'informazione e informatica*, 1996, 4/5, 604. La Corte dichiarò l'illegittimità costituzionale delle norme del Decency Act che punivano la diffusione di questi contenuti

dignità, della libertà, dell'eguaglianza e della diversità di ogni persona, che costituiscono i principi in base ai quali si effettua il bilanciamento con altri diritti.

All'articolo due della dichiarazione, viene posto l'accesso ad *Internet* come un vero e proprio diritto fondamentale della persona, da esercitare in condizioni di parità, non solo come possibilità di collegamento alla rete ma anche nei suoi presupposti sostanziali, con la garanzia da parte delle Istituzioni Pubbliche di intervenire per il superamento di «divari digitali», per genere, condizioni economiche, o vulnerabilità personale.

Come condizione necessaria per l'esercizio di suddetto diritto, vi è il principio di neutralità della rete, sancito dall'articolo 4 della stessa Dichiarazione «Ogni persona ha il diritto che i dati trasmessi e ricevuti in *Internet* non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuto dei dati, dispositivo utilizzato, applicazioni o, in generale, legittime scelte delle persone».

Venendo a tempi più recenti, la sicurezza e tutela dei diritti in rete è stata anche posta come uno dei principali interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR), attuato dall'Agenzia per la Cybersicurezza Nazionale (ACN), con l'obiettivo di proteggere le imprese e i dati dei loro clienti da attacchi digitali, per identificarli e ridurne gli effetti.

Alla sicurezza informatica, infatti, sono stati destinati all'Italia 191 miliardi di euro, di cui 623 milioni alla *cybersecurity*, 301 milioni sono necessari per il potenziamento e la resilienza *cyber*, finanziati dal programma europeo "Next Generation Eu" (NGEU).

Al PNRR si aggiungono anche i fondi stanziati con la legge di Bilancio 2023, tra cui il fondo per l'attuazione della Strategia Nazionale di *Cybersicurezza*, che si occupa di investire sulla autonomia tecnologica, ma anche il fondo per la gestione della *cybersicurezza*.

Questi investimenti mirano a migliorare le procedure di monitoraggio, prevenzione e risposta contro le minacce *cyber*, per introdurre una rete nazionale per la rilevazione del rischio a supporto delle pubbliche amministrazioni e industrie.⁷

Già nel decreto-legge n. 105/2019 all'articolo uno si stabilisce l'obbligo per gli enti pubblici di segnalazione e notifica degli incidenti *cyber*, ma lo stesso obbligo vige anche nella direttiva “NIS 2” n. 2555/2022 (recepita con il d.lgs. n.138/2024) prevedendo delle tempistiche: per la segnalazione, di ventiquattro ore dalla conoscenza dell'incidente significativo, per la notifica entro settantadue ore.

La legge n. 90 del 2024 ha rafforzato ulteriormente la resilienza cibernetica inasprendo le pene e potenziando gli strumenti di contrasto.

Con il capo secondo della suddetta legge, si modificano invece le parti del Codice penale inerenti alle norme in materia di contrasto dei reati informatici e si coordinano gli interventi in caso di incidenti.

Inoltre, quest'ultima prevede l'istituzione all'interno dell'ACN di un centro nazionale di crittografia che dovrà implementare delle la sicurezza informatica per la protezione

⁷ Piano Internazionale di Ripresa e Resilienza, disponibile sul sito ufficiale del Governo, Italia Domani

dei dati, ma anche la creazione di uffici di cybersicurezza interni alle PA, al fine di rafforzare la difesa delle aziende dagli attacchi informatici.

Tuttavia, questa normativa non può definirsi completa poiché mancano accenni alla competenza dell'ACN in materia di Intelligenza Artificiale, strumento fondamentale per il rafforzamento della sicurezza informatica nel nostro Paese.

Tornando al PNRR, nella Missione uno vengono istituiti i principali obiettivi: Primariamente, digitalizzare la pubblica amministrazione mediante tecnologie *cloud*, affiancandola con degli esperti che la aiuteranno nel processo di trasformazione digitale.

In seguito, si predispone il fine di rafforzare l'identità digitale già esistente, come *Spid* e migliorare servizi e comunicazione come "Pago.pa".

Altro scopo sarebbe incentivare l'erogazione di dati sanitari tramite il fascicolo sanitario elettronico e raggiungere un alto livello di sicurezza informatica, per far fronte agli attacchi informatici a cui le aziende sono sottoposte: come phishing, malware e *ransomware*, che possono causare danni sia a livello economico che reputazionale.⁸

Fondamentale risulta anche garantire la confidenzialità, l'integrità e la disponibilità dei dati per proteggere informazioni classificate e promuovere una *cybersicurezza* volta alla ricerca e all'innovazione dei metodi di tutela.

Il compito di rinforzare le difese informatiche del paese è stato attribuito al Ministero per l'Innovazione Tecnologica e la Transizione Digitale.

Gli investimenti in tema di *cybersecurity* hanno il fine di realizzare ventotto laboratori per l'analisi forense, realizzare il Centro per la valutazione del Ministero dell'Interno, istituire il *Security Operation Center* (S.O.C. del Dipartimento di Pubblica sicurezza.

1.1 (Segue): La responsabilità del *Provider* del servizio *Internet*: Teorie e nuovi risvolti

Il tema in esame è stato oggetto di grande dibattito tra Dottrina e Giurisprudenza, nelle quali sono andate delineandosi due principali teorie che hanno come fulcro lo sviluppo di una posizione di garanzia nel *cyberspazio*.

Secondo la prima tesi, se i fornitori del servizio (*Internet service provider*, *ISP*, detto anche *ISP hosting*) operassero un controllo sulla rete si creerebbe un sistema di «censura privata» che la corte EDU definisce con "*collateral censorship*"⁹.

Con questa, si vuole valorizzare i principi sopracitati enunciati nell'art 21 della costituzione riguardante la libera manifestazione di pensiero, il principio di "auto-responsabilità" dei singoli per cui lo Stato interverrebbe solo in caso di abuso, e il

⁸ Rapporto Clusit 2024, sulla Sicurezza ITC Italia, Associazione Italiana per la Sicurezza Informatica, gli attacchi informatici in Italia nel 2023 sono aumentati del 40%, di cui il 20% sono di tipo governativo.

⁹ Corte EDU, sez. II, sent. 24 settembre 2013 ric. n. 48898/99, Belpietro c. Italia

"principio di neutralità della rete", in base al quale *internet* deve essere un "luogo" sicuro e aperto a tutti, non discriminatorio, indipendentemente dai contenuti, dal servizio, dal mittente o destinatario¹⁰.

A livello sovranazionale la normativa di riferimento per la responsabilità dei *provider* è la Direttiva 2000/31 sul commercio elettronico, nominata «Direttiva E-commerce» (*infra*, § parag. 3 capitolo 1) la quale, all'articolo 14 comma primo, prevede che il prestatore del servizio non sia responsabile per i contenuti pubblicati dagli utenti qualora non sia effettivamente a conoscenza del contenuto illecito, oppure se, venutone a conoscenza, si occupi nell'immediato di rimuovere le informazioni o disabilitarne l'accesso.

Inoltre, secondo l'articolo seguente, non vigerebbe per l'*hosting provider* un obbligo generale di sorveglianza sulle informazioni.

L'articolo 17 del decreto legislativo 70/2003 esenta gli ISP da un dovere generale di controllo "*ex ante*"¹¹ ex art 40 cpv, circa la liceità o meno dei dati che trasmettono o memorizzano i *provider*.

Tuttavia, mantiene un obbligo di comunicazione e collaborazione con l'autorità giudiziaria in caso in cui venga a conoscenza di un fatto illecito¹².

Se, infatti, essendo a conoscenza della illiceità del contenuto, l'*ISP* non ha prontamente informato l'autorità, allora avrà una responsabilità di tipo civile, seguendo l'articolo 2043 c.c.

La Corte di Cassazione nel 2019¹³ ha stabilito che hai fini della attribuzione di quest'ultima *all'ISP* bisogna distinguere fra ruolo attivo e passivo.

Avrà un ruolo attivo quando partecipa nella produzione del contenuto oppure se ne agevola la divulgazione, mentre avrà un ruolo passivo se è solo il mezzo, in senso tecnico, mediante il quale avviene la diffusione del contenuto.

In ogni caso la Corte di Giustizia Europea ha ribadito molto spesso¹⁴ che non sussisterebbe un obbligo di controllo *ex ante* in capo al *provider* dei contenuti pubblicati, seppur avendo un ruolo attivo nella loro costituzione.

I sostenitori della tesi contrapposta pongono a carico del *provider* una forma di "responsabilità oggettiva"¹⁵ o per colpa, in presenza di un contenuto evidentemente illecito.

In questo caso, il fornitore del servizio, dando luogo al collegamento, concorre nel fatto illecito in quanto dà un apporto causale alla commissione dello stesso¹⁶.

¹⁰ Articolo 3,4,5, regolamento n. 2120/2015

¹¹ v. anche d.lgs. 9.4.2003, n. 70; in Giurisprudenza, Cass. Pen. sez. V 20.3.2019, n. 12546

¹² rinvio ad art 14 e ss. d.lgs. 70/2003.

¹³ Cass. Civ., sez. I, sent. 19/03/2019 n° 7708

¹⁴ Corte EDU, sez III, 7 agosto 2018, Causa C-521/17 cooperative Vereniging snb-react U.A. Contro. DM

¹⁵ Trib. Napoli, 8 agosto 1997 in *Diritto e giurisprudenza.*, 1997, 472, con nota di CATALANO; Trib. Roma 22.03.1999

¹⁶ Trib. Roma, 22 marzo 1999, in *Diritto dell'informazione e informatica* 2000, 66 con nota di SAMMARCO, in *Rivista del diritto commerciale* 1999, II, 273 con nota di VISCONTI

A sostegno di quest'ultima tesi ma anche della ipotesi per cui *Internet* viene visto come un luogo di potenziale rischio per i diritti fondamentali dell'individuo, vige innanzitutto la stessa finalità "preventiva" del diritto penale, fondata sul controllo delle fonti di rischio piuttosto che sul neutralizzare i pericoli concreti per la sicurezza collettiva¹⁷.

L'intervento quindi, sarebbe volto, da un lato a evitare che un condannato possa realizzare ulteriori reati, e perciò si tratterebbe di un intervento "*post delictum*", dall'altro impedire tramite l'utilizzo di specifiche misure, "*ante delictum*", che un soggetto possa cedere al reato.

Di conseguenza, secondo quest'ultima tesi, la tutela dei diritti del singolo può essere assicurata solo tramite un controllo preventivo sull'operato degli utenti.

Successivamente al recepimento della direttiva sopraindicata si è formata una ulteriore tesi secondo cui il legislatore dovrebbe "bilanciare" la tutela dei diritti di dignità, reputazione, onore e riservatezza con la libertà di pensiero.

Per questo motivo, si renderebbe applicabile il principio secondo cui l'*Internet Service Provider* dovrebbe adottare previsioni di massima sicurezza e ogni accorgimento, che, come tale, possa prevenire l'evento dannoso, senza però ascrivere a questi ultimi una "responsabilità di posizione" che si concretizzi in una sorta di responsabilità oggettiva¹⁸.

Perciò l'*ISP* sarebbe ritenuto responsabile solo nel caso in cui esso aderisca al contenuto illecito, anche mettendo in atto comportamenti omissivi, come la non tempestività nel segnalare l'illiceità all'autorità competente o la mancata tempestiva rimozione del contenuto, in seguito alla segnalazione dell'autorità giudiziaria.

Infatti, necessaria ai fini della rimozione stessa, è la "*notification*": la notifica qualificata emessa dall'autorità giudiziaria competente; tuttavia, in merito alla comunicazione, la direttiva rinvia alle normative nazionali.

I principali titolari dell'obbligo di impedire che un certo evento possa accadere, ex art 40 comma 2 c.p. sono vari: primo fra tutti, "*l'internet service provider*", figura chiave che potrebbe essere descritta a grandi linee come una organizzazione necessaria non eventuale che presta servizi di connessione, messaggistica, memorizzazione e indicizzazione, e che svolge, al fine di consentire l'accesso alla rete, il ruolo di gestione del flusso di informazioni intercorrente tra terzi.

Anche il "*titolare del trattamento dei dati personali*" viene considerato come titolare dell'obbligo, poiché sarebbe responsabile per non aver adottato misure di sicurezza idonee a prevenire il reato e quindi colpevole per concorso omissivo del reato doloso commesso da altri.

Altra figura è il "*moderatore di un blog o forum di discussione*", che avrebbe la responsabilità dei reati commessi sulla sua piattaforma.

¹⁷ nozione di rischio nel diritto penale, V. MILITELLO, *Rischio e responsabilità penale*, Milano, 1988; più di recente C. PERINI, *Il concetto di rischio nel diritto penale moderno*, Milano, 2010.

¹⁸ Cass. Civ. Sez. V n 8180/2018; Cass. Civ. Sez. III n 8095/2006; Cass. Civ. Sez. III n 1219/1997

Infine "*il direttore del periodico online*", a cui si può estendere il regime ex art 57 c.p., previsto per il responsabile di testate giornalistiche.

Non si può non citare in merito il famoso caso Google vs Vividown per cui la Corte di Cassazione ha sottolineato l'assenza di una posizione di garanzia, ex art 40 cpv, per i fornitori del servizio, statuendo che vi sia in capo a questi ultimi, essendo anche *hosting providers*, un obbligo generale di sorveglianza dei dati immessi da terzi, sul sito che gestiscono¹⁹.

Considerando quanto detto, gli *ISP* devono mettere in atto forme di autoregolamentazione mediante l'attuazione di linee guida in materia di contenuti illeciti sulla rete e sulle loro piattaforme.

Sono stati anche previsti termini d'uso per regolamentare la responsabilità degli utenti e i contenuti di cui è vietata la pubblicazione.

L'attività di cancellazione e di segnalazione è sotto il controllo degli stessi *provider* in modo da limitare fenomeni criminosi.

La sentenza n. 131/2014, della Corte di Giustizia Europea Grande Sezione, viene considerata come *l'incipit* di una maggior tutela ai fini della instaurazione del procedimento di cancellazione dei contenuti.

In quest'ultima, si stabilisce che le azioni aventi ad oggetto la richiesta di rimozione, cancellazione o deindicizzazione di un contenuto che viene immesso nella rete, possono essere indirizzate sia al soggetto che pubblica le informazioni, sia ai gestori dei motori di ricerca.

La decisione ha consolidato il diritto di richiedere ai motori di ricerca di effettuare una procedura di dissociazione del proprio nome o dati personali da pagine *internet* e siti di natura diffamatoria, inesatta od offensiva o riportanti informazioni errate e non aggiornate.

Ancora, in merito alla cancellazione, nella legge 71/2017 sulla prevenzione e contrasto al *cyberbullismo*, all'articolo due recita «ogni soggetto che abbia subito taluno degli atti di cui all'articolo 1, nonché in caso di minore di anni diciotto, ciascun genitore o soggetto esercente la responsabilità genitoriale, può inoltrare al titolare del trattamento o al gestore del sito *internet* o del social media una istanza per l'oscuramento, la rimozione o il blocco delle immagini o video privati sessualmente espliciti pubblicati senza il consenso delle persone ivi rappresentate, diffusi nella rete internet, previa conservazione dei dati originali.

Qualora entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto responsabile, titolare o gestore, non abbia comunicato di aver assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco, ed entro le quarantotto ore successive non abbia provveduto, o comunque nel caso in cui non sia

¹⁹ Cass. Pen. Sez. III n 5107/2013, il caso riguardava un ragazzo disabile sottoposto ad atti di bullismo, il video di queste azioni era stato pubblicato su *Google* video, in più di sottofondo si sentiva voci ingiuriose verso l'associazione *Vividown*. Vennero condannati per non aver impedito il delitto di diffamazione *online* e per il reato all'articolo 167 del d.lgs. 196/2003 tre *managers* di Google.

possibile identificare il titolare del trattamento o il gestore del sito internet, l'interessato può esperire le azioni previste dall'articolo 140 bis e ss. del codice in materia di protezione dei dati personali di cui d.lgs. n 196/2003.»

In ultima analisi, il legislatore deve: individuare i garanti, valorizzare i modelli di *compliance* e di controllo successivo piuttosto che preventivo, mettendo le basi necessarie affinché possa avvenire un bilanciamento tra il bisogno di vigilanza e di rimozione dei contenuti dannosi dalla rete, e la tutela dei diritti.

1.2 (Segue): L'utilizzo dei *Social Network* per finalità Illecite

I siti più in voga per la commissione di reati contro la persona, più nello specifico il *Revenge Porn* (la diffusione illecita di immagini o video sessualmente espliciti), sono i "*social network*": in particolare i nuovi sistemi di messaggistica istantanea come Facebook, Telegram, Whatsapp, Instagram.

L'utilizzo di codesti per la perpetrazione di reati è progressivamente aumentato durante la pandemia: si è osservato infatti un incremento del 77% rispetto all'anno precedente soprattutto per reati commessi verso i minori²⁰, considerati come la categoria più debole e a rischio a causa del loro alto livello di influenzabilità e della "progressiva normalizzazione della pornografia"²¹.

Infatti, secondo uno studio della azienda californiana che si occupa di sicurezza informatica, la *McAfee*, almeno il 49% della popolazione invia foto, video o messaggi di testo a scopo sessuale, almeno una volta nella loro vita, utilizzando i *social*²².

Non bisogna sottovalutare la connotazione di "insanabilità" legata alla pubblicazione online di un determinato contenuto, infatti una volta caricato sulla rete, l'azione potrebbe essere irreversibile, considerando la possibilità di fatto degli utenti di visionare il contenuto, commentarlo, scaricare i file o di effettuare delle "registrazioni schermo", quindi essere oggetto di una possibile più ampia divulgazione, definita "*one to many*".

Un esempio lampante di questa condizione è il caso Cantone, che affronteremo più nel dettaglio in seguito, per cui i video girati e caricati in rete sono circolati in rete, addirittura negli Stati Uniti, dopo tre anni dalla morte della ragazza, sotto inchiesta sono sette *account* su siti pornografici tramite i quali i video sono stati diffusi. (*Infra* § parag. 3 cap.1).

Uno dei siti più utilizzati è senz'altro *Telegram* che garantisce l'anonimato della fonte, poiché non richiede un recapito telefonico aggiuntivo per configurare l'*account*, inoltre è possibile creare gruppi in cui è consentita la partecipazione di grandi numeri di utenti e ciò certamente contribuisce alla diffusione dei contenuti illeciti.

²⁰ dati sono forniti dal Cncpo, il Centro nazionale per il contrasto alla pedopornografia online

²¹ Riv. *Diritto Penale contemporaneo*, 3/2018 Gian Marco Caletti

²² McAfee Corp. - global report "*Cyberbulling in plain sight*", 2022

In merito a questa applicazione, la terza Sezione Penale della Corte di Cassazione²³ ha affermato, in riferimento alla «fruibilità» della *res*, in una sentenza per la detenzione di materiale pedopornografico archiviato nella chat di gruppo *Telegram*, che ai sensi dell'articolo 600 quater comma primo «l'agente ha piena ed incondizionata possibilità di fruire del materiale archiviato, indipendentemente dal fatto che sia stato lui stesso o altri ad aver effettuato l'operazione di salvataggio».

Per questo, specifica la Corte, «anche il semplice fatto di far parte di un gruppo chiuso su questa applicazione, che condivide materiale pedopornografico, anche senza scaricare i file sul proprio dispositivo, costituisce un reato di detenzione di tale materiale».

Altra peculiarità di *Telegram* è la presenza di canali tematici gestiti da "*Robot*", abbreviato "*Bot*": sistemi automatici equiparabili a dei *software*, in grado di interagire con gli utenti, il che rende più complicato individuare l'autore del reato.

Come altre piattaforme, tra cui *Snapchat* o *Whatsapp*, *Telegram* consente di creare *chat* segrete, impostare un *timer* di autodistruzione dei messaggi, sia dopo la visualizzazione che oltre un determinato numero di ore, rendendo più complesso il recupero dei dati sul dispositivo dell'utente.

Su questa piattaforma, oltre allo scambio illecito di immagini sessualmente esplicite, può verificarsi anche lo scambio di foto comuni, che non siano a sfondo sessuale, come il caso avvenuto nel 2017 dove un uomo è stato condannato per aver creato un catalogo su *Telegram* con foto di donne prese dal loro profilo *Facebook*, e i loro dati resi pubblici, definendole «in offerta a 5 euro, il costo di un drink», l'imputato è stato condannato a un anno e sei mesi di reclusione.

Altro esempio è il recente caso di una ventiduenne di Perugia, la quale era venuta a conoscenza della presenza di una sua foto *hot*, mandata al fidanzato anni prima, su un canale *Telegram*: questa con l'aiuto della polizia postale si è infiltrata nel gruppo fingendosi uomo e avviando una *chat* privata con due amministratori.

Alla fine, la donna ha potuto identificarli e denunciarli alle autorità, per i colpevoli, nel 2023 è stato richiesto il rinvio a giudizio per disporre la messa alla prova²⁴.

Più difficoltosa risulta la diffusione di contenuti illeciti con mezzo *Facebook*, il quale è vincolata all'obbligo, per coloro che si vogliono iscrivere, di immettere i propri dati anagrafici all'interno della piattaforma.

Tuttavia, la reale identità dell'utente non può essere verificata con certezza perché l'interessato potrebbe aver inserito dati falsi, creando un cosiddetto profilo "*fake*", oppure addirittura potrebbe aver creato un profilo *fake* a nome della vittima stessa e condividere *chat* erotiche o immagini pornografiche.

Considerando più approfonditamente quest'ultima ipotesi, la vittima potrebbe essere oggetto di scherno nelle cosiddette "*chatlines*", ossia raggruppamenti di persone in un numero potenzialmente indefinito, che si iscrivono e che possono mandare messaggi

²³ Cass. Pen., Sez. III, 4 settembre 2023 (ud. 4 aprile 2023), n. 36572

²⁴ Antioco Fois, La Repubblica, 23 giugno 2023

in tempo reale, previa manifestazione di una accettazione ad iscriversi alla *chat* e al momento della condivisione del contenuto illecito.

In questo caso sarebbe configurabile il reato di sostituzione di persona articolo 494 c.p.²⁵, spesso però viene ritenuto ascrivibile anche il reato, come vedremo in seguito, di diffamazione all'articolo 595 c.p., quando l'agente dopo aver creato un profilo falso su *Facebook* a nome di un altro soggetto inconsapevole, contatti conoscenti della persona offesa in maniera diffamatoria²⁶.

Su questo *social*, tuttavia, il singolo titolare del profilo ha la facoltà di decidere il livello di *privacy* delle sue informazioni, ponendole in modalità pubblica o privata, determinando di fatto, chi può interagire con i propri *post* multimediali o testuali, e da chi può ricevere messaggi.

Per questo motivo è consigliato, per una maggiore protezione, porre il profilo privato in modo tale da permettere solo a chi si conosce di accedere ai dati, anche se ciò non assicura una piena tutela; infatti, è a discrezione della persona la decisione di continuare a condividere fotografie.

Facebook ha deciso di implementare la sicurezza del proprio sito inserendo al suo interno algoritmi che impediscono l'immissione di materiale multimediale che possa danneggiare gli iscritti, e che consentono all'utente di segnalare in maniera immediata la probabilità che il contenuto sia stato pubblicato, lesivo dei diritti della persona (*Infra*, § parag. 2 Cap. 3).

A causa di queste restrizioni, l'utente malintenzionato potrebbe decidere di non pubblicare direttamente il contenuto illecito sulla piattaforma ma di inserirvi un *link* esterno riconducibile a portali che ne consentono la pubblicazione.

Tuttavia, la rimozione di quest'ultimo da parte della piattaforma potrebbe non essere immediata e quindi il contenuto potrebbe rimanere, seppur per un periodo limitato di tempo, accessibile e divulgabile.

In merito al "*like*" che viene apposto su piattaforme come *Facebook* ai contenuti illeciti, la giurisprudenza è ondivaga.

Per alcuni, metterne uno non integra il concorso di reato di chi pubblica immagini sessualmente esplicite su *internet* senza approvazione della vittima²⁷.

²⁵ Cass. Pen. sez. V, 28 novembre 2012 n. 18826 in *Danno e responsabilità*. 8/2023 nota di MENGONI, chattare con un nickname riconducibile ad altri integra il reato di sostituzione di persona

²⁶ Cass. Pen. Sez. V, 12 giugno 2018 n. 38911 in *Dir & Giust.* 2018, nel caso di specie si faceva riferimento all'invio di una lettera ai genitori della vittima nella quale si diceva che il figlio era *gay*, oltre all'affissione sulla porta della sua casa di un volantino con scritto "serate gay", a causa della sua relazione con un altro uomo.

²⁷ G.i.p. Trib. La Spezia, sez. II, 4 ottobre 2018 n.331 in *de jure*

Mentre per la Cassazione, mettere like potrebbe rappresentare una volontà di condivisione dell'illiceità del contenuto²⁸, perciò può venir considerato come un aggravamento della portata lesiva della condotta incriminata.

Da considerare è anche la piattaforma di messaggistica *Whatsapp*, che consente di inviare messaggi contenenti immagini, file audio, fare videochiamate, registrazioni vocali o messaggi di testo.

A differenza degli altri *social*, qui il principale metodo di riconoscimento è il collegamento al numero di telefono dell'utente, che risulta presupposto necessario per la creazione dell'account.

La comunicazione è consentita sia "*one to one*" che "*one to many*", offrendo la possibilità di creare gruppi, per cui l'*audience* a cui potrebbe essere inviato il contenuto illecito aumenta esponenzialmente.

Secondo una recente sentenza della Cassazione Penale²⁹, i messaggi inviati su *Whatsapp* costituiscono prova legale in quanto hanno "validità di documento" ai sensi dell'art 234 cod. proc. Pen.

La Corte sottolinea anche il principio secondo cui sarebbe utilizzabile la mera riproduzione fotografica (*screenshot*) dei messaggi anche in assenza di un provvedimento di sequestro del dispositivo e di una procedura di intercettazione delle comunicazioni.

Whatsapp ha da poco introdotto anche delle funzionalità che sono simili a quelle sopracitate per altri *social network*, come ad esempio la possibilità di inviare immagini "ad una sola visualizzazione", cioè foto o video, che una volta visualizzate non sono più visibili al destinatario.

Su questa novità, l'applicazione, per una maggiore tutela, ha previsto l'impossibilità di effettuare *screenshot* o videoregistrazioni al contenuto; infatti anche se la persona prova a salvare il contenuto, nella galleria del telefono troverà una pagina totalmente bianca; tuttavia, quest'ultimo potrebbe sempre essere in grado di registrare con un secondo telefono o trovare metodi alternativi per salvare le suddette.

Altra caratteristica inserita di recente sono i messaggi "effimeri" ossia delle comunicazioni testuali temporanei, che scompaiono dopo sette giorni dall'attivazione della funzionalità, e con essi anche i file multimediali inviati; tranne nel caso in cui si fosse attivata la funzione di salvataggio nella memoria del dispositivo.

Tuttavia, la piattaforma nelle FAQ chiarisce che sebbene il messaggio "sparisca" dopo sette giorni, ciò non preclude il permanere di tracce del messaggio nel sistema e nella memoria del dispositivo: come in caso di *backup* effettuato entro il tempo limite per la sparizione, o in alternativa se il messaggio viene inoltrato a una persona che ha disattivata questa funzione.

²⁸ questo principio è stato affermato anche per associazione con finalità di terrorismo internazionale, nel caso di specie la Cassazione ha ritenuto concorso il *like* a video inneggianti il martirio islamico riferito alla guerra in Siria (Cass. Pen., Sez V, 25 settembre 2017, n. 55418)

²⁹ Cass. Pen., Sez. II, 19 ottobre 2022 (ud. 1° luglio 2022) n. 39529

Non sono pochi i casi di *Revenge Porn*, disciplina che verrà approfondita in seguito, per cui viene utilizzato come strumento principale della diffusione del contenuto illecito proprio *Whatsapp*.

Uno tra questi è il caso dell'insegnante di Torino, maestra d'asilo licenziata a causa di un video *hard* diffuso fra le varie chat di gruppi *whatsapp* del paese, da parte del suo ex fidanzato, foto circolate poi tra i colleghi.

I giudici della Corte di Appello di Torino hanno confermato la sentenza che infligge alla dirigente tredici mesi di reclusione per violenza privata e diffamazione e un anno anche per una mamma, colei che ha dato inizio alla diffusione³⁰.

Strumento molto in voga soprattutto in Inghilterra per la circolazione di immagini a sfondo sessuale è *Airdrop*, un servizio di condivisione che viene usato tra i dispositivi *Apple* che consente di inviare e ricevere *file*.

Questo fenomeno viene definito "*cyber flashing*": consiste nell'invio mediante *Airdrop* di immagini di genitali o di video senza il consenso della persona che li riceve, che il più delle volte è sconosciuta, ma che si trova nello stesso luogo o nelle vicinanze di chi li invia.

Per far fronte a questo problema ci sono vari modi come il limitare la possibilità di ricevere *file* soltanto alle persone conosciute, quindi ai contatti del telefono.

Per quanto concerne la repressione di questo fenomeno, non esiste una normativa ad hoc, ma è stata fatta ricomprendere nell'art 660 c.p.: molestia e disturbo alle persone, previa denuncia della vittima.

L'articolo prevede quanto segue: «Chiunque, in un 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 lire cinquemila».

Questa fattispecie cita espressamente "un luogo pubblico", tuttavia di recente la Corte di Cassazione ha definito *Facebook*, e quindi per analogia anche le piattaforme analoghe, come "una *community* aperta" perciò accessibile a chiunque³¹, tuttavia ciò non consentirebbe di ricomprendere anche la messaggistica privata, anche se la Giurisprudenza piano piano si sta orientando in tal senso, criminalizzando queste condotte.

In conclusione, l'uso dei *social network* ha limitato il principio di "auto-responsabilità" a cui dovrebbe sottostare colui che agisce su *Internet*, perché i reati compiuti con questa modalità vengono percepiti dall'abusante come meno gravi e con meno probabilità di essere identificati.

Ciò comporta una de-responsabilizzazione dell'autore e una de-umanizzazione della vittima: a causa, sia dell'anonimato, che molte volte viene utilizzato per commettere

³⁰ Corte di Appello di Torino, febbraio 2023, in *Ius in Itinere*, Valeria D'Alessio, *Revenge porn: Caso Tavassi e Maestra di Torino*

³¹ Cass. pen., sez. I, sent 12/09/2014 n° 37596

questi abusi, ma anche per la percezione di essere fisicamente lontani dalla persona offesa³².

In questo modo *Internet* viene considerato dal soggetto attivo come un vero e proprio "muro" che lo divide dal soggetto passivo.

2.0 (segue): Da dove deriva il termine “*Revenge Porn*”? Analisi terminologica e storia della fattispecie

Per comprendere meglio questo fenomeno, si deve sottolineare come già nella prima metà del 1800 con l'avvento della fotografia e le prime foto in bianco e nero di nudo femminile e di parti intime, si registravano già allora i primi casi di diffusione non autorizzata di contenuti sessualmente espliciti, un cosiddetto “antenato” del *Revenge Porn*.

Un esempio dell'esistenza di queste vicende, anche all'epoca, è l'arresto nel 1888 del fotografo newyorkese *Le Grange Brown*: la polizia trovò in casa sua un archivio di più di 500 foto che ritraevano donne anche dell'alta e media borghesia della *New York* dell'epoca.

In quell'episodio, gran parte delle fotografie erano state realizzate con la tecnica del fotomontaggio, ritagliando i volti delle povere donne, da fotografie scattate loro in momenti di vita quotidiana e decontestualizzate, come eventi di beneficenza e cerimonie pubbliche, incollandoli su dei corpi di terze donne nude, spesso di origini non nobili e che, a causa della loro condizione, vendevano per pochi dollari al fotografo.

I fotomontaggi in questione giravano, dietro grande corrispettivo, in contesti prevalentemente goliardici maschili (come saloni di barbieri, taverne).

Il caso di *Le Grange Brown* e dei suoi “fotomontaggi”, utilizzati per vendere le fotografie ad altri uomini, può considerarsi l'antenato dell'odierna e crescente piaga del “*deepfake*” (infra, § *cap. 3 parag. 3*), tecnica, di cui tratteremo più avanti, che con l'aiuto di *software* di Intelligenza Artificiale, permette la creazione di foto e video a sfondo sessuale, fittizi usando volti di donne e corpi di altre³³.

Più di recente invece, negli anni '80, si utilizzavano cd, dvd e riviste per soli uomini, come la rivista *Hustler*, che aveva una rubrica che pubblicava foto inviate dai lettori, in cui venivano inquadrare delle donne nude, inconsapevoli³⁴.

³² BRUNO A., CAMPANELLA L., *Elementi di Vittimologia*, 2023

³³ JESSICA LAKE, UNSW Law Journal 2019, *Disembodied data and corporeal violation: our gendered privacy law priorities and preoccupations*

³⁴ E. MONTE, *l'Art. 612 ter, diffusione illecita di immagini o video sessualmente espliciti, tra buoni propositi, denegato diritto all'oblio e "morti social"*, Giappichelli editore

Alcune volte, queste fotografie comportavano l'inizio di procedimenti legali da parte delle vittime³⁵.

Il termine "*Revenge Porn*" o di minor uso "*Revenge Pornography*", nasce nella cultura anglosassone, e venne introdotta per la prima volta nel 2007 nel dizionario «*Urban Dictionary*» sito dedicato a definire i neologismi inglesi.

Nel 2011 in Inghilterra è diventato famoso un sito denominato "*is anyone up*" in cui potevano essere caricati immagini o video sessualmente esplicite dei propri ex *partner*, aggiungendo però anche i *link* alle pagine *Facebook* della vittima, con l'obiettivo di aumentarne il fattore degradante.

In seguito, questo fenomeno venne definito dal dizionario di Oxford come «*revealing or sexually explicit images or videos of a person posted on the internet, typically by a former sexual partner, without the consent of the subject, in order to cause them distress or embarrassment*», letteralmente si tradurrebbe con «immagini o video sessualmente esplicite che vengono postate, normalmente da un partner sessuale, su internet senza l'assenso dell'interessato, per poter arrecare a quest'ultimo angoscia e imbarazzo».

Per la tutela dei diritti contro questo tipo di reato è stata introdotta, in Inghilterra e nel Galles, nel 2015 il "*Criminal Justice and Courts Act*" il quale, catalogandolo come "*sexual offence*", prevedeva che a seguito della prova del mancato assenso dell'interessato, colui che diffonde il contenuto sessualmente esplicito debba essere condannato ad almeno due anni di reclusione³⁶.

Precedentemente, le fattispecie di *common law* erano basate sul criterio di imputazione a titolo di dolo specifico³⁷.

La disciplina introduceva anche delle cause di non punibilità: una di queste si verificava nel caso in cui chi divulgava il contenuto credeva erroneamente che la persona ritratta l'avesse già diffuso, oppure ignorava il fatto che non era presente l'approvazione liberamente espressa della vittima.

Altre cause potrebbero verificarsi se il materiale è stato diffuso nel corso o in vista della pubblicazione di materiale giornalistico, o se era convinto che la divulgazione servisse per prevenire e agevolare delle indagini di reato (*Infra*, § parag. 4 cap. 2).

Inoltre, questa fattispecie copre anche la condivisione di contenuti espliciti via *e-mail*, siti o addirittura la distribuzione fisica di copie, come dischi o foto.

Con la legge in questione, ci si riferisce alla parola "*sexual*" come immagini o video che espongano i genitali di una persona o che possa essere ritenuta dalle altre persone come "sessuale".

Questa visione è sicuramente in linea con la nostra Giurisprudenza, che si è espressa in merito alla definizione di "contenuto sessualmente esplicito" per l'articolo 612ter, che

³⁵ Corte d'Appello USA, 11 settembre 1984, 736 F.2d 1084 (5th Cir. 1984), Wood vs Hustler Magazine

³⁶ Section 33 of Criminal Justice and courts Act, 2015.

³⁷ CALETTI G.M., *Revenge Porn e tutela penale, prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze anglo-americane*, 2018 cit. pag. 67

introduce la fattispecie di diffusione illecita di immagini o video sessualmente esplicite (*infra*, § cap. II, parag. 2.3).

Infatti, ciò che ha portato alla sua recente introduzione, non sono stati solamente i recenti fatti di cronaca che tratterò in seguito, di Tiziana Cantone e della Deputata Giulia Sarti (*infra*, § cap. I, parag. 3.1), ma anche la necessità di rapportarsi con le discipline straniere, in un contesto di tutela più ampio, per il quale diventa fondamentale il rispetto della *privacy* e dei diritti fondamentali.

Tuttavia, prima della costituzione della disciplina inglese, si poteva far riferimento ad altre fonti, a seconda del caso specifico: il "*Communication Act*" del 2003, se la condotta fosse reiterata, anche la disciplina prevista dal "*Protection from Harrassment Act*" del 1997.

Nel 2021 è entrata in vigore la sezione 69 del "*Domestic Abuse Act*" il quale sancisce la costituzione come reato anche della sola minaccia di divulgazione di fotografie e filmati a sfondo sessuale privati.

Oggi, alcuni giornali italiani e l'Accademia della Crusca descrivono il "*Revenge Porn*" come "vendetta pornografica" o "porno vendetta", ciò consentirebbe di definire questa fattispecie come un particolare tipo di ritorsione di carattere sessuale: tuttavia il fine potrebbe non sempre essere quello della vendetta, come vedremo in seguito, ma potrebbero celarsi anche altri motivi come divertimento, noia o fini remunerativi³⁸.

Pertanto, questa definizione sembra essere, secondo gli studiosi, non del tutto precisa. Di opinione opposta è il gruppo Incipit, studiosi dell'Accademia della Crusca che si sono espressi in merito alla questione: a seguito della approvazione da parte della Camera nel 2019 dell'emendamento che introduce l'art 612 ter nel Codice penale, il gruppo, da un lato si complimenta con il legislatore per aver espresso con termini idonei il reato oggetto del dibattito, dall'altra critica alcuni commentatori e giornalisti di utilizzare «forestierismi opachi» per descrivere la fattispecie.

Per questi, il termine più corretto sarebbe proprio "porno-vendetta", poiché utilizzare inglesismi potrebbe portare a sottovalutare la gravità del fatto.

Tuttavia, secondo la studiosa di linguistica Licia Corbolante questa traduzione è scorretta³⁹, poiché letteralmente *Revenge porn* significa "pornografia vendicativa".

Infatti, facendo riferimento alla grammatica inglese, il determinato del nome è "*Porn*" non "*Revenge*"; pertanto, si definirebbe come un particolare tipo di materiale pornografico che viene divulgato con intento vendicativo al fine di causare alla vittima umiliazione, degradandola a mero oggetto sessuale.

Il disegno di legge che istituisce l'art 612ter non nomina né la locuzione "*Revenge porn*" né "porno vendetta" ma parla correttamente, come vedremo in seguito (*infra*, § cap. II

³⁸ cfr. G.M. CALETTI, *Libertà e riservatezza sessuali all'epoca di internet*, cit., p. 2084: «gli studi angloamericani dimostrano come tante altre ipotesi di pornografia non consensuale, per le quali impropriamente il linguaggio mediatico scomoda il neologismo "*Revenge porn*", si verifichino sulla base di finalità molto diverse dalla vendetta».

³⁹ Articolo de "Il post" 5 aprile 2019 "dovremmo trovare un altro nome al *Revenge porn*"

parag. 2) di "diffusione illecita di immagini o video sessualmente espliciti" sebbene anche questa locuzione abbia creato non pochi dubbi in Giurisprudenza.

Altri invece, come Matteo Bordone, *blogger* de "Il Post", usa il termine "diffamazione pornografica": è una espressione breve, chiara, adatta per la comunicazione pubblica, ma anche questa non del tutto precisa.

La Corbolante propone delle alternative come "porno vendichevole" o "porno per vendetta", oppure "porno ostile" "porno doloso" o "porno illecito".

Ulteriori autori invece, parlano di "pornografia non consensuale"⁴⁰ o "sfruttamento sessuale basato sull'immagine" di Powell (2009, 2010) o "abuso sessuale basato sull'immagine" di McGlynn & Rackley (2017)⁴¹, queste espressioni consentirebbero di dare portata più ampia alla fattispecie designata, comprendendo non solo immagini pornografiche, ma anche immagini utilizzate come forma di sfruttamento sessuale⁴².

3.0 (segue): La mancanza del consenso e gli effetti sulla vittima di *Revenge porn*

In Italia, uno studio condotto da TF Group S.r.l., una società di analisi e ricerche specializzata nella gestione della reputazione online, per conto di PermessoNegato.it APS, che offre supporto alle vittime di Pornografia Non-Consensuale, ha rivelato che circa due milioni di italiani sono stati vittime di *Revenge porn*.

Inoltre, 14 milioni di persone hanno guardato in rete immagini di pornografia non consensuale, e circa il 9% conosce la vittima. Questi dati emergono da un questionario online sottoposto a campione statistico su 2.000 individui⁴³.

Per tali ragioni è imperativo garantire una tutela particolare alle vittime, data la crescente incidenza di questi atti criminali.

Considerando la definizione del fenomeno di *Revenge porn* come la pubblicazione e la diffusione di immagini o videoregistrazioni sessualmente esplicite su *Internet* senza l'accettazione da parte della vittima, si deve porre come base del nostro studio il fatto che nella realtà moderna le immagini assumono un ruolo fondamentale, come se fossero un "documento digitale", per questo la diffusione di questo tipo di contenuti potrebbe creare molti problemi alle vittime, data la celerità con cui vengono divulgati. Queste immagini vengono definite non più come mezzi mediante il quale avviene un tipo di comunicazione, ma come dei "fenomeni" «non esistono di per sé, ma accadono;

⁴⁰ Cfr. CALETTI G.M., *Libertà e riservatezza sessuali all'epoca di internet*, cit., p. 2089 e "Can Affirmative Consent Save "Revenge Porn" Laws?", cit., p. 161. L'autore definisce come «più opportuno [...] fare uso di altre espressioni meno connotate come, ad esempio, "pornografia non consensuale"». Cfr. nuovamente "Revenge porn" e tutela penale, cit., p. 92.

⁴¹ cfr. N. HENRY, *Imaged-based sexual abuse. A study on the causes and consequences of non-consensual nude or sexual imagery*, Londra, 2021.

⁴² *International Journal of Cyber Criminology* – ISSN: 0974-2891 July - December 2019. Vol. 13(2): 418-438; 2019

⁴³ Report su permessonegato.it "state of Revenge 2022"

hanno luogo sia che si tratti di immagini in movimento (...) sia che invece si tratti di immagini statiche. Esse accadono grazie alla trasmissione e alla percezione⁴⁴» perché suppongono il venire ad esistenza di un vero e proprio rapporto comunicativo.

Per questo il legislatore ha percepito la più che valida necessità di inserire all'interno del Codice Rosso l'articolo 612 ter.

Il fine ultimo del *Revenge porn* quindi, è la stessa che ha ipotizzato il legislatore inglese, ossia il danneggiamento morale, reputazionale della persona offesa, esercitando una forma di vendetta e di supremazia sulla vittima, per screditarla e infondere paura.

Le principali emozioni scatenanti questo tipo di comportamento sono rabbia, gelosia, disperazione, apatia, senso di perdita del controllo, causate per esempio dalla fine di una relazione.

Tuttavia, tale contesto può rivelarsi errato per alcuni casi, confermati dalla recente casistica italiana e internazionale, ove si attestano episodi di (presunto) “*Revenge pornography*” per cui la vittima non ha nessun tipo di relazione (in corso o esaurita) o ogni altro rapporto di conoscenza con l'agente, per esempio si pensi al caso di Giulia Sarti, deputata che è stata vittima di un hacker⁴⁵.

Di fondamentale rilievo nell'esame della disciplina è il consenso alla diffusione delle proprie immagini.

L'approvazione per il trattamento dei dati e della propria immagine, secondo l'articolo 4 del Regolamento Generale sulla protezione dei dati (GDPR) deve consistere in «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

In merito, si deve fare una distinzione tra quello prestato alla registrazione e quello dato per la diffusione; in quanto il più delle volte, sebbene fosse consentita dal soggetto attivo la registrazione del contenuto, l'approvazione viene a mancare per la successiva divulgazione, e a volte questa può persino essere revocata dalla vittima durante la registrazione del contenuto stesso.

Per la configurazione del reato, infatti, specifica la Corte di Cassazione con una sentenza molto recente⁴⁶, ai fini della diffusione illecita di immagini o contenuti sessualmente espliciti non assume rilevanza la circostanza che la vittima abbia prestato il suo consenso per farsi ritrarre nel video successivamente divulgato a sua insaputa.

Infatti, la sentenza precisa che, affinché possa trovare applicazione questo principio, l'assenso deve riguardare esplicitamente anche la diffusione stessa.

L'assenza di adesione della vittima, come vedremo più nel dettaglio in seguito analizzando la normativa, costituisce al comma 2 dell'art 612 ter, "elemento

⁴⁴ BOEHM, *Il ritorno delle immagini*, in *Teorie dell'immagine. Il dibattito contemporaneo*, a cura di Pinnotti-Somaini, Milano, 2009, 42 ss.

⁴⁵ cfr. M. PUCCIARELLI, “Caso Sarti, un ex deputato 5S: “Il furto delle foto da un pc in dotazione alla Camera”, in *la Repubblica*, 20 marzo 2019.

⁴⁶ Cass. Pen. Sent, Sez. V, n. 19201 del 15 maggio 2024

costitutivo" della fattispecie, come accade anche in tema di violenza sessuale o di consenso informato del medico⁴⁷.

Frequentemente associato a quest'ultimo fenomeno è la frase utilizzata nelle manifestazioni contro tutti i reati di matrice sessuale "*no means no*" e "*only yes means yes*"⁴⁸(*infra*, § cap 2. parag. 4.3), queste locuzioni vengono considerate alquanto esplicative per definire l'importanza dell'autorizzazione dell'altra persona, soprattutto in materia sessuale⁴⁹.

Molto spesso, come definisce un ulteriore studio condotto da *TF Group S.r.l.* per conto di *permessonegato.it*, il settanta per cento di persone nel nostro paese che hanno subito *Revenge porn* sono donne e il trenta per cento uomini, mentre il tredici per cento appartiene alla comunità LGBTQ+⁵⁰.

Inoltre, la "*Data and Society Research Institute*" ha svolto una ricerca dalla quale è emerso che il quindici per cento degli utenti *gay*, lesbiche e bisessuali hanno subito il ricatto di diffusione di loro foto o video sessualmente esplicite⁵¹.

Ulteriori studi hanno dimostrato come molti uomini si dichiarino d'accordo con le motivazioni conseguenti all'attuazione del reato, considerando giusta la vendetta di divulgazione di materiale pornografico⁵².

Alla base di ciò ci sarebbe la presunta perdita di controllo della relazione da parte del compagno e quindi la necessità di ristabilire «l'ordine» perpetrando un atto di supremazia, cercando di farsi giustizia.

È condotta molto diffusa il fatto che le persone tendono a sottovalutare la mancanza di approvazione del soggetto passivo, non solo in relazione al reato di *Revenge porn*, ma anche per molestie di altro tipo, ricercando una giustificazione nel comportamento del perpetratore, considerandolo come un atto emotivo inconsapevole.

Queste in gergo psicologico vengono chiamate "tecniche di neutralizzazione" della vittima.

⁴⁷ Cass. Pen. sez. IV, 27 novembre 2013 n 2347 in *Guida dir.*, 2014, 10,72 parla di libera disponibilità del paziente capace di intendere e di volere che in autonomia può decidere sulla sua vita

⁴⁸ Parla di "ley del solo sí es sí" M. CANCIO MELLA', *Guerra cultural y reforma de los delitos sexuales*, in *El País*, 7 giugno 2022. Per un'indagine comparata sugli schemi del "no means no" e del "yes means yes" si rimanda a MATTHEUDAKIS, *Un'indagine comparatistica sulla configurazione dei reati sessuali per colpa (grave) sui profili di consenso della vittima*, in *Revista de Direito Brasileira*, 2020, 10, 280 ss.; "no means no" legislatore tedesco cfr. HORNLE, *The New German Law on Sexual Assault and Sexual Harassment*, in *German Law Journal*, 2017, 6, 1309 ss.; cfr. CALETTI, *Can Affirmative Consent Save "Revenge Porn" Laws? Lessons from the Italian Criminalization of Non-Consensual Pornography*, in *Virginia Journal of Law & Technology*, 2021, 25, 3, 112 ss.

⁴⁹ Dottrina inglese. Cfr. A.A. GILLESPIE, *"Trust me, it's only for me" Revenge Porn and the criminal law*, 2015; C. MCGLYNN, E. RACKLEY, *Image-Based Sexual Abuse*, 2019, in *Oxford Journal of legal studies*

⁵⁰ Dati estrapolati dall'articolo del 13 giugno 2022 su *repubblica.it*

⁵¹ Cfr. A.E. WALDMAN, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, in *L.S.Inquiry*, 44, 4, 2019, p. 987 ss.

⁵² HALL-HEARN, *"Revenge pornography and manhood acts: a discourse analysis of perpetrators' accounts"*, in *Journal of Gender Studies*, 2019, XXVIII (2.)

Secondo uno studio di una famosa criminologa di Milano, queste frasi vengono usate per minimizzare la loro responsabilità e arrivare addirittura indirettamente a colpevolizzare la vittima al fine di ridurre la sensazione collettiva di illiceità del fatto. Locuzioni spesso utilizzate in questi contesti sono «mi ha provocato» o «se l'è cercata»⁵³, oppure «Non fare la vittima perché molto del tuo modo di fare attira malati di mente, la cultura dello stupro la propagandate voi»⁵⁴.

Queste frasi sono tipiche del processo di "*Victim Blaming*"⁵⁵: letteralmente indica una "colpevolizzazione della vittima"⁵⁶ la quale rappresenta una opposta tendenza ad accusare la vittima di aver causato la nascita di un evento di carattere sessuale e il conseguente danno, tramite la propria condotta "superficiale e sconsiderata".

Spesso questo meccanismo di plagio comporta nelle vittime uno stato di impotenza, il non sentirsi adeguate nel ricevere tutela dei propri diritti, per questo molte volte non denunciano alle autorità.

Il fenomeno in questione però può realizzarsi non solo in una situazione relazionale, ma anche in ambito lavorativo o di rapporti sociali, e addirittura tra le Corti in sede giurisprudenziale: i casi famosi sono tanti, nel 1999 in Italia, la Corte di Cassazione ha negato una violenza sessuale perché la vittima indossava i jeans e nella motivazione della sentenza si legge che «i jeans non possono essere sfilati senza la fattiva collaborazione di chi li porta»⁵⁷.

⁵³ MERZAGORA I., 2019, Università degli studi di medicina legale di Milano, «*l'idealismo pervertito per una giusta causa?*»

⁵⁴ Intervista su Open, FABIO GIUFFRIDA, 2021, "le mie foto date in pasto a 100 mila uomini su Telegram, questa è una violenza" una ragazza che ha subito *Revenge porn*, i cui commenti sulle sue foto sono riportati dall'intervista fatta open consultabile al link,

⁵⁵ Per quanto messo in luce dall'ISTAT, il 40% degli intervistati ritiene che sia delle donne la responsabilità per le violenze subite, in particolare a causa del loro modo di vestire, ritenendo che chi davvero vuole, può riuscire ad evitarle. Cfr. *Violenza sulle donne. Colpa di come vestono*, in *Corriere della Sera*, 26.11.19. Cfr. SPACCATINI, F. GRASSI, E. GIOVANNELLI, I., PAGLIARO S., PACILLI MG, *se l'è cercata: il victim blaming nei confronti delle vittime di violenza di genere.*; DR TAYLOR J., *why women are blamed for everything: exposing the culture of victim blaming*, 2021

⁵⁶ Il c.d. "*victim blaming*", termine nominato per la prima volta dall'opera del sociologo WILLIAM RYAN pubblicata nel 1971 ed intitolata, *Blaming the victim*. Cfr. G.M. CALETTI, nel libro "*Revenge porn*" e tutela penale, cit., p. 72, richiamando il parere di una commissione del Senato australiano di Canberra, che «il termine "*Revenge*", rimandando ad un atto vendicativo, sembra suggerire che si tratti di un atto in qualche misura "giustificabile"». Per maggiori approfondimenti in tema vedi. C.

CALVERT, *Revenge Porn and Freedom of Expression: Legislative Pushback to an Online Weapon of Emotional and Reputational Destruction*, in *Fordham Intellectual Property Media & Entertainment Law Journal*, 2014, 673 ss. ; C. BARMORE, *Criminalization in Context*, 2015, cit., 467, mette in luce anche la non collaborazione della stessa polizia americana nel recepimento delle prime denunce, riportando il caso di un agente che, a fronte della denuncia presentata da una ragazza, le avrebbe risposto: «*why would you take a picture like this if you didn't want it on the internet?*»; G.M. CALETTI, "*Revenge porn*" e tutela penale; A. VERZA, *Aggredire attraverso l'immagine*, cit., *passim*, 2017

⁵⁷ Corte di Appello di Napoli, 13.10.99 n.1636; La Giurisprudenza successiva poi si è discostata da questa sentenza, con una successiva Cass. Pen., sez. III, sentenza 21/07/2008 n° 30403, affermando che il fatto di avere i Jeans non incide sulla verifica della avvenuta violenza.

Per un altro caso, la Corte Europea dei diritti dell’Uomo⁵⁸ ha condannato l’Italia a seguito di una sentenza di Appello per i quali erano stati assolti i sei condannati a quattro anni di reclusione per violenza sessuale aggravata, con la motivazione di incongruenze e inattendibilità delle dichiarazioni della vittima, definendola come «soggetto femminile fragile, ma al tempo stesso creativo, disinibito, capace di gestire la propria (bi)sessualità», protagonista, nel corso della serata, di “atteggiamenti particolarmente disinvolti ... in un clima ... goliardico (e) godereccio»⁵⁹.

Secondo la Corte Europea, sebbene il quadro normativo italiano sia soddisfacente, è emersa comunque una violazione dell’articolo 8 della CEDU, il quale prevede il diritto al rispetto della vita privata.

Diverso invece è il caso di consenso putativo⁶⁰: quando il perpetratore suppone erroneamente la presenza di consenso della vittima.

In questa situazione il soggetto agente sarà esente da colpa: secondo la disciplina dell’errore sulle cause di giustificazione, non gli verrà attribuita la responsabilità penale per mancanza di dolo.

Se si tratta invece di un evento colposo, e la legge lo riconosce come tale, allora il soggetto risponderà a titolo di colpa.

Secondo la Cassazione⁶¹ la libertà sessuale (fra cui rientra anche la tutela dalla diffusione di immagini intime) è assistita da tutela di rango Costituzionale, essendo riconosciuta come diritto inviolabile dell’uomo dall’articolo 2 della Costituzione.

Perciò il reato risulterà integrato sia in presenza di manifesto dissenso, sia in assenza di consenso (che deve perdurare sia per la ripresa delle immagini/video, che per la divulgazione), non espresso neanche in forma tacita dalla vittima.

Una sezione della Suprema Corte solleva dubbi, in caso di errore sull’espressione del consenso/dissenso «sulla ricorrenza di un valido elemento soggettivo solamente nel caso in cui l’errore si fondi sul contenuto espressivo, in ipotesi equivoco, di precise e positive manifestazioni di volontà promananti dalla parte offesa⁶²».

In questa, si precisa che il consenso putativo può essere ritenuto una causa di giustificazione solo per il caso in cui: ci sia una situazione oggettivamente valutabile, non creata dal perpetratore, che possa indurre in errore il soggetto attivo sull’effettiva esistenza del consenso.

In conclusione, si deve trattare di un episodio per cui sarebbe ragionevole presumere che il soggetto passivo, titolare del diritto, avrebbe espresso il suo consenso se avesse potuto⁶³.

⁵⁸ Corte EDU, *J.L. c. Italia*, ricorso n. 5671/2016, sentenza 27 maggio 2021 (Prima Sezione)

⁵⁹ Corte di Appello di Firenze, sez. II Penale, n. 858, 4/03/2015

⁶⁰ articolo 50 e 59 comma 4 c.p., Codice penale commentato, Luigi Alibrandi, 2024, cinquantesima edizione

⁶¹ Cass. Pen. sent n. 20780/2019, Cass. Pen. Sent. n. 25727/2004

⁶² Cass. Pen. n.2400/2018

⁶³ Cass. pen. sent. n. 17210/2011

Di recente, la Cassazione ha chiarito questo punto per un caso di violenza sessuale, parlando però in via generale di reati di carattere sessuale, tra cui anche il 612ter, per cui il dissenso della vittima deve ritenersi sempre presunto salvo prova contraria⁶⁴.

In ogni modo, il giudice valuterà la situazione caso per caso, secondo il suo apprezzamento; cosa che diventa difficile per l'articolo 612 ter, perché il soggetto attivo dovrebbe dimostrare di esser stato indotto in errore nel carpire l'accettazione alla divulgazione da parte della persona offesa.

Trattando invece gli effetti sulla vittima, la pubblicazione del contenuto per il quale non ha prestato il consenso, comporta gravi conseguenze nella vita della stessa⁶⁵.

A livello social-lavorativo, potrebbe essere esclusa da determinati ambiti della vita quotidiana; essendo possibile in alcuni casi il riconoscimento della vittima tramite la divulgazione anche di informazioni private come l'indirizzo di casa, il nome, il numero di telefono, come è avvenuto nel caso della maestra di Torino sopracitata.

Tuttavia, le conseguenze potrebbero anche essere di carattere psicologico: potrebbe sviluppare come meccanismo di difesa una volontà generale di non aver più alcun tipo di relazione con gli uomini, basandosi sull'idea che questi abbiano come fine ultimo quello di comportarsi allo stesso modo del suo aguzzino.

A livello inconscio le vittime potrebbero anche adottare altri comportamenti volti a proteggersi, i quali prevedono il controllo della vita e delle azioni della persona che ha diffuso le immagini, cercando di prevenire gli effetti e di poter evitare ulteriori danni alla sua quotidianità.

Tuttavia, in questo modo la vittima continua a essere inevitabilmente legata a quell'episodio senza riuscire più a distaccarsi emotivamente da chi ha commesso l'atto illecito⁶⁶.

I principali danni causati dall'accaduto son devastanti a livello psicologico⁶⁷: tra cui ansia, stress, depressione, disturbo da stress post traumatico, isolamento sociale e pensieri suicidi, la sfiducia generatasi sia nei confronti del prossimo che verso sé stessi può portare la vittima a una forte sensazione di inadeguatezza e una progressiva riduzione della propria autostima.

Secondo Bates, oppositamente, la persona sottoposta a tali livelli di stress potrebbe anche adottare un meccanismo comportamentale negativo, nel tentativo di non pensare a quanto accaduto, che potrebbe sfociare nell'evitamento, nel consumo di alcol o droghe.

Molte sono le ragazze che si sono aperte durante le interviste sull'accaduto: una vittima di diffusione illecita di immagini a sfondo sessuale di diciotto anni, dichiara in una

⁶⁴ Cass. Pen. Sez. III, n.19599/2023

⁶⁵ BATES S., *Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors*, *Feminist Criminology*, Vol. 12(1) 22–42, 2017.

⁶⁶ SORGATO A., *Revenge Porn*, Giuffrè Francis Lefebvre Spa, Milano, 2020

⁶⁷ BATES S. "Revenge Porn and mental health: a qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology*" 2016; 1-21.

intervista: «Mi viene da piangere, sono a pezzi, l'ansia non mi sta lasciando in pace un attimo. Vedere ogni volta cosa ci hanno scritto è devastante.

Vedere le foto di altre ragazze, tutto quel *Revenge porn*, mi fa venire la nausea.

È disgustoso, sono dei mostri. Il nostro corpo viene usato come merce di scambio senza considerare poi le minacce, i nomi e gli indirizzi. Ho il voltastomaco»⁶⁸.

Un caso che sottolinea il grande stato perturbante creato dalla diffusione di immagini a sfondo sessuale, senza l'approvazione della vittima, è avvenuto nel 2017: Michela Deriu, una ragazza sarda di ventidue anni, si è suicidata soffocandosi con un laccio a casa della migliore amica, a seguito della diffusione di suoi video hard.

Tre persone della cerchia di amici di Michela, sono stati iscritti nel registro degli indagati dal procuratore Gianluigi Dettori.

Questi ultimi, sere prima del suicidio, hanno ricattato la donna, estorcendole soldi per evitare di diffondere ulteriormente i filmati.

Gli inquirenti hanno valutato gli indizi andando a ritroso e cercando di ricostruire i fatti il più fedelmente possibile.

Alla fine, gli inquirenti sono risaliti alla traccia da cui il video è stato caricato in rete, che sarebbe partita da un *personal computer* appartenente a uno dei tre indagati.

A seguito del ritrovamento, sono stati sequestrati tutti i dispositivi mobili di questi ultimi.

Gli indagati sono stati accusati di tre capi di imputazione, tra cui quello di aver diffuso questi video, di aver causato la morte della vittima come conseguenza del reato di diffamazione (considerando i fatti come movente del suicidio, a causa del grave stato di turbamento arrecato, dopo che la donna ne avrebbe scoperto la diffusione) e la tentata estorsione.

La ragazza, prima di suicidarsi ha lasciato due lettere, una alla amica, e l'altra, tutta stropicciata, nella quale si riferisce a "scheletri di anni fa".

Tuttavia, Il GUP Caterina Internaldi ha dichiarato il "non luogo a procedere" per insussistenza del fatto.

Infatti, la stessa Procura di Tempio Pausania, aveva richiesto l'assoluzione, mettendo in evidenza il fatto che non c'era nessuna prova del collegamento tra la diffusione del video *hot* e il suicidio della ragazza⁶⁹.

Nel caso in cui la vittima sia un minore, le conseguenze possono essere ben più gravi⁷⁰, comportando una interruzione dello sviluppo emotivo e della formazione della personalità dell'individuo, andando a incidere sul *quomodo* relazionale della persona verso l'esterno⁷¹.

⁶⁸ intervista su Open, Fabio Giuffrida, 2021

⁶⁹ Articolo del Fatto Quotidiano, F.Q., 1° dicembre 2017

⁷⁰ Al riguardo v. Eurispes Osservatorio *Cyber Security*, *Revenge porn: la vendetta può colpire chiunque*, 17 dicembre 2019.

⁷¹ Corriere della sera, articolo di Alberto Pinna

Il fatto più eclatante, è che i minori non si rendono conto dei pericoli di *Internet* e quindi tendono ad affermare la propria sessualità nel *cyberspazio* in maniera molto più disinibita, senza pensare a una possibile diffusione incontrollata del materiale.

Prima della Riforma del Codice Rosso, ai soggetti minorenni (ultraquattordicenni) che avevano condiviso le immagini erotiche veniva contestato il reato di cessione di materiale pornografico ai sensi dell'art. 600-ter, IV c.p.

Alla persona che invece aveva conservate le foto, la detenzione di materiale pornografico ai sensi dell'art. 600-quater, c.p.⁷²

Facendo riferimento a qualche dato statistico, secondo l'organizzazione "*Cyber Civil Rights Initiative* (CCRI)", tramite uno studio effettuato durante la campagna "*end Revenge porn*" sul loro sito nel periodo che va dall'agosto 2012 a dicembre 2013⁷³, su 1606 risposte, 361 le vittime, il 93% ha affermato di aver sofferto un grande disagio emotivo per la sua condizione di vittima di *Revenge porn*.

L'82% ha dichiarato che il fatto ha avuto un grande impatto sulla loro vita e danni a livello sociale, lavorativo, il 49% ha dichiarato di aver subito stalking o di esser stato molestato dagli utenti che hanno visto il contenuto illecito, il 26% ha dovuto creare una nuova identità online e chiudere le precedenti.

Per ovviare e cercare di ridurre al massimo gli effetti di questi fenomeni, l'associazione Europea Permesso Negato ha attivato una serie di servizi messi a disposizione delle vittime.

Per esempio, il servizio attivo 24h su 24, "Primo Soccorso Psicologico", consiste in un percorso di tre consulenze virtuali per dare assistenza psicologica alle persone che hanno subito *Revenge porn*.

Inoltre, da poco, Motorola e Telefono Rosa hanno sviluppato un progetto intitolato "Non mi violare", con la collaborazione della Polizia di Stato.

Questa iniziativa punta ad informare i giovani e a sensibilizzarli su questa tematica, ma anche ad un uso più consapevole sia dei *social network* che del cellulare più in generale. Manuela De Giorgi, Primo dirigente della Polizia di Stato e Dirigente del Centro Operativo per la Sicurezza Cibernetica della Polizia Postale Lombardia, in merito a questo progetto ha affermato «Dal nostro Osservatorio emerge un incremento preoccupante delle denunce di *Revenge porn*, soprattutto fra le adolescenti, e sappiamo che tali numeri rappresentano soltanto la punta dell'iceberg, perché la vittima ha difficoltà e vergogna a denunciare.

Ma il silenzio è il peggior nemico e chi viene colpita non deve mai sentirsi sola, ma deve poter contare sul supporto e sull'aiuto di una rete di professionisti».

Questo programma fornisce accesso diretto a una guida pratica scaricabile in rete⁷⁴.

⁷² Cass., Pen., sez. III, 21 marzo 2016, n. 11675

⁷³ *End Revenge porn, a campaign of the Cyber Civil Rights Initiative*, le partecipanti sono state per lo più donne perché è la categoria che visita maggiormente il loro sito

⁷⁴ Guida disponibile sul sito ufficiale Nonmiviolare.it, Motorola in collaborazione con Telefono Rosa

Tuttavia, le modalità di prevenzione e di aiuto delle vittime di *Revenge Porn* verrà approfondito con più enfasi nel capitolo tre del presente elaborato (*Infra*, § cap. 3 parag. 3.4).

3.1 (Segue): Il caso di Tiziana Cantone

Un episodio che ha fatto Giurisprudenza è il caso Cantone definito dalla madre stessa come un caso di "femminicidio social"⁷⁵.

Tiziana Cantone venne ritrovata morta nel 2016, all'età di trent'anni, nella sua casa a Napoli, in seguito alla diffusione di suoi filmati intimi sulla rete.

La ragazza filmò nel 2015 dei video *hard* con il suo ragazzo, e in un primo momento la donna denunciò quattro uomini, che a detta di quest'ultima aveva conosciuto online, tuttavia come diremo in seguito, risulteranno essere estranei ai fatti.

Per la registrazione di sei filmati la Cantone acconsentì, ma non diede il consenso alla loro diffusione.

Questi vennero prima inviati su *whatsapp* e successivamente con una portata molto più ampia, su *Facebook* tramite la condivisione di quattro link che rimandavano a siti a sfondo sessuale.

La Cantone ottenne un provvedimento ex art 700 cod. proc. civ che ordinava la rimozione immediata dei contenuti lesivi per illecito trattamento di dati e diffamazione (*Infra*, § cap. 2 parag. 2.2).

Successivamente furono aperti altri due fascicoli, uno per il reato di violazione della privacy, l'altro su istanza della madre della vittima, di istigazione al suicidio, poiché Tiziana cantone si tolse la vita non riuscendo a sopportare il dolore.

Facebook decise di impugnare l'ordinanza emessa nel 2016 dal Tribunale di Napoli, mediante reclamo, perché riteneva che fosse cessata la materia del contendere in quanto uno dei *link* rientranti nell'oggetto dell'ordinanza non era accessibile sulla piattaforma *Facebook*.

Richiedeva inoltre, l'accertamento della violazione della precedentemente citata Direttiva "*e-commerce*" la quale prevede all'articolo diciassette, che il direttore del *social network* non ha il dovere di controllare anticipatamente i contenuti immessi dagli utenti, ma venutone a conoscenza, deve adoperare un controllo successivo per impedire l'ulteriore diffusione e caricamento dei contenuti stessi.

Inoltre, *Facebook* lamentava l'eccessiva generalità della richiesta di rimozione, visto che non erano stati forniti *URL* idonei a identificare le pagine *Facebook* oggetto di cancellazione.

⁷⁵ "Uccisa dal web – Tiziana Cantone", ROMINA FARACE, LUCA RIBUSTINI, sulla testimonianza di Maria Teresa Giglio

Il Tribunale di Napoli accoglie parzialmente il reclamo⁷⁶ disponendo l'immediata rimozione e cessazione dei *link* dalla piattaforma e di impedirne l'ulteriore caricamento. Quest'ultimo, condanna *Facebook Ireland Ltd* al pagamento nei confronti di Teresa Giglio, madre della vittima, dei 2/3 delle spese e delle competenze professionali.

Inoltre, rigetta la richiesta nella parte in cui si prevedeva che «non vi fosse un obbligo della piattaforma di intervenire vista la mancanza di un ordine di una autorità giurisdizionale o amministrativa».

Tuttavia, la parte lesa deve dimostrare, come è stato fatto con l'integrazione di documenti, che *Facebook* fosse a conoscenza di questo contenuto e che non si sia prontamente attivato, prevedendo che in caso di ritardo o inosservanza dell'ordine di rimozione, ex art 614 bis cod. proc. civ, venga applicata una somma a titolo di sanzione. Il Tribunale, infatti, inquadra *Facebook* come un "*hosting provider*", fattispecie disciplinata dall'art 14 del d.lgs. 70/2003, esonerandolo da una responsabilità diretta per l'illecito, ma prevedendone una «indiretta» nel caso di mancata attivazione per la rimozione degli effetti del contenuto dannoso.

Tuttavia, il giudice, nonostante ci fosse già un provvedimento di rimozione d'urgenza dal *web* delle immagini, non riconosceva alla Cantone il diritto all'oblio (*Infra*, § cap. 2 par. 2.2), cioè il diritto alla cancellazione dei propri dati dal *web*.

Venne inoltre condannata a rimborsare le spese legali ai siti Facebook, X, Yahoo, Google e YouTube, sui quali girò il contenuto illecito, per un totale di 20.000 euro.

A seguito di quanto appena enunciato, scaturì la seconda denuncia in procura per violazione della *privacy*.

A causa della circolazione sempre più veloce delle immagini e delle voci, insulti sul suo conto, la vittima veniva costantemente riconosciuta e derisa: infatti la madre dichiarò sui social «Sono sette anni che lotto anche contro quella che è diventata protagonista sul web e sui social: la gogna mediatica», e secondo quest'ultima è stato proprio questo a far sì che Tiziana si sentisse senza via d'uscita.

Secondo la memoria difensiva, la vittima infatti, decide di non uscire più di casa per paura, di lasciare il lavoro e di cambiare il suo cognome in quello della madre, disponendo il suo trasferimento in Toscana.

«Mia figlia aveva il timore di finire in prima pagina, di vedere violata la sua doppia fragilità[...] aveva paura di essere riconosciuta e umiliata, non voleva farsi vedere in giro»⁷⁷, dichiarò la Giglio.

Il 13 settembre 2016 Tiziana muore, apparentemente, per suicidio.

Il caso porta talmente tanto scalpore che viene nominato anche dalla *BBC*, dal *New York Times*, e la *CNN*⁷⁸.

⁷⁶ procedimento per reclamo Trib. di Napoli, n 9799/2016, II sez civile.

⁷⁷ ROBUSTINI FARACE "*uccisa dal web: Tiziana Cantone. La vera storia di un femminicidio social*".

Dalla testimonianza diretta di Maria Teresa Giglio, Jouvence, 2019.

⁷⁸ *BBC*, "*Tiziana Cantone: suicide following years of humiliation online stuns Italy*", 2016; *New York Times*, "*Viral sex tapes and a suicide prompt outrage in Italy*", 2016, GAIA PIANIGIANI

Ciò che inevitabilmente ha scosso in maniera permanente Tiziana Cantone è la velocità con cui questi contenuti sono girati e la concreta impossibilità di impedirne la circolazione, che è avvenuta in vari momenti.

Innanzitutto, il suo partner ha condiviso i video privati con un gruppo di conoscenti, in secondo luogo, alcuni di questi hanno condiviso i video con altri contatti *WhatsApp*, soggetti, che vivevano prevalentemente nell'area metropolitana di Napoli⁷⁹.

In terzo luogo, qualcuno ha pubblicato i video su portali pornografici, condividendoli con un pubblico potenzialmente vasto di utenti del web.

Infine, alcuni hanno creato sottoprodotti dei video originali (clip più brevi, video parodici) pensando si trattasse addirittura di una pubblicità per introdurre nel mercato pornografico una nuova *pornostar*, questa definizione venne attribuita dal giornale "Il Fatto Quotidiano" salvo poi scusarsi in un secondo momento per la "negligenza". Poco dopo la morte della ragazza, pertanto venne aperta una inchiesta per istigazione al suicidio⁸⁰.

Durante la fase di ricerca delle prove, venne analizzata la *pashmina* utilizzata dalla Cantone per togliersi la vita e venne sentito l'ex fidanzato Sergio di Palo.

Tuttavia, il Gip archivì il fascicolo e nessuno venne iscritto nel registro degli indagati poiché era necessario accedere ai contenuti dello *smartphone* di Tiziana, che non era possibile sbloccare.

Il secondo venne aperto a carico proprio di Sergio di Palo, nel 2018 per i reati di: calunnia, accesso abusivo a sistemi informatici e falsità privata rispettivamente secondo gli articoli 368 c.p., 615 ter c.p., 483 c.p.

L'accusa prevedeva che l'ex fidanzato, insieme alla Cantone avessero programmato di denunciare le quattro persone di diffamazione⁸¹ e violazione della *privacy*, che però per indagini successive risultano estranee ai fatti, grazie alla presenza di alcune incongruenze nelle dichiarazioni della vittima.

Infatti, queste persone avevano sì ricevuto i video, ma non c'era alcuna prova della loro diffusione da parte di questi ultimi.

Tiziana essendo già deceduta, non è stata imputata per questi fatti.

La prima udienza si è tenuta a Napoli a porte chiuse nel 2019: secondo quanto definito dall'accusa, la quale chiese 4 anni di reclusione, il fidanzato plagìò Tiziana al fine di denunciare i quattro (questa ipotesi era condivisa anche dalla mamma di lei).

L'indagato, suppostamente in un secondo momento, si sarebbe fatto aiutare da un esperto tecnico di informatica e avrebbe cancellato le prove dei video dal *computer* e dal telefono di Tiziana, perciò i legali della signora Giglio hanno parallelamente presentato un esposto anche per frode processuale, per poter analizzare l'iter dell'attività di estrapolazione dei dati e del *modus operandi* dell'analisi condotta dalla polizia giudiziaria, poiché secondo la donna i dati non sarebbero stati estratti

⁷⁹ FILIPPO FACCI, *Storia di Tiziana Cantone*, IL POST, (Sept. 15, 2016)

⁸⁰ LEANDRO DEL GAUDIO, *La morte di Tiziana, il Pm chiede il processo per l'ex compagno*, IL MATTINO, (May 20, 2018, 2:04 AM)

⁸¹ articolo 595 c.p., Stefano Canestrari et Al., *Manuale di Diritto Penale* 594 (2d ed. 2017)

correttamente a causa della mancata rilevazione della polizia giudiziaria di alcun dato rilevante negli apparecchi della vittima.

La difesa sostenne che l'imputato ha sempre cercato di aiutare l'ex fidanzata pagando sia le spese legali che quelle per la psicoterapia.

Il Tribunale di Napoli decise quindi per l'assoluzione di Sergio di Palo, con le seguenti formulazioni: per la falsità con forma "il fatto non sussiste", per l'accusa di calunnia con "il fatto non costituisce reato", dall'accesso abusivo al profilo *Facebook* di lei, per "improcedibilità" perché è un reato procedibile a querela e quest'ultima era mancante, e dalla simulazione di reato perché "il fatto non sussiste"⁸².

La madre di Tiziana è stata affiancata dall' "Emme Team", una squadra di investigatori informatici di *Los Angeles*.

Questi ultimi si dichiaravano in possesso di prove di una manomissione degli strumenti di *iPhone* e *tablet* quando questi erano nello stato di sequestro.

Secondo loro, risulterebbe un accesso al cellulare e una successiva cancellazione dei dati *post mortem* della vittima, più precisamente tre giorni dopo.

Tuttavia, per i periti della procura il telefono era inaccessibile per la presenza del pin. In totale, le incongruenze suppostamente riscontrate da questo gruppo di investigatori sarebbero diciannove, e queste, a detta loro, sono risultate fondamentali per la compromissione delle indagini.

Altre anomalie riscontrate riguardano la cronologia eventi e *browser* Internet dell'*IPad*, consegnata alla fine delle indagini vuota, «come se per tutto il tempo in cui è stato nella disponibilità di Tiziana Cantone, non sia mai stato utilizzato o connesso al web». È stato in seguito possibile dimostrare, a detta di questi investigatori, che l'attività era presente e che è stata cancellata.

Lo strumento usato dalla vittima è stato poi «restituito alla madre, con la totale assenza di messaggi, rubrica e account per l'utilizzo del dispositivo stesso»; è stata anche accertata, a detta loro, «la totale assenza di messaggi, video, musica e attività connessa con *Itunes nell'IPad* per anni utilizzato da Tiziana», «Dal controllo della Mappe e della posizione del dispositivo nel tempo, si è altresì appurato la mancata presenza di attività, malgrado questo dispositivo fosse stato usato da Tiziana Cantone per svariati anni»⁸³. Anche se la cronologia del telefono non era presente, dalle indagini emergono, alla riapertura di Safari «4 pagine web, ma nessuna nei mesi prima della morte di Tiziana. Unica spiegazione logica e tecnica è che la cronistoria sia stata volontariamente cancellata. Azione che non può di certo avvenire in automatico da parte del sistema»⁸⁴.

L'emme Team, nel settembre 2021 ha deciso di “chiarire” alcuni aspetti di queste incongruenze, tramite i suoi portali: secondo alcuni, Tiziana era stata trovata morta in cantina, mentre la verità, secondo loro, è che è stata trovata in taverna, ambiente che

⁸² Giudice Dario Gallo, Tribunale di Napoli, sent. di assoluzione 8 novembre 2022

⁸³ dichiarazioni dell'Avv. Pettorossi durante delle interviste

⁸⁴ informazioni estrapolate da intervista di Martina Capit, Fidelitynews, 2020 Tiziana cantone: anomalie nei cellulari usati per Revenge porn, ridotti a tabula rasa

aveva una entrata indipendente rispetto al resto della casa, ingresso non visibile a chi si trova ai piani superiori.

Inoltre, secondo il *Team*, molti hanno fatto passare delle "*fake news*" su *internet*, in merito alla analisi della pashmina e degli strumenti elettronici di Tiziana.

Questi sono stati sottoposti a una prima verifica da personale esterno a Emme *Team*, poi dai consulenti Emme e successivamente passati a due Università, una straniera ed una italiana, che ne hanno confermato la precisione.

Il gruppo di esperti, dicono, non ha voluto diffondere l'inezzezza delle informazioni proprio al fine di scovare le *fake news*.

I dati inerenti al traffico internet del telefono sono stati forniti e certificati da: *Vodafone, Libero, Gmail e Facebook, Inc.*

Il *team* ha riportato notizie inerenti al caso, le più importanti: il solco al centro del corpo della vittima, risultante come non compatibile ad una eventuale impiccagione e un secondo segno evidentemente realizzato *post mortem* a simulare il suicidio⁸⁵.

A sostegno di ciò il Prof. Mariano Cingolani, Ordinario di Medicina Legale presso l'Università degli Studi di Macerata e già perito nel caso Meredith Kercher, è arrivato alla medesima conclusione: sul collo della vittima non è presente una singola lesione, come affermato in modo errato dalla procura, ma due solchi.

Secondo il Professore, un solco è da strangolamento, e l'altro da impiccagione; tuttavia, il medico legale che nel 2016 si è occupato dell'analisi dei solchi, li ha indicati entrambi ma ha deciso di tenerne in considerazione solo uno, concludendo per il suicidio.

L'emme *team* dichiarava anche di aver eliminato dalla rete, mediante il ritrovamento degli indirizzi IP, di tutti i video che circolano di Tiziana Cantone.

Come ben sappiamo a causa della mancata possibilità di eliminare totalmente il contenuto dal web, sorgono dubbi sulla veridicità delle affermazioni di questa agenzia statunitense.

Loro stessi parlano di *fake news*, ma in realtà sono loro che hanno diffuso notizie inventate o parzialmente modificate.

Infatti, analizzando più nel dettaglio le vicende pregresse, si ritiene che questa società sia truffaldina⁸⁶.

Molti personaggi, come Roberta Bruzzone, l'avvocato Annamaria Bernardini De Pace e la psicologa Maria Rita Parsi sono state truffate da queste "società" e dalla persona che la gestisce: Mirko Zeppellini.

Anche la giornalista Selvaggia Lucarelli in un articolo pubblicato nel 2020 su TPI aveva sollevato dubbi sui dati forniti nel caso Cantone; ci fu persino un servizio delle Iene in merito.

La procura campana, tramite il Pm Giovanni Corona ha iscritto nel registro degli indagati per associazione a delinquere finalizzata alla frode processuale, per calunnia e

⁸⁵ operazioni di esame necroscopico presso l'obitorio comunale di Napoli, presso l'AUP Federico II, 14.09.2016

⁸⁶ Corriere della Sera, "Emme team di Mirko Zeppellini, cos'è e cosa c'è dietro alla società tornata alla ribalta per il caso Biondo", di Redazione Login, 8 agosto 2023

truffa il gruppo Emme team, tra cui Zeppellini, l'Avv. Salvatore Pettirossi, l'Avv. Luciano Faraone, e il consulente Mirko Miele.

Secondo il Pm Corona, l'associazione ha "confezionato dei falsi", infatti il Dott. Agostini che aveva analizzato la pashmina ha ammesso di aver condotto una analisi superficiale, mentre Miele avrebbe ammesso durante l'interrogatorio di aver messo in atto una relazione fasulla, egli stesso insieme al consulente Lorenzo Laurato avrebbero smentito la tesi di manomissione dei cellulari.

Il Pm Corona definisce le azioni di questa "società" come «inutili indagini su casi chiusi ma dotati di notevole appeal televisivo»⁸⁷.

Tornando ai fatti di cronaca, il terzo fascicolo viene ad esistenza il 28 maggio 2021 quando la madre della vittima fa richiesta al Pm Giovanni Corona di riesumazione del corpo per disporre l'autopsia che non venne mai eseguita, perché non crede che la figlia si possa esser suicidata.

A sostegno della sua tesi Il gruppo di Emme *Team* dichiarò di essere in possesso di vari elementi: tra questi, di rilievo è il ritrovamento sul foulard del DNA, oltre che della madre e della zia, che fu la prima a rinvenire il corpo esanime della giovane, anche di tracce biologiche maschili, per questa ragione venne predisposta l'apertura del fascicolo di omicidio contro ignoti.

La madre della vittima richiese anche l'aiuto della criminologa Roberta Bruzzone per farsi assistere nelle indagini.

Invero il Gip di Napoli Raffaele Coppola dispose ulteriori indagini, a seguito dell'opposizione presentata contro l'archiviazione del procedimento dai difensori della madre della vittima, analizzando la concreta possibilità che Tiziana possa essere morta per l'asfissia da impiccagione utilizzando la sciarpa ritrovata al suo collo e legata all'attrezzo per fare ginnastica, in correlazione alla posizione in cui il suo corpo è stato ritrovato.

Secondo quanto verificato dal biologo forense Vincenzo Agostini, interpellato per il caso, il foulard non potesse aver ucciso per strangolamento Tiziana, perché posizione del corpo rendeva impossibile il "penzolamento con conseguente asfissia".

Secondo il Gip Coppola, «lo stato scheletrico del corpo, riesumato nel maggio 2021 a distanza di cinque anni dalla morte rende impossibile qualsivoglia valutazione sulle consulenze di Pm e parte offesa», cioè sulle perizie medico-legali eseguire sul corpo di Tiziana; ciononostante assumono rilevanza le consulenze relative alla dinamica della morte, che posto un interrogativo importante relativamente all'ipotesi del suicidio, pertanto secondo il Gip, «si può ipotizzare una metodica asfittica riconducibile a strangolamento al pari di un soffocamento da suicidio».

Secondo I medico-legali Vittorio Fineschi e Aniello Maiese, i consulenti della Procura avrebbero omesso di esaminare durante l'autopsia la cosiddetta "vitalità del solco", che

⁸⁷ intervista al Fatto Quotidiano di Vincenzo Iurillo, 11 Gennaio 2024

può dare maggiori informazioni sul *quomodo* della morte, se è stata effettivamente causata “da una meccanica di impiccamento o strangolamento”⁸⁸.

La Procura quindi si è occupata, tramite esperimento giudiziale, dell’accertamento riguardante la compatibilità della sciarpa, dell’attrezzo ginnico e della posizione in cui il corpo è stato ritrovato, con un decesso per asfissia da impiccagione; tuttavia, gli esiti non portarono alcuna traccia di eventuali strangolamenti.

Da ultimo, concluse le ulteriori indagini condotte dal Pm Corona, non sono stati rinvenuti elementi sufficienti che possano portare a una disposizione di giudizio per omicidio volontario contro ignoti.

Analizzando anche i dati che emergono dalla riesumazione del cadavere richiesto dalla madre della vittima non sono state riscontrate informazioni utili, pertanto, il Giudice Coppola ha deciso per l’archiviazione del caso.

Questo evento di cronaca ha creato talmente tanto scalpore che ha posto l’attenzione sulla necessità di una svolta a livello legislativo riguardante i fenomeni di *Revenge porn* e di *cyber-bullismo*.

Il caso Cantone venne pertanto discusso in Senato dalla settimana successiva alla morte della donna.

È stata portata avanti una vera e propria campagna di sensibilizzazione per cui, alla fine, si è deciso di approvare una legge per la prevenzione e il contrasto del *cyber-bullismo*⁸⁹.

Inoltre, questo caso ha posto le basi per l’introduzione all’interno del "Codice Rosso" dell’emendamento che introduce il *Revenge porn*, derubricato diffusione illecita di immagini o video sessualmente espliciti, come reato nel c.p. (*infra* § parag. 2 cap. 2).

In conclusione, Il giorno dopo l’approvazione alla Camera Teresa Giglio afferma: «Ciò che ha subito Tiziana non ha eguali in nessuna parte del mondo e sono contenta che finalmente chiunque si trovi in una situazione simile oggi possa sapere di avere la legge della propria parte».

⁸⁸ ansa.it edizione del 15 febbraio 2023 Napoli

⁸⁹ Legge n.71/2017 «Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo» (17G00085) (GU Serie Generale n.127 del 03-06-2017) entrata in vigore il 18/06/2017.

3.2 (Segue:) *Internet e Revenge Porn*, pericoli e insidie per i minori

A causa del sempre più frequente uso degli strumenti tecnologici, di videogiochi, di *social network* da parte dei più giovani, si è sviluppato il fenomeno della "deresponsabilizzazione".

Proprio per la loro giovane età, questi non riescono a formulare un pensiero critico sulle effettive conseguenze che potrebbero esserci, sia dal punto di vista legale alla propria persona, sia dal punto di vista psicologico verso della vittima.

Per questo, la tutela dei minori dai reati di carattere sessuale, compreso il *Revenge porn*, è diventato un argomento di vitale importanza.

È fondamentale, infatti, che i genitori avviino un controllo a tutto tondo sull'uso dei dispositivi elettronici dei figli, per monitorare il loro comportamento online.

È anche molto diffusa oggi, la pratica dei genitori stessi di condividere immagini dei propri figli sui *social network*, le quali possono poi essere viste potenzialmente da malintenzionati e utilizzarle come materiale pedopornografico o utilizzarlo per ricattare gli stessi genitori.

Secondo il GDPR, il regolamento generale sulla protezione dei dati (UE/2016/679) i parenti possono utilizzare alcune accortezze per evitarne l'uso da parte di terzi delle immagini, come rendere irriconoscibile il viso del minore o coprirlo con faccine, oppure limitare la propria *privacy* dei profili *social* solo alle persone che si conoscono. Il Tribunale di Roma ha stabilito con una ordinanza del 2017⁹⁰ che il giudice può disporre la rimozione delle immagini e il pagamento di una somma di denaro in favore dei figli.

Non sono pochi i casi giurisprudenziali: infatti, nel 2017 e 2019 si sono espressi i giudici del Tribunale di Mantova⁹¹ sulla questione, definendo necessario l'assenso di entrambi i genitori per la pubblicazione di foto dei figli in rete, prevedendo che la pubblicazione «determina la diffusione delle immagini fra un numero indeterminato di persone, conosciute e non, le quali possono essere malintenzionate e avvicinarsi ai bambini dopo averli visti più volte in foto *online*.

Non si può inoltre non fare riferimento all'ulteriore pericolo costituito dalla condotta di soggetti che "taggano" nelle foto i minori e, con procedimenti di fotomontaggio, ne traggono materiale pedopornografico da far circolare fra gli interessati, come ripetutamente evidenziato dagli organi di polizia».

Un esempio di quest'ultima condotta è "*Bikini Off*", una applicazione che utilizza l'intelligenza artificiale e algoritmi *deepfake* (*infra*, § parag. 3 cap. 3) che ha come scopo quello di utilizzare foto reali e creare immagini di nudo basate su queste ultime, quindi creando materiale pedopornografico.

⁹⁰ Trib. di Roma, 23 Dicembre 2017, procedimento n. 39913/2015

⁹¹ Trib. di Mantova, ricorso n. 2881/17, 19 settembre 2017

Questo programma di *deepfake* può essere utilizzato mediante il *social network* Telegram, e al momento non è previsto un limite di età per l'utilizzo di questa applicazione.

Il giornale La Repubblica, ha raccontato un episodio per cui due quattordicenni sono stati indagati di diffusione di materiale pedopornografico (art 600 ter c.p. il quale prevede una pena fino a quattordici anni di reclusione) per aver preso immagini di due compagne di scuola e averle spogliate mediante l'uso di questa *app* e successivamente le hanno fatte circolare su *whatsapp*.

Tuttavia, il Gip Federico Falzone ha deciso di archiviare le indagini e di non procedere contro gli adolescenti, descrivendo il fatto come «imprudenza ascrivibile a leggerezza tipicamente giovanile» sottolineando che *l'app* era accessibile a tutti, che i due ragazzi siano incensurati e che si siano impegnati prontamente a eliminare le foto, considerandola questa una sorta di condotta "risarcitoria".

Un altro caso rilevante riportato dalla Corte di Cassazione è quello per cui un soggetto adulto aveva inviato tramite *whatsapp* numerosi messaggi sessualmente espliciti ad un minore, costringendola tramite minaccia a scambiare tra le altre cose, immagini erotiche: questa condotta secondo la Cassazione integra anche il reato di violenza sessuale⁹².

Tuttavia, l'episodio più sconvolgente successo in Italia, in materia di minori e tutela digitale del *cyberspazio*, è il caso di Carolina Picchio, ragazza di quattordici anni che nel 2013, dopo aver visto caricato *online* un suo video in cui era ubriaca e alcuni conoscenti le si sono avvicinati simulando atti sessuali, effettuando insinuazioni e comportamenti espliciti; il video diventa virale.

La ragazza non riesce a sopportare la quantità di odio che riceve in seguito, e decide di suicidarsi buttandosi dalla finestra della sua camera.

Prima di questo gesto estremo, ha scritto una lettera nella quale descriveva l'accaduto e dava i nomi dei colpevoli, in quest'ultima si legge "Le parole fanno più male delle botte. Ciò che è accaduto a me non deve più succedere a nessuno".

I cinque ragazzi coinvolti vennero sottoposti a un periodo di messa alla prova, in quanto tutti minorenni.

Il Tribunale di Torino li dichiarava come "colpevoli e pentiti"⁹³ dei reati a loro ascritti: morte come conseguenza di altro reato (*stalking*), detenzione di sostanze stupefacenti, violenza sessuale di gruppo (contestata a tre di loro), diffamazione, detenzione e divulgazione di materiale pornografico (queste ultime erano alcune delle fattispecie che si applicavano in mancanza di una legge sul *Revenge porn*, argomento che approfondirò più avanti) (*Infra*, § cap. 1 Parag.4).

Il padre di Carolina ha, nel corso degli anni, contribuito ad effettuare molte campagne di prevenzione e sensibilizzazione nelle scuole, per evitare che episodi simili possano

⁹² Cfr. Cass. Pen., sez. III, 8 settembre 2020, n. 25266, Nello stesso senso, cfr.: Cass. Pen, sez. III, 16 giugno 1994, n. 8453; Cass. Pen., sez. III, 26 marzo 2013, n. 19033; Cass. Pen. sez. III, 30 ottobre 2018, n. 17509.

⁹³ La stampa, 19 dicembre 2018, Marco Benvenuti

di nuovo accadere ed ha anche istituito la “Fondazione Carolina”, insieme ad esperti del settore.

Prima del 2013, non si parlava ancora di *cyber bullismo*, ma grazie a lei nacque la prima legge sulla prevenzione e educazione al *cyber bullismo* in Italia, diventata ufficialmente legge nel 2017⁹⁴.

La nuova legge definisce il “bullismo telematico” all’articolo uno comma secondo, come «Qualsiasi forma di pressione, molestia [...] diffamazione, acquisizione illecita, denigrazione, trattamento illecito di dati personali in danno a minorenni, realizzata per via telematica [...] il cui scopo sia quello di isolare un minore ponendo in atto un serio abuso, un attacco dannoso o la messa in ridicolo»⁹⁵.

Guardando qualche dato, il Garante della *privacy* nella relazione annuale del 2020 ha evidenziato dei dati statistici secondo cui si è registrato un incremento di circa il 132%, rispetto al 2019, dei casi trattati dal Centro nazionale per il contrasto della pedopornografia e un aumento del 77% dei casi di vittimizzazione dei minori per *grooming*, *cyberbullismo*, furto d’identità digitale, *sextorsion*.

I minori infatti vengono ricompresi da molte fonti regolamentari, nella categoria degli “interessati vulnerabili”⁹⁶.

Il Considerando n. 75 del GDPR, istituisce «una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali».

Da tenere in considerazione è anche l’art 8 GDPR, il Regolamento Generale sulla protezione dei dati, il quale pone un limite legale di età per il consenso: «Qualora si applichi l’articolo 6, paragrafo 1, lettera a), per quanto riguarda l’offerta diretta di servizi della società dell’informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno sedici anni.

Ove il minore abbia un’età inferiore ai sedici anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale».

Tuttavia, il Regolamento consente agli Stati Membri di fissare autonomamente la soglia, purché non venga collocata sotto i tredici anni, per l’Italia è stato fissato a quattordici anni⁹⁷.

⁹⁴ Legge n.71, 29 maggio 2017, il 17 maggio l’aula di Montecitorio vota unanime il disegno di legge a tutela dei minori per la prevenzione ed il contrasto al *cyberbullismo*. La presidente della Camera, Laura Boldrini, dedica l’approvazione a Paolo Picchio e a sua figlia Carolina

⁹⁵ G.U. legge n. 71/2017

⁹⁶ A. MANGIONE, *La tutela penale del minore da violenze, abusi e sfruttamento a sfondo sessuale*, in *La giustizia penale minorile: formazione, devianza, diritto e processo*, Terza edizione, A Pulvirenti (a cura di), Milano, Giuffrè Francis Lefebvre, 2020

⁹⁷ recita la normativa del Codice penale art 609-quater comma 1 “Un maggiorenne può compiere atti sessuali consenzienti con minori, se hanno compiuto 14 anni”, Codice Penale commentato, Giorgio Lattanzi, Giuffrè, 2024

Quindi per tutti quei servizi di informazione che utilizzano dati di minori, se non si è raggiunta l'età necessaria per l'approvazione consapevole, prevista dalla norma in esame, serve l'assenso del soggetto che detiene la potestà genitoriale.

Di rilievo è la pronuncia delle Sezioni Unite⁹⁸ in cui si afferma la liceità della pornografia domestica, definita nella pronuncia in esame come «la condotta di chi realizza materiale pornografico in cui sono coinvolti minori che abbiano raggiunto l'età del consenso sessuale nei casi in cui tale materiale è prodotto con il consenso di tali minori e unicamente a uso privato delle persone coinvolte».

Con questa specificazione, si prevede quindi la possibilità di detenzione di suddetto materiale con il consenso dei soggetti coinvolti e solo per fini personali, onde evitare, secondo la Corte, una «iper-criminalizzazione delle condotte, [...] data l'appartenenza di queste ultime all'ambito della autonomia privata sessuale».

Per questa ragione, al fine di rispettare i principi fondamentali del diritto di ragionevolezza e di offensività⁹⁹, si vuole dare rilevanza penalistica solo alle condotte concretamente lesive dei beni giuridici di riferimento.

In relazione a quanto previsto dal Regolamento, molte piattaforme *social* hanno posto un freno alla possibilità del minore di agire indisturbato su *Internet*: come *YouTube*, che a tutela di questi ultimi ha introdotto la possibilità di usufruire della piattaforma, seguendo quanto stabilito dai termini di servizio *Google*, ai bambini che non hanno meno di tredici anni¹⁰⁰.

Si è istituito anche il servizio "*YouTube Kids*" che è l'unica area per i minori di tredici anni che consente ai bambini di utilizzare il servizio in modo più autonomo, ma in un ambiente maggiormente controllato.

Pertanto, se non venisse posto un freno o un controllo alle attività del minore online questo potrebbe essere esposto potenzialmente a una serie illimitata di rischi come il venire a contatto con malintenzionati, essere vittima di *cyber bullismo* o pedopornografia, all'esposizione dei propri dati personali su *internet* e le proprie abitudini.

I giovani, essendo anche facilmente influenzabili, sono soggetti anche a "giochi pericolosi" che nascono sui *social network*: come quello che anni fa spopolava chiamato "*Blue Whale challenge*", un gioco di origine russa che spingeva i ragazzi al suicidio come conclusione di una cinquantina di sfide assegnate da un "*tutor*".

In merito la Corte di Cassazione si è espressa nel 2017¹⁰¹ prevedendo l'integrazione del reato di adescamento di minore all'art 609 *undecies* c.p., il quale recita «Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso

⁹⁸ Cass. Pen. S.U. n.51815/2018

⁹⁹ Per una analisi sul tema vedi: a cura di A. MASSARO- M. TRAPANI, *Temi penali*, Giappichelli, 2013; R. GALLI, *Nuovo corso di diritto penale*, Wolters Kluwer, 2017; A. SCAFFIDI, *Il principio di offensività e le forme di anticipazione della tutela giuridica*, in *Diritto.it*, 18.03.2021

¹⁰⁰ termini di servizio YouTube consultabili sul sito ufficiale

¹⁰¹ Cass. Pen, sez. V, Sent. n. 57503 del 22 dicembre 2017 (ud. del 23 novembre c.a.)

artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete *internet* o di altre reti o mezzi di comunicazione».

Incriminato, in particolare, è un messaggio inviato dal *tutor* alla minorenni «Manda un audio in cui dici che sei mia schiava e della vita non ti importa niente e me la consegna». Da definire è anche la condotta, molto in voga, del cosiddetto "*selfie*" a sfondo sessuale prodotto dal minore stesso, il quale però secondo la Giurisprudenza antecedente alla riforma dell'art 612 ter, non è stato considerato come rientrante nell'art 600 ter c.p. sopracitato, nel caso in cui il materiale pedopornografico consista in autoscatti.

Questa novità è stata introdotta dalla Cassazione nel 2016 (*infra*, § cap. 1 par. 3.3) prevedendo che se il minore in maniera consapevole, non indotta, e quindi del tutto volontaria, ha prodotto con autoscatto e inviato questo tipo di materiale a terzi, questi ultimi non sono punibili secondo l'art 600 ter e quater, *indi per cui* la minore non può ritenersi "utilizzata" (*Infra*, § cap. 2 par. 2.1) da soggetti terzi altrimenti si svilupperebbe una analogia in *malam partem*¹⁰².

Parimenti, sarà configurabile il reato se il minore è sotto costrizione o minaccia (*Infra*, § cap. 1 par. 3.3).

A livello sovranazionale, sono varie le fonti di tutela: è stato da poco adottato il *Digital Service Act* (DSA)¹⁰³ nel 2022 che pone come obiettivo quello di creare un ambiente sicuro sulla rete (*infra* § cap. 3 par. 1.3)

Rilevante è la Convenzione sui diritti dell'infanzia e dell'adolescenza approvata dall'Assemblea generale delle Nazioni Unite il 20 novembre 1989, la quale all'articolo 34 stabilisce che gli Stati Parte si impegnano a proteggere il fanciullo contro ogni forma di sfruttamento sessuale e di violenza¹⁰⁴.

L'Unione Europea ha inoltre emanato la decisione quadro GAI n. 68/2004¹⁰⁵ in materia di lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile, con la quale vengono stabilite sanzioni proporzionate, dissuasive ed efficaci¹⁰⁶.

L'Ue, inoltre, per poter integrare la disciplina alla luce dei significanti risultati dei dati statistici riguardanti i reati sessuali sui minori, ha avvertito l'esigenza di intervenire di nuovo sull'argomento, rendendo più omogenee le normative nazionali.

Per questo nei "Considerando" n. 4 e 5 è stata introdotta la definizione di "Pornografia infantile": materiale illecito che ritrae o rappresenta visivamente «un bambino (persona

¹⁰² Cass. Pen. Sez. III, 18 febbraio 2016, n 11675; in Dir. & Giustizia, 2016, 15,42 con nota di ALOVISIO e in ilpenalista.it, 2 maggio 2016, con nota di Ventura.

¹⁰³ *Digital service Act* approvato come Regolamento UE 2022/2065, è un regolamento dell'UE per modernizzare e ampliare la Direttiva sul commercio elettronico 2000/31/CE

¹⁰⁴ La ratifica in Italia è avvenuta con legge 27 maggio 1991, n. 176, depositata presso le Nazioni Unite il 5 settembre 1991. Il Parlamento nazionale, a causa di questa legge ha inserito all'interno del Codice gli art. 600bis ss. c.p. con la legge 3 agosto 1998, n. 269.

¹⁰⁵ Direttiva sostituita dalla n.92 del 2011

¹⁰⁶ Considerando n. 10: «Le caratteristiche specifiche della lotta contro lo sfruttamento sessuale dei bambini debbono indurre gli Stati membri a stabilire, nel loro diritto nazionale, sanzioni efficaci, proporzionate e dissuasive. Tali sanzioni dovrebbero inoltre essere adottate in linea con l'attività svolta dalle persone giuridiche».

di età inferiore a diciotto anni) reale implicato o coinvolto in una condotta sessualmente esplicita, fra cui l'esibizione lasciva dei genitali o dell'area pubica, oppure immagini di un bambino inesistente implicato o coinvolto nella medesima condotta».

Nel 2002 è stata introdotta la Direttiva n 58 del Parlamento Europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. Direttiva relativa alla vita privata e alle comunicazioni elettroniche), il cui ambito di applicazione è stato esteso dal "Codice europeo delle comunicazioni elettroniche", istituito con la Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio.

Il Consiglio d'Europa ha emanato la Raccomandazione R (2001)16 sulla protezione dei minori contro lo sfruttamento sessuale, la Convenzione di Budapest sul Cybercrime (2001) e la Convenzione di Lanzarote (2007).

Secondo quest'ultima, gli Stati Membri devono sanzionare la produzione, la messa a disposizione, la diffusione, l'offerta ed il possesso di materiale pedopornografico.

In base all'art. 20, par. 3, agli Stati Membri è stata concessa la facoltà di non punire il possesso di pedopornografia soltanto nei casi in cui abbia ad oggetto rappresentazioni simulate o immagini realistiche di minori, non esistenti o comunque immagini prodotte dagli stessi minori con il loro assenso e per un utilizzo privato.

In particolare, mediante ratifica da parte dell'Italia nel 2012 di questa Convenzione, sono stati introdotti nel Codice penale i reati di adescamento di minorenni (art. 609-undecies), perpetrati anche attraverso l'utilizzo di *Internet*, e di istigazione e apologia di pratiche di pedofilia e di pedopornografia (art. 414-bis c.p.).

Anche L'AGCOM si è mossa indicando una consultazione pubblica il 16/22 al fine di deliberare delle linee guida per l'attuazione dell'art 7 bis del decreto legislativo 30 aprile 2020 n 28 intitolato "Sistema di Protezione dei minori nel cyberspazio".

In queste ultime, si delinea un sistema che dà la possibilità ai siti internet di adottare il "*parental control*" ossia un filtro capace di oscurare i contenuti che non sono adatti per i minori e bloccare questi ultimi se non si sono raggiunti i diciotto anni di età. Solo il titolare del contratto ha la facoltà di disattivazione, il quale è soggetto a identificazione. Da tenere in considerazione è anche il fatto che reati di matrice sessuale contro i minori, come il *Revenge porn*, possono essere ricompresi nella categoria più ampia del *cyber bullismo*, ponendo come oggetto della condotta penalmente rilevante la diffusione delle immagini sessualmente esplicite.

La normativa di riferimento è la legge 29 maggio 2017, n. 71 il cui obiettivo è quello di agire preventivamente, sia in caso in cui il minore sia vittima della condotta che invece sia il perpetrante, assicurando un intervento da parte delle istituzioni scolastiche, di pronta rimozione del contenuto.

3.3 (Segue): Le nuove sottocategorie di *Revenge Porn* e i fenomeni ad esso associati

A causa dello sviluppo sempre più celere del fenomeno del *Revenge porn* e della evoluzione continua della tecnologia, sono venute ad esistenza altre fattispecie di reato che sono meritevoli di tutela e per le quali si auspica che il legislatore introduca delle discipline *ad hoc* nel Codice penale.

Uno dei più diffusi sia tra giovani che tra adulti, è il "*sexting*"¹⁰⁷, termine di matrice anglosassone.

Il termine costituisce l'unione di due parole inglesi "*sex*" e "*texting*" e indica lo scambio di messaggi, foto o video a sfondo sessuale tra due persone, prevalentemente partner o soggetti tra cui intercorre una relazione amorosa, mediante l'utilizzo di telefoni o altri strumenti informatici.

Questa modalità di "comunicazione" è prodromica al reato di diffusione illecita di immagini di carattere sessuale, in quanto porta alla condivisione di foto intime, che potrebbero essere divulgate a più persone.

Secondo una analisi condotta da ANSA¹⁰⁸ questo tipo di condivisione è sempre più frequente; infatti, uno studio dichiara che il 55% delle ragazze ha inviato messaggi di questo tipo e per i ragazzi il 52%, tra i 13 e i 19 anni, con picchi del 75% tra i più grandi.

Secondo un ulteriore studio, circa l'80% dei casi di *Revenge porn* sono costituiti dalla diffusione non consensuale di fotografie auto-scattate ed inviate al partner sessuale (Madigan et al., 2018).

La dottrina definisce il "*sexting* primario", la condotta di invio, di solito consensuale, da parte dello stesso protagonista delle immagini o del testo (potrebbe però non essere consensuale, infatti in proposito, pare opportuno riportare questa fattispecie con il fenomeno del c.d. "*upskirting*", ovvero la prassi di scattare foto alle donne in luoghi pubblici sotto la gonna (o dentro la scollatura, c.d. "*down blouses*").

In questi casi, sebbene avvenga la pubblicazione di immagini prive di riferimenti alla persona ritratta, si pone maggiormente attenzione in riferimento all'aspetto della molestia nel ricevere una fotografia indesiderata in una zona intima.)¹⁰⁹.

Invece, il "*sexting* secondario" viene descritto come il caso in cui il destinatario la diffonda a terzi estranei al rapporto con la vittima.

Secondo alcuni studi in materia, chi pratica *Revenge porn* tramite *sexting* tende a una maggiore competizione intrasessuale e a bassi livelli di empatia.

Questi tratti sono legati molto spesso ad elevati livelli di impulsività ed aggressività, ma anche la manipolazione interpersonale, che molto spesso viene utilizzata per

¹⁰⁷ QUAYLE, E. *Self-produced images, sexting, coercion and children's rights*. ERA Forum23, 237–251 (2022)

¹⁰⁸ ansa.it articolo del 10 luglio 2024 di Antonio Michienzi

¹⁰⁹ Sul tema, C. MCGLYNN, J. DOWNES, *We Need a New Law to Combat "Upskirting" and "Downblousing"*, in *Inherently Human*, 2019.

convincere la vittima, anche con la psicologia inversa, ad inviare foto pornografiche, in questo modo quest'ultima si sentirà in colpa e accetterà la richiesta, sopraffatta dalla situazione¹¹⁰.

Mentre nella vittima, sempre secondo questi studi, da una analisi effettuata sulla loro salute mentale, si nota che gli effetti derivano tanto dall'esposizione non consensuale delle loro immagini alla mercè altrui, quanto alla stessa rappresentazione di sé durante un atto intimo.

Tuttavia, anche il semplice raccontare l'abuso subito, provoca danni a livello psicologico, come per esempio episodi di stress post traumatico¹¹¹.

La Cassazione Penale si è espressa varie volte sulla questione: con sentenza del 2016¹¹², che aveva ad oggetto il caso di una minore che si era scattata delle foto a contenuto pornografico e le aveva inviate a propri coetanei, che a loro volta, senza alcun consenso, le hanno cedute a terzi, salvo un ragazzo che le teneva per sé.

Ai minori si contestava il reato di cessione di materiale pedopornografico di cui all'art. 600 *ter* comma 4 c.p. mentre all'imputato che aveva tenuto per sé l'immagine si contestava la fattispecie di cui all'art. 600 *quater* c.p.

Nel caso di specie la produzione del materiale pornografico era avvenuta in maniera volontaria da parte della minore¹¹³, mediante *sexting*, ma mancavano i requisiti giuridici della diversità dell'autore della condotta rispetto al minore sfruttato, di conseguenza veniva meno la strumentalizzazione del minore, non potendosi ritenersi integrata la fattispecie di reato prevista dall'art. 600 *ter* c.p., per questo il giudice prevedeva la formula del "non doversi procedere" per "insussistenza del fatto".

Successivamente la Cassazione si è di nuovo espressa sul tema per un caso avvenuto nel 2018¹¹⁴ dove si riteneva che la vittima fosse stata "costretta" mediante richieste passive e ripetute dell'ex fidanzato di mandargli *selfie* erotici, che poi avrebbe condiviso con un amico su Facebook.

In questo caso verrebbe meno la caratteristica fondamentale del *sexting* primario, che è la consensualità, poiché la condotta è avvenuta mediante "costrizione passiva"; mentre potrebbe configurarsi la fattispecie di *sexting* secondario, visto che il perpetratore del reato ha inviato senza accettazione della vittima, le immagini a terzi; condotta che lo ha portato a una condanna di tre anni di reclusione e una multa di diciottomila euro.

Tuttavia, in questo caso si potrebbe configurare una forma di *Revenge porn* svincolata dal carattere di "vendetta" tipica della fattispecie, ma pur sempre con la stessa volontà

¹¹⁰ VERONICA V., DI GIACOMO D., "Implicazioni psicologiche del fenomeno del *Revenge porn*: prospettive cliniche", gennaio - febbraio 2022, vol. 57 n.1 *Riv Psichiatrica* 2022;57(1):10-17

¹¹¹ BATES S. "Revenge Porn and mental health: a qualitative analysis of the mental health effects of *Revenge porn* on female survivors". *Feminist Criminology* 2016; 1-21.

¹¹² Cass. Pen. Sez III, 18 febbraio 2016, n 11675; in *Dir. & Giustizia*, 2016, 15,42 con nota di Alovio e in *ilpenalista.it*, 2 maggio 2016, con nota di Ventura.

¹¹³ ROSANI D., *Il trattamento penalistico del sexting in considerazione dei diritti fondamentali del minore d'età*, *Diritto penale contemporaneo – Rivista trimestrale* 1, 9 (2019)

¹¹⁴ Cass. Pen. Sez III, 10 maggio 2018 n 39039 in *Guida dir.* 2018, 41,50

di prevaricazione e di umiliazione della vittima, esponendo quest'ultima a un ulteriore pericolo: la probabilità che la foto potesse trapelare e finire nelle mani di pedofili.

Un seguente orientamento della Suprema Corte ha evidenziato come il requisito della diversità attribuito alle condotte del primo comma dell'art 600 ter c.p. si riferisca non tanto alla condotta delittuosa di cui al primo comma, quanto piuttosto al materiale pedopornografico prodotto.

Ne consegue che per le condotte illecite previste successivamente al primo comma, cioè alla divulgazione, commercio, pubblicizzazione, diffusione o distribuzione del materiale pornografico, non sia rilevante ai fini della configurabilità del reato il fatto che il materiale sia auto-prodotto dalla vittima.

Per queste ragioni sul tema appare necessario che avvenga un intervento del legislatore, anche a fronte della più recente introduzione della ulteriore possibilità di criminalizzazione delle condotte dell'art 612 ter, che analizzeremo nel dettaglio in seguito.

Altra fattispecie collegata è il "*sex-extorsion*" o "*sex-torsion*", pratica di ricatto molto diffusa, attraverso il *web*, per cui la vittima viene ricattata con il fine di ricevere denaro, da colui, di solito di genere maschile, che risulta in possesso del materiale pornografico. È dunque un reato che potrebbe realizzarsi sia in assenza di un legame sentimentale con la vittima, sia in presenza di una relazione con essa¹¹⁵.

Tuttavia, sebbene questa categoria abbia in comune con il *Revenge porn* i diritti che vengono potenzialmente lesi, come la reputazione, l'onore, la dignità e la libertà morale, la autodeterminazione dell'individuo, e anche la volontà di umiliare e degradare la vittima, la differenza tra questi appare sostanziale.

Infatti il *sex-extorsion* non prevede la finalità di vendetta, fondamentalmente costitutiva della disciplina in questione, ma la volontà di ricevere un vantaggio indebito a danno della persona interessata, che sia di denaro o di natura sessuale.

La definizione secondo l'Accademia della Crusca è «Estorsione di denaro, di favori sessuali o altro ai danni di una persona, dietro minaccia di rendere pubblici contenuti personali compromettenti di natura sessuale (messaggi di testo, foto o video)».

Questo fenomeno era già presente negli anni '50, in forma primordiale, tramite fotografie, come è accaduto a Marilyn Monroe che per questioni economiche decise di posare nuda per un servizio fotografico.

Dopo anni, durante l'avvio della sua carriera, queste foto iniziarono a circolare minacciandone la carriera, ma l'attrice decise di rivelare la verità e di non agire per vie legali¹¹⁶.

¹¹⁵ DE VITA R., M. DELLA BRUNA, *Non Consensual Pornography: dal revenge porn alla sexual extortion*, Osservatorio Cyber Security dell'Eurispes, 17.12.2019.

¹¹⁶ SCHELLER S.H., *A Picture Is Worth a Thousand Words: The Legal Implications of Revenge Porn*, in 93 NCL Rev. 551 (2015)

Il *sextorsion*, non essendo regolamentato da una specifica norma, viene molte volte punito proprio con il reato di estorsione all'articolo 629: il quale prevede una pena maggiore rispetto a quella prevista dall'art 612 ter.

Per questo motivo, la fattispecie, in caso di commissione di reato in concorso, verrebbe assorbita da quella più grave, cioè l'estorsione.

Famosissimo è il caso dell'*hacker* messicano, Luis Mijangos arrestato nel 2011 e condannato a sette anni per aver spiato più di duecentotrenta persone, tra cui alcuni minorenni, per esser entrato negli hard disk e aver rubato informazioni.

Per comprendere bene questa disciplina è logico fare una comparazione con quella prevista in merito al reato di estorsione, infatti l'articolo 629 c.p. prevede «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».

Un recente approdo della Cassazione¹¹⁷ ha precisato che questa figura di reato non può essere applicata nel caso in cui, come accade nel caso di specie, il danno non abbia natura patrimoniale.

Di recente, il decreto convertito in legge n. 153/2024 recante “disposizioni in materia di rafforzamento della *cybersicurezza* nazionale e di reati informatici” dispone un inasprimento delle sanzioni per alcuni reati, tra cui l'estorsione compiuta con mezzi informatici (tra questi reati figura anche l'accesso abusivo a sistemi informatici e la diffusione di malware).

La legge è stata approvata in senato il 20 giugno 2024, con 80 voti a favore, tre contrari e diciassette astenuti).

L'Europol con il report “*Online sexual coercion and extortion as a crime affecting children. Law enforcement perspective*”, pubblicato a maggio del 2017, ha voluto portare alla luce il fatto che le condotte di *Sexual-extorsion* sono perlopiù finalizzate all'ottenimento di ulteriori elementi di carattere sessuale, il 78% di casi analizzati riguardano ancora, minori.

Per quanto concerne, invece, le minacce che hanno come fine ultimo quello di ottenere dalla intimidazione un guadagno di tipo economico, si è rilevato che queste condotte di solito vengono realizzate da organizzazioni criminali, che hanno base al di fuori dei confini dell'Unione Europea¹¹⁸.

Da questa breve panoramica del contesto giuridico, si evince l'assenza di una regolamentazione unitaria idonea a delineare una piena tutela per queste nuove fattispecie di reato.

Altro fenomeno che ritengo necessario analizzare è il *doxxing*, o "*doxing*" il termine “dox” deriva dall'utilizzo in gergo di “doc” stante a indicare “documenti”.

¹¹⁷ Cass. Pen. Sez II, 12/10/2006 n. 34128 udienza n. 23/05/2006

¹¹⁸ consultabile sul sito ufficiale dell'Europol

A livello legislativo, il termine non ha una definizione, in quanto il legislatore europeo e italiano non si è occupato di legiferare in merito.

Storicamente i *doxer* cercavano nei *database online*, ma anche in posti fisici, come in registri anagrafici o nelle piattaforme *social*, più informazioni possibili sulle loro vittime, che potrebbero essere sia persone fisiche, ma anche giuridiche come aziende o addirittura Nazioni.

I *doxer* possono anche far leva su fonti esterne per la ricerca di ulteriori informazioni, come le persone vicine alla vittima.

Una volta raccolte le notizie necessarie, le pubblicano direttamente *online* o tramite un portale di condivisione di *link*.

Infatti, con questa fattispecie si vuole mettere in luce la possibile diffusione di documenti, informazioni personali e identificativi, dati sensibili (per esempio le cartelle cliniche) di una persona fisica vittima di *Revenge porn*.

Molto spesso i due fenomeni infatti avvengono congiuntamente.

In comune con il la fattispecie oggetto di analisi ha l'assenza del consenso da parte della persona interessata.

Riguardo allo scopo, alla base potrebbe altresì esserci la comune vendetta, come per la fattispecie oggetto d'esame, ma il *quid, sic et simpliciter*, si ritrova soprattutto nella volontà di rendere angosciante la minaccia, di generare paura, panico.

La sua funzione fondamentale è quindi quella di rendere riconoscibile la persona violando la sua privacy, condividendo informazioni come l'indirizzo di casa, il numero di telefono, l'indirizzo e-mail, nome e cognome, profili *social*, luogo di lavoro ma anche la fedina penale, foto di conversazioni private, dati del conto bancario o dettagli personali imbarazzanti.

Affinché ciò non accada molte organizzazioni utilizzano misure di *cybersicurezza* come *software* di crittografia o *firewall*, che aiutano nella lotta contro potenziali minacce.

In Europa, la normativa GDPR, Regolamento Generale per la Protezione dei Dati Personali, garantisce all'articolo 1, la protezione dei diritti sui propri dati personali¹¹⁹: ciò riguarda anche le aziende e le modalità in cui detengono e archiviano questi ultimi. In base a questa regolamentazione, ogni organizzazione ritenuta colpevole di aver violato queste norme può incorrere in multe fino a 20 milioni di euro o al 4% del fatturato annuo globale, a seconda di quale sia il valore più alto.

Tuttavia, per quanto concerne gli attacchi di carattere personale, le persone fisiche sono sempre più esposte ad “aggressioni” di questo genere, soprattutto in caso in cui detengano un profilo pubblico sui *social*, dove qualsiasi persona può accedere più facilmente alle informazioni.

¹¹⁹ Altri elementi di tutela forniti agli articoli 4 n. 2 Regolamento UE n. 679/2016; art. 2 *decies* d.lgs. n. 196/2003; STANZIONE M.G., *Il regolamento europeo sulla privacy, origini e ambito di applicazione*, 2016

Così facendo, sia familiari della vittima, che terzi estranei potrebbero riconoscerla, prenderla in giro, con il fine di renderla un vero e proprio bersaglio di *stalking* virtuale o reale, di crimini di odio o attacchi sessuali, come era successo a Tiziana Cantone.

Le ripercussioni, infatti, sono molto simili al *Revenge porn*: considerando anche i possibili danni alla reputazione e la probabilità che i datori di lavoro o colleghi possano venire a conoscenza dei dati sensibili diffusi senza consenso.

Secondo il *Washington Post*¹²⁰ anche *Anonymous*, gruppo attivista di *hacker* famosi per i loro attacchi nei confronti di società e istituzioni governative, nel 2015 ha utilizzato questo metodo di esposizione pubblica di dati, pubblicando su *X* una lista di profili individuali *Facebook* di persone che appartengono al Ku Klux Klan.

Inoltre, questi ultimi, di recente, hanno avviato una campagna contro i gruppi dedicati alla diffusione illecita di immagini o video sessualmente espliciti, che ci sono su Telegram, tramite l'hashtag #Revengegram: hanno identificato i soggetti colpevoli mediante gli indirizzi IP e hanno divulgato online le loro informazioni¹²¹.

Ci sono anche, quindi, casi in cui il *doxing* potrebbe essere utilizzato in buona fede, come per l'attacco alla maratona di *Boston* nel 2013 dopo il quale sono state diffuse delle immagini e informazioni di un giovane universitario, che si riteneva fosse presente al momento dell'attacco e che sarebbe stato ritenuto responsabile, ma in verità il ragazzo era morto prima del verificarsi di questi eventi¹²².

Rilevante per l'analisi fin qui condotta è il *cyber stalking*, articolo 612 bis cp, introdotto dal decreto-legge n. 11/2009, per cui è punito «chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita».

Il comma secondo di questo articolo, introdotto solo in seguito, con la legge n. 119 prevede la possibilità che questo tipo di reato avvenga attraverso l'uso di strumenti "informatici o telematici".

Si tratta quindi di comportamenti insistenti, di messaggi minatori, ma può consistere, nei casi più gravi anche nell'installazione sui dispositivi della vittima di *spyware* o sistemi GPS.

Un caso che costituisce la perfetta commistione tra *cyberstalking* e *Revenge porn* è quello di Tiziana Cantone.

Nel 2021 uno studio ha rivelato che l'Italia si trova al secondo posto tra gli Stati Europei, con 611 persone che hanno subito *cyber-stalking*, dopo la Germania con 1012 persone.¹²³

¹²⁰ Articolo del *Washington post*, 11/05/2015 “*Anonymous’s KKK ‘leak’ targets the elusive online world of white nationalism*”

¹²¹ Articolo su “*La Repubblica*” di Arturo di Corinto, 10 aprile 2020

¹²² Articolo della BBC News, 2013 “*Boston Bombing, how internet detectives got very wrong*”

¹²³ KASPERSKY, Studio “*Lo stato dello stalkerare*”, 2021

I soggetti attivi che mettono in atto questa condotta di solito sono persone molto vicine alla vittima o *ex partner*.

Fondamentale per potersi difendere da questo fenomeno e ridurre al minimo gli attacchi è mantenere una protezione elevata dei propri dati utilizzando programmi di crittografia, l'autenticazione a due fattori per i profili *social*, utilizzare *password* lunghe con più tipologie di caratteri e limitare le informazioni che si condividono online.

Il reato di diffusione illecita di immagini a carattere sessuale può anche essere messo in atto quindi, mediante nuovi strumenti che risultano insidiosi per il legislatore.

Un esempio è lo “*wireless spy camera*”, che nascosto in luoghi pubblici o privati, permette di effettuare filmati o video a distanza dal sistema che li avvia.

In questo caso, prima dell'entrata in vigore dell'art 612ter, si applicava, a seconda del caso di specie, l'articolo 615 bis, reato di interferenze illecite nella vita privata (fattispecie introdotta nel 1974 nella sezione dei delitti contro l'inviolabilità del domicilio).

L'articolo prevede che «chiunque, mediante l'uso di strumenti di ripresa, visiva o sonora si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.

Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo».

Tuttavia, oggi, con l'introduzione del nuovo reato grazie alla Riforma del Codice Rosso, si segue la clausola di salvaguardia, indi per cui, essendovi un rapporto di specialità reciproca tra i due articoli, si applicherà quello con la pena più grave.

Altro strumento che si potrebbe utilizzare, per commettere questo reato è il c.d. “*trojan*” ad accesso remoto, strumento che serve per entrare nelle telecamere dei computer portatili¹²⁴.

La modalità che desta preoccupazione, al pari delle precedenti, è l'utilizzo del “*phishing*”, un tipo di truffa attuata su *Internet* che ha come finalità quello di ingannare la persona che la subisce, ottenendo informazioni sensibili, o più in generale l'utilizzo di sistemi di *hackeraggio* con la volontà di trarre informazioni dai dispositivi della vittima.

Una delle vittime di questa modalità è stata Guendalina Tavassi, che ha subito *Revenge porn*, tramite la divulgazione su *Telegram* e su *PornHub* di un video intimo girato con il marito, destinato a rimanere privato, che aveva caricato *sull'iCloud* del proprio telefono.

La donna ha immediatamente fatto denuncia alla polizia postale, o anche come è successo a Diletta Leotta, vittima della “*sextorsion*” per il quale si chiedeva una somma di denaro per non diffondere i suoi contenuti intimi.

¹²⁴ si tratta del cosiddetto *Voyeurismo digitale*: è un disturbo della sfera sessuale, che spinge l'individuo a spiare l'intimità degli altri, in tutte le sue forme.

Altra fattispecie che si “incastra” perfettamente nella disciplina del *Revenge porn* è il “*fake porn*” o anche “*porno deep fake*” di cui parleremo in maniera più approfondita in seguito (*infra*, § cap. 3 paragr. 3).

Si è sviluppato nel 2017 nell'ambito del fenomeno del *deepfake*, e consiste nel combinare, sovrapporre immagini o video che già si trovano su *Internet* o che già esistono, per mezzo di appositi *software* di Intelligenza Artificiale, con l'obiettivo finale di modificare o ricreare, in modo estremamente realistico, i movimenti di un volto o di un corpo e imitarne la voce¹²⁵.

Specificatamente, con questa fattispecie denominata “*porno deep fake*”, o *deepnude*, si vuole applicare foto o video contenenti volti di persone vere, note o meno, a video pornografici preesistenti.

Tramite questo tipo di diffusione di immagini o video non consensuali, è aumentato progressivamente il ricorso alla pornografia non consensuale.

Il fine è quello di modificare e manipolare contenuti multimediali altrui per creare materiale pornografico falso ma realistico, all’insaputa della vittima, per poi poterlo diffondere in siti pornografici e *social network*.

Una società di *cyber* sicurezza con base nei Paesi Bassi, “*Deeptrace*” monitora la diffusione, direi a macchia d'olio, del fenomeno del *deep fake* per il quale l'Italia si trova in cima alla vetta dopo gli Stati Uniti, la Russia e l'Argentina.

Da una approfondita analisi condotta, pubblicata nel 2019¹²⁶, è risultato che i video *deepfake online* erano più o meno 15.000, il 96% erano video porno.

L'anno successivo i numeri sono aumentati: nel solo mese di luglio, nelle *chat* private dell’app di *Telegram*, le immagini di 104.852 donne sono state virtualmente “spogliate” con l'utilizzo della AI, e successivamente sono state rese pubbliche¹²⁷ (*infra*, § cap. 3 Parag. 3).

Il *Revenge porn* ha anche molte caratteristiche in comune con una forma di violenza detta “*cum tribute*”, pratica famosa soprattutto in Inghilterra e negli Stati Uniti, tramite cui uomini postano su social appositi, come *Twitch* o *Telegram* o anche su siti pornografici, foto di donne, di ogni genere, anche semplici *selfie* con gli amici o in spiaggia, perciò non per forza immagini pornografiche, per poi culminare l'atto di autoerotismo e postare il risultato online.

Il fenomeno ha colpito non solo persone non conosciute, ma anche attori famosi come Emma Watson.

Per questo tipo di contenuti il “*cum tributer*” riceve anche dei soldi da altri uomini che visualizzano il contenuto e commentano, incitando la persona interessata a postare ulteriori contenuti.

¹²⁵ Garante della protezione dei dati personali, *informativa sui rischi dell’uso malevolo di questa tecnologia*, 2020

¹²⁶ *The State of Deepfakes: Landscape, Threats, and Impact*, HENRY AJDER, GIORGIO PATRINI, FRANCESCO CAVALLI, AND LAURENCE CULLEN, September 2019.

¹²⁷ report PATRINI G. “*Automating Image Abuse, Deepfakes Bots on Telegram*”, 2022

Infatti, alla base di ciò è presente la volontà di ottenere apprezzamenti da altri uomini sul loro "operato" e quindi di far riferimento a una sorta di "solidarietà" tra uomini, ma soprattutto quello di umiliare la vittima, degradarla a mero oggetto sessuale con il solo fine di essere ridicolizzata pubblicamente e mercificare il suo corpo, per potersi sentire superiore.

Secondo *Similar web*¹²⁸, una società informatica che fornisce servizi di *web analytics* con sede nel Regno Unito, *Reddit* sarebbe la piattaforma più usata per questo tipo di pratica, infatti riceverebbe quasi 4,8 milioni di visite al mese.

Sergio Messina nel lontano 2006 parlava già di questo fenomeno parlando della "gloria" che secondo lui ne deriva ¹²⁹.

Dal punto di vista normativo questa pratica potrebbe essere sanzionata tramite l'uso di due articoli: il 612 ter, secondo quanto previsto per la condivisione illecita di immagini o video sessualmente espliciti, nel caso in cui accanto la foto rappresentante il risultato dell'atto, verrebbe anche ripresa una parte di organi genitali o foto di ragazze nude o in atteggiamenti intimi.

Alternativamente, potrebbe essere utilizzato l'articolo 167 del codice della *privacy* (d.lgs. 196/2003) sul trattamento illecito di dati personali, che analizzeremo nel seguente paragrafo.

4.0 (segue): Le figure di reato che venivano applicate prima della Riforma del Codice Rosso

Tornando alla disciplina oggetto d'esame, antecedentemente alla riforma del 2019 che introduce l'articolo 612 ter, il reato di diffusione illecita di immagini o video sessualmente espliciti non era criminalizzato con una fattispecie *ad hoc*, ma era riconducibile ad altre discipline previste dal nostro ordinamento, e con queste veniva criminalizzata tale condotta.

Per ovviare il vuoto normativo¹³⁰ la Giurisprudenza e la Dottrina facevano riferimento a varie discipline.

Innanzitutto, la fattispecie di diffamazione prevista dall'art 595¹³¹, specificatamente il comma terzo, che recitava «Se l'offesa è recata con il mezzo della stampa, o con qualsiasi altro mezzo di pubblicità, ovvero con atto pubblico, la pena è della reclusione da sei mesi a tre anni, o della multa non inferiore a cinquecento sedici euro».

¹²⁸ questo sito può analizzare i competitor come *Google*, *Facebook*, e altri, fornendo dati sul traffico digitale e sugli insight.

¹²⁹ intervista dal sito *vice.com*

¹³⁰ Parlava di "vuoto normativo" A. VERZA, *Aggredire attraverso l'immagine. Cristallizzazioni tecnologiche, genere e diniego di tutela nella logica disciplinante neoliberale*, in *Ragion pratica*, 2017, n. 2, 467 ss.; cfr. G.M CALETTI, "Revenge porn" e tutela penale, cit., 82 ss.

¹³¹ CALETTI, *Revenge porn e tutela penale*, in *DPC.it* 3/2018

Altrimenti, si utilizzava anche la normativa prevista dal d.lgs. 196/2003 per illecito trattamento di dati personali, articolo 167, oppure la disciplina di atti persecutori prevista dall'articolo 612 bis c.p., articolo 617 septies c.p. in riferimento a diffusione di riprese e registrazioni fraudolente, articolo 615 bis c.p. interferenze illecite nella vita privata e infine l'estorsione all'articolo 629 c.p., in riferimento a quelle condotte che hanno ad oggetto l'utilizzo di materiale a contenuto sessualmente esplicito per ottenere un ingiusto profitto.

Queste normative però non hanno garantito, col tempo, una adeguata repressione alla condotta di diffusione di immagini o video diffuse senza il consenso della vittima, perciò, a seguito degli episodi di Tiziana Cantone e Giulia Sarti, si è deciso di introdurre una disciplina *ad hoc* che potesse criminalizzarne la condotta.

4.1 (Segue): Il reato di Diffamazione

Partiamo analizzando l'art 595 del c.p., che recita «Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a mille e trentadue 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 duemila sessantacinque 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 cinque centosedici 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». Questa disciplina è contenuta nel titolo del Codice dedicata ai delitti contro l'onore ed è perseguibile mediante querela da parte dell'interessato.

L'oggetto di tutela è la dignità del soggetto passivo, sia dal punto di vista, secondo la dottrina maggioritaria, dell'onore inteso come la reputazione che la persona gode agli occhi della società, sia nella accezione relativa alla propria immagine di sé.

Pertanto, prima dell'introduzione dell'articolo 612 ter ci sono state numerose massime della Corte di Cassazione che hanno aderito a questa visione¹³².

L'oggetto tutelato è distinto però dalla diffusione illecita di immagini a sfondo sessuale; poiché vedremo in seguito, l'art 612ter ha come principale obiettivo quello di tutelare non solo l'onore, ma anche la riservatezza, l'ambito di auto determinazione della propria libertà sessuale e l'integrità fisica della vittima stessa, che potrebbe essere compromessa in caso di ripercussioni di carattere psicologico e sullo stato di salute.

¹³² Cass. Pen n. 19659/2019; Cass. Pen., sez. 05, del 19/06/2008, n. 30664; Cass. pen. sez. V, 14/11/2016, n.4873

Inoltre, opinione comune rilevasi in Dottrina e in Giurisprudenza, prevede che l'inadeguatezza dell'articolo 595 c.p. può essere rilevata nella considerazione per il quale il contenuto di quest'ultima è indirizzato "a più persone" (la Suprema corte definisce il *web* come "un ambiente comunicativo per sua natura destinato ad essere normalmente visionato da più persone"¹³³) facendo sì che venga ad esistenza un vuoto di tutela per tutti quei casi in cui la prima condotta posta in essere, non è la diffusione verso più persone, ma la fruibilità del contenuto esclusivamente fra due individui, materiale che poi in un secondo momento, verrà divulgato nei confronti di terzi, estranei al rapporto fra la vittima e il destinatario del contenuto.¹³⁴

Altra considerazione va effettuata in riferimento *al locus commissi delicti*, problema che caratterizza la maggior parte dei reati informatici.

Secondo un orientamento prevalente, bisogna considerare integrato il requisito del comma terzo dell'articolo oggetto di analisi, che considera come "mezzi di pubblicità" anche i *social network*.

Questi vengono definiti dalle Sezioni Unite¹³⁵ come "luoghi virtuali" su cui possono essere inseriti contenuti sessualmente espliciti.

Per entrambe le discipline oggetto d'esame sorgono molti dubbi in relazione alla commissione *online* dell'illecito, data l'impossibilità di esatta decifrazione del luogo da cui una informazione viene immessa nella rete.

Secondo la Giurisprudenza¹³⁶ «La diffamazione, che è reato di evento, si consuma nel momento e nel luogo in cui i terzi percepiscono l'espressione ingiuriosa» perciò fondamentale ai fini della configurabilità del reato e della sua perfezione, è la possibilità del terzo di percepire la lesione.

Anche considerando l'ipotesi aggravata della diffusione mediante mezzo informatico, previsto al comma terzo «col mezzo della stampa o qualsiasi altro mezzo di pubblicità», la Cassazione con alcune successive sentenze¹³⁷, mette in luce la necessità di tenere presente, anche in virtù della natura di reato istantaneo di evento, il fatto che quest'ultimo si consuma nel momento in cui l'immagine o i video diffamatori vengono immessi nella rete: quindi contestualmente o dopo poco tempo, considerando l'immediata fruibilità da parte di terzi del contenuto illecito.

Tuttavia, in relazione a quanto concerne la disciplina prevista all'articolo 6 comma 2 del cod. pen., riguardante la determinazione della competenza per la commissione del reato sul territorio nazionale, occorre effettuare una verifica in concreto sul luogo effettivo da cui la persona offesa ha avuto accesso al contenuto lesivo.

¹³³ Cass. Pen. Sez. V, n. 3963 del 06/07/2015, Rv. 265815

¹³⁴ ANDREUCCIOLI, "misure per il contrasto della diffusione non autorizzata di materiale sessualmente esplicito" in A.S. 2016, servizio studi del senato n 57 marzo 2019.

¹³⁵ Cass. Pen. sez. unica 21 gennaio 2015 n 31022 in giur. cost. 2015,3,1055 con nota di Diotallevi

¹³⁶ Cass. Pen. Sez. V sent. n. 25875 del 25 luglio 2006

¹³⁷ Cass. Pen. Sez. 5, n. 22787 del 30/04/2021, Rv. 281261 ; Cass. Pen. Sez. 5, n. 38099 del 29/05/2015, Rv. 264999

Se non è possibile, allora si fa riferimento ai criteri suppletivi stabiliti all'art 9 comma 1 e 2 del cod. di proc. pen., per il quale, se non è possibile determinare il luogo di consumazione del reato, ovvero nel luogo di domicilio dell'imputato, la competenza va radicata nel luogo in cui è stata messa in atto parte dell'azione¹³⁸.

Per quanto riguarda la nuova disciplina della pornografia non consensuale, come per l'altra fattispecie oggetto di analisi, vale lo stesso principio della difficoltà di stabilire precisamente il *locus commissi delicti*.

Si tratta infatti di una condotta che si verifica sul *web*, e quindi svincolata dalla territorialità della commissione del reato, in quanto il soggetto attivo ha la possibilità di "essere" allo stesso tempo in luoghi diversi.

Il professor Bellacosa¹³⁹, sottolinea infatti come «le categorie spazio-fisico-temporali entrano in crisi, in quanto vengono in considerazione la "smaterializzazione" di dati e informazioni, raccolti e scambiati in un contesto virtuale, senza contatto diretto o intervento fisico su di essi e la "delocalizzazione" di risorse e contenuti, collocabili in una sorta di "meta territorio" (..); "la detemporalizzazione" delle attività che possono essere svolte attraverso operazioni automatizzate programmate dall'utente, in modo da non aver poi bisogno di un collegamento o contatto fisico tra persona e sistema informatico; la possibilità per l'utente di avvalersi delle caratteristiche di "ubiquità", velocità e anonimato offerte dalla rete globale a chi vi opera».

Perciò, mentre per il reato di diffamazione si intende congruente l'ipotesi in cui la competenza va ricercata nel luogo in cui i terzi percepiscono il danno arrecato alla persona offesa¹⁴⁰, per il delitto di diffusione illecita di contenuti a sfondo sessuale, si ritiene integrata l'ipotesi per cui la consumazione avviene nel momento di realizzazione delle condotte che vengono elencate nei commi 1 e 2, per esempio il reato si riterrà integrato se la condotta di sottrazione del materiale dal contesto privato viene messa in atto, senza la conoscenza e l'approvazione della persona offesa.

A conferma di questo principio, il Tribunale di Milano¹⁴¹ ha stabilito che il Giudice competente sarà tale in relazione al domicilio dell'imputato, il quale tramite un *hardware* in grado di connettersi alla rete, è entrato nel *web* predisponendo il caricamento dei dati e la conseguente violazione degli articoli oggetto d'esame.

¹³⁸ Cass. Pen., Sez.V, sent n. 854.2021

¹³⁹ BELLACOSA M., in *Diritto Penale Contemporaneo*, "il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite", 2015,7.

¹⁴⁰ GULLO, "delitti contro l'onore", in Viganò, Piergiallini (a cura di), "reati contro la persona e contro il patrimonio", Torino, 2015,157; TABARELLI DE FATIS, "prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione online", in Picotti (a cura di) "tutela penale della persona e nuove tecnologie", Padova, 2013, 220; PANATTONI, "I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace" in *Sistema Penale*, 2020, 5, 310 ss.; Cass. Pen. sez. I n 2739/2010

¹⁴¹ Trib. di Milano, sez IV penale, giudice monocratico, 3 ottobre 2017 n 9393

Anche la Corte di Cassazione si è espressa, per la diffusione *online* di materiale pedopornografico articolo 600 ter comma terzo c.p., individuando il momento consumativo nell'inserimento in rete¹⁴².

I giudici precisano che il *locus commissi delicti* si identifica nel luogo di immissione nella rete delle immagini, in quel momento si ritiene perfezionata la fattispecie¹⁴³.

Per il reato di diffusione illecita di immagini o video sessualmente espliciti, come l'articolo 600 ter comma terzo, non è necessaria, ai fini dell'integrazione della fattispecie, la percezione della lesione da parte della persona offesa, per questo, anche la successiva cancellazione del contenuto dal *web* risulta irrilevante¹⁴⁴.

Altra considerazione da tenere a mente sulla differenza tra i due articoli riguarda la pena stabilita: infatti mentre l'art 595 c.p. prevede la reclusione fino ad un anno e una multa da circa mille euro, l'art 612 ter, dispone la reclusione da uno a sei anni e una multa da 5 mila fino a 15 mila euro.

Pertanto, si può dedurre *ictu oculi* che la disciplina riguardante la diffamazione può essere prevista in concorso con l'articolo 612 ter.

Nel caso in cui però chi commette l'atto illecito viene indagato esclusivamente in relazione al comma primo dell'articolo 612ter, comma che non prevede che la persona offesa lamenti un danno alla reputazione, allora la condotta di lesione all'onore potrebbe essere integrata in concorso, ogniquale volta in cui sussista una lesione dell'identità personale intesa come distorsione, alterazione, travisamento e offuscamento del patrimonio intellettuale, politico, sociale, ideologico dell'individuo, quando viene realizzata mediante l'offesa alla reputazione dei soggetti medesimi¹⁴⁵.

A sostegno di questa previsione, una recente sentenza della Cassazione¹⁴⁶ ha affermato l'uso del concorso formale fra questi reati stabilendo che il caso in esame poteva ricondursi a diverse ipotesi criminose.

Infatti la Corte fa riferimento, oltre alla diffusione via *web* di immagini intime ritraenti la persona offesa, anche alla diffamazione art 595 comma terzo, la diffusione illecita di dati personali art 167 del codice della privacy, e l'articolo 612 bis "atti persecutori".

Altro esempio di concorso è fornito da una sentenza della Suprema Corte¹⁴⁷ nel 2017, per il quale un uomo era imputato sia per reato di diffamazione, specificatamente per il comma terzo, per aver condotto persone sconosciute presso il domicilio della persona offesa promettendo appuntamenti di natura sessuale e quindi ingiuriando e molestando la persona offesa, sia per aver diffuso su *Facebook* foto di carattere sessuale e dati personali con gli amici della persona offesa.

¹⁴² Cass. Pen. Sez. III, n. 28524/57 del 9/06/2009; Cass. Pen. Sez. III, n. 25232 del 21/06/2005, P.M. in proc. Brancato, Rv. 231814

¹⁴³ Cass. Pen. Sez. I, n. 47086/2018; Cass. Pen. Sez. III, n. 8296 del 2/12/2004

¹⁴⁴ Cass. Pen. Sez. III, n. 41231 del 17/01/2018

¹⁴⁵ Cass. pen. Sez. V sentenza n. 37383 del 17 ottobre 2011

¹⁴⁶ Cass. Pen., sez. V, n. 30455/2019

¹⁴⁷ Trib. di Milano, V sez. pen, giudice monocratico 8 novembre 2017 n 10945

Nel 2013 invece un soggetto di sesso maschile denunciava¹⁴⁸ una conoscente per aver creato un profilo *Facebook* a suo nome, senza autorizzazione, allegandovi delle sue fotografie di nudo (nella motivazione di questa si fa riferimento alla disciplina di sostituzione di persona).

Il Tribunale descrive la condotta come capace di produrre nocumento all'ambito social lavorativo della vittima, libero professionista, e perciò si intende integrato il reato di diffamazione.

Tuttavia, oggi, grazie all'introduzione del Codice Rosso, in questi casi si ritiene possa essere applicata anche la disciplina di *Revenge porn*, avendo pubblicato foto sessualmente esplicite senza l'accettazione del soggetto interessato.

Contrariamente, ci sono anche previsioni speciali da parte del Giudice di Legittimità, secondo cui non risulterebbe integrato il reato di diffamazione *online*, se venissero pubblicate delle foto di una donna nuda, nel caso in cui avvenga in un contesto non osceno e non abbia una concezione negativa¹⁴⁹.

Altra casistica prevederebbe che il consenso prestato alla pubblicazione di una immagine, se questa venga riprodotta in un contesto alternativo rispetto a quello per cui l'assenso è prestato, non possa essere una scriminante del delitto di diffamazione¹⁵⁰. Alternativamente, grazie anche al carattere sussidiario della norma, la fattispecie prevista all'articolo 595 cp potrebbe anche subire il fenomeno di assorbimento nella più grave fattispecie della diffusione illecita di immagini all'articolo 612 ter, tenendo a mente anche la presenza della clausola di salvaguardia - salvo che il fatto costituisca più grave reato - presente all'inizio di quest'ultimo articolo¹⁵¹.

4.2 (Segue): art 167 d.lgs. 196/2003

Altra disciplina alla quale veniva assimilato il reato di diffusione illecita di immagini a sfondo sessuale senza il consenso della persona offesa, prima della venuta ad esistenza della Riforma n. 69 del 2019 che ha introdotto il reato all'art 612 te, è l'art 167 del codice della privacy (d.lgs. 196/2003) riguardante il trattamento illecito di dati personali, modificato dal GDPR.¹⁵²

¹⁴⁸ Trib. di Bari, sez. I, 5 marzo 2013 n 584 in “*de iure*”

¹⁴⁹ Cass. Pen. sez. III n 19659 in *CED* 2019; Cass. Pen sez V n 42130/2011

¹⁵⁰ Cass. Pen Sez. VI n 38571/2008 in *CED* Cass. Pen. rivista 241509-01

¹⁵¹ Rinvio a BAFFA G., *Gli atti persecutori. Gli elementi costitutivi della fattispecie e la definizione dei rapporti specifici con altre norme incriminatrici*, in *Temi penali*, Vol. II, *Delitti contro la persona. Delitti contro il patrimonio*, a cura di M. Trapani, A. Massaro, Giappichelli, 2019, 229 ss.

¹⁵² il codice della *privacy* è stato ampiamente rivisitato proprio dal D.lgs. n. 101/2018, e di nuovo modificato con legge n. 205/2021 per assicurare continuità e semplificazione nell'applicazione del nuovo Regolamento GDPR. In tale prospettiva, nel riformulato art 167 è stata introdotta la previsione

Per dati personali, il GDPR indica qualsiasi informazione riguardante una persona fisica già identificata o che potrebbe essere tale. Pertanto, anche le immagini, le foto e i video, quando ci consentono l'identificazione dei soggetti rappresentati, sono considerati dati personali; perciò, in quanto tali, meritano la tutela che il GDPR impone¹⁵³.

La fattispecie in questione prevede «Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli due *sexies* e due *octies*, o delle misure di garanzia di cui all'articolo 2 *septies* arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.

Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

Il Garante trasmette al Pubblico Ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato.

La trasmissione degli atti al Pubblico Ministero avviene al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.

Quando per lo stesso fatto è stata applicata a norma del presente Codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita».

Il concetto di "nocumento", non è definito da alcuna norma legislativa, tuttavia in questo caso è elemento costitutivo del reato.

del "danno" come elemento caratterizzante in alternativa allo scopo di profitto. Perciò non si terrà conto unicamente del profitto economico dell'autore dell'illecito, ma anche del danno arrecato agli interessati, comprendendo in questo modo il danno d'immagine e alla reputazione della vittima, ricomprendendo quindi anche la fattispecie di *Revenge Porn*. La riforma ha anche introdotto due nuovi articoli, il 167 bis che prevede la comunicazione e la diffusione illecita di dati personali oggetto di trattamento su larga scala, e il 167 ter che riguarda l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala; BELISARIO E., RICCIO G.M., SCORZA G., (a cura di) GDPR e normativa privacy commentario, II ed., 2022

¹⁵³ Regolamento UE 679/2016; FIRMIANI MOIRA, *Compendio di normativa sulla privacy per il trattamento dei dati personali, guida alla lettura del codice della privacy e GDPR*, I ed., 2022

Questo, potrebbe essere definito, secondo una pronuncia del 2016, come "un pregiudizio giuridicamente rilevante di qualsiasi natura, patrimoniale e non, cagionato sia alla persona alla quale i dati illecitamente trattati si riferiscono sia a terzi come conseguenza della condotta illecita"¹⁵⁴.

Secondo la Suprema Corte il nocumento si identifica come la non consentita divulgazione di dati relativi alla vita sessuale della persona offesa da parte dell'indagato¹⁵⁵, questo fenomeno quindi, viene definito letteralmente come «la propalazione da parte dell'indagato di informazioni relative alla vita sessuale della persona offesa» (*Infra*, § cap. 2 parag. 2.1).

Questa concezione viene a configurarsi come più ampia rispetto al mero danno, ricomprendendo nella fattispecie non solo una problematica di carattere patrimoniale ma anche di sofferenza psicologica, «volendo esso abbracciare qualsiasi effetto pregiudizievole che possa conseguire alla arbitraria condotta invasiva degli altri»¹⁵⁶. Tuttavia, questa disciplina viene considerata eccessivamente ampia poiché non dà adeguata copertura a livello sanzionatorio.

Ciò avviene sia per il caso di divulgazione del contenuto (previsto invece nella condotta tipica del *Revenge porn*) da parte di soggetti che non hanno intenzione di arrecare "nocumento" in quanto non conoscono direttamente la vittima, ma sono mossi da altri motivi (si tratta dei cosiddetti "secondi distributori"¹⁵⁷) (*Infra*, § cap. 2 parag. 2.1), sia per l'ipotesi in cui il soggetto attivo sia legato da una relazione affettiva o sentimentale alla vittima, caso per il quale verso la persona interessata si avrebbe una portata maggiormente lesiva.

Il dolo specifico, in via generale, ha un elemento in più rispetto al dolo generico: Il primo, viene a configurarsi nella previsione in cui l'autore, abbia l'intenzione di compiere un'azione mirata al raggiungimento di uno scopo specifico oppure al fine di arrecare danno, in maniera volontaria, all'interessato¹⁵⁸.

In questo caso, è stato inserito il concetto di nocumento nella normativa (e il conseguente dolo specifico), al fine di dare una maggior tutela a tutti quei casi di *Revenge porn* che non rientravano in una disciplina apposita.

Pertanto, questo articolo è quello che meglio si accosta alla fattispecie oggetto d'esame. In relazione al danno si può far riferimento ad un altro articolo del Codice della Privacy, l'art 13, il quale statuisce che chiunque arreca un danno ad altri, per effetto del

¹⁵⁴ Cass.Pen. sez III, n. 15221/2016 in conformità con sent della stessa sezione n. 40356 del 2015.

¹⁵⁵ Cass. Pen. Sez. III, 7 febbraio 2017, in CED rivista n. 270458

¹⁵⁶ Cass. Pen. III, sent. 8.10.2015, n. 40356. Nel caso di specie la Corte ha ritenuto verificatosi l'illecito previsto dall'art. 167 d.lgs. 196/2003 nel comportamento del soggetto, il quale pubblicava su YouTube un video sessualmente esplicito ritraente una donna, la quale non aveva prestato il suo consenso alla diffusione.

¹⁵⁷ Sull'elemento soggettivo del dolo specifico, cfr. S. CANESTRARI *et al.*, *Manuale di diritto penale. Parte generale*, Bologna, 2017, p. 540 e L. PICCOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, pp. 547 ss., secondo i quali una delle funzioni del dolo specifico è quella di restringere l'ambito della punibilità.

¹⁵⁸ MOSCO E., FIANDACA G., *Diritto penale, parte generale*, Nona ed., 3 aprile 2024

trattamento dei dati personali, risponde con risarcimento del danno ai sensi dell'art 2050 cc, articolo che riguarda la responsabilità per l'esercizio di attività pericolose per sua natura o per i mezzi adoperati.

Ciò sta a sottolineare, come viene considerato dal legislatore, che il trattamento di dati è una attività potenzialmente pericolosa proprio per la sua importanza e per i danni che potrebbe provocare all'individuo.

Tuttavia, il titolo contenente questa norma è stato abrogato dalla successiva riforma del d.lgs. 10 agosto 2018, n 101.

Con il trattamento illecito di dati personali, il bene giuridico si identifica nella riservatezza: questo coincide con il diritto dell'individuo a «preservare la propria sfera personale dalle attenzioni di quanti non abbiano titolo per ingerirsi in essa ed attiene, quindi, all'aspetto interiore dell'individuo, che ha diritto a proteggersi dalle indiscrezioni altrui»¹⁵⁹ : ciò è quanto affermato dalla Corte di Cassazione, che in molte pronunce accosta il trattamento dei dati personali alla disciplina della diffamazione, applicandole in concorso.

La tutela penale della riservatezza viene anche definita come «interesse della persona a mantenere nell'ambito della propria sfera privata quegli atti o quelle vicende che la persona stessa desidera restino tali, impedendo l'attività dei terzi che vogliono divulgarle rendendole di pubblico dominio»¹⁶⁰.

Tuttavia, *de facto* la Corte di Cassazione, mette in luce l'effettiva distinzione delle due normative: in questa pronuncia sottolinea la differenza con l'art 595 c.p. dove l'oggetto, e quindi il bene giuridico leso dalla condotta illecita, è la reputazione.

Non mancano le circostanze per cui, però, questa disciplina venga assorbita, come precedentemente visto per il reato di diffamazione.

Infatti da segnalare sul tema è la pronuncia del Tribunale di Milano¹⁶¹ ove l'imputato risponde per violazione degli articoli 595 c.p. e 167 del d.lgs. 196/2003, il giudice prevede che quest'ultimo articolo venga assorbito nel reato all'articolo 595 considerandolo come condotta più grave e quindi dando attuazione alla clausola di salvaguarda che fa capo all'illecito trattamento di dati personali.

Per questo motivo, viene considerato in Giurisprudenza che la tutela prevista dalla norma che regola il reato più grave, il quale è posto a salvaguardia del medesimo interesse, venga applicato a discapito di quello che prevede una sanzione meno grave.

¹⁵⁹ Cass. pen., Sez. V, 10 luglio 2019, n. 30455

¹⁶⁰ BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, 1970, cit. pag.1069 ss.

¹⁶¹ Trib. di Milano sez. pen. V, giudice monocratico, 25 settembre 2017 n 8940

4.3 (Segue): Atti persecutori

L'articolo 612 bis disciplina la materia degli atti persecutori, comunemente definiti con la locuzione anglosassone di "*stalking*"¹⁶².

Esso recita «Salvo che il fatto costituisca più grave reato, è punito con la reclusione da un anno a sei anni e sei mesi 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, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se il fatto è commesso attraverso strumenti informatici o telematici.

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. La remissione della querela può essere soltanto processuale.

La querela è comunque irrevocabile se il fatto è stato commesso mediante minacce reiterate nei modi di cui all'articolo 612, secondo comma.

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»¹⁶³.

Secondo il Rapporto Italia 2021 dell'Eurispes¹⁶⁴, quasi un italiano su dieci è stato vittima di *stalking*.

Le donne sono oggetto di atti persecutori tre volte in più rispetto agli uomini, le donne straniere sono particolarmente vulnerabili, con un tasso di vittimizzazione del 15,8%, solo il 13,7% delle vittime denuncia le proprie esperienze alle autorità.

La condotta di *Revenge porn* può essere messa in relazione con questo articolo al fine di evidenziare un unico disegno criminoso da parte del perpetratore.

Da questa ipotesi si giustifica la scelta del legislatore di collocazione del reato di diffusione illecita di immagini a sfondo sessuale, immediatamente dopo lo *stalking*, nello stesso Titolo di delitti contro la libertà morale¹⁶⁵.

¹⁶² MUSCATIELLO V.B., *Il cosiddetto stalking*, in Scritti in memoria di Giuliano Marini, cit., p. 563 ss.; DE SIMONE G., *Il delitto di atti persecutori*, Roma 2013, passim; A. Valsecchi, *Il delitto di "atti persecutori" (il cd. stalking)*, in Riv. it. dir. proc. pen., 2009, p. 1377 ss.; MACRI' F., *Atti persecutori (Art. 612 bis)*, in I delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti, in Trattato di diritto penale. Parte speciale, Vol. IX, diretto da Cadoppi, S. Canestrari, Manna, Papa, Torino, 2011, p. 351 ss.

¹⁶³ introdotto con il d.l. n. 11/2009 convertito in legge n. 38/2009

¹⁶⁴ trentatreesimo Rapporto Italia 2021, Eurispes

¹⁶⁵ MANTOVANI F., *Diritto penale. Parte speciale, I, Delitti contro la persona*, Padova 2019

Infatti in questo caso, la tutela della libertà morale va intesa nella sua concezione più ampia, in relazione a condotte che offendono la libera autodeterminazione dell'individuo, la vita affettiva, l'integrità psico-fisica¹⁶⁶.

La fattispecie di Atti Persecutori, al momento della sua entrata in vigore, ha destato non poche perplessità, come anche per l'articolo 612ter, a causa dell'indeterminatezza di alcuni termini utilizzati dal legislatore, che rende molto ostica sia la prova degli elementi costitutivi in fase di giudizio, sia alcuni elementi aggravanti¹⁶⁷.

Si tratta di due normative che in molti definiscono “sorelle”, in quanto accomunate dalla stessa necessità di urgenza quando sono entrate in vigore, tramite il cosiddetto “pacchetto sicurezza”¹⁶⁸.

In comune, le due discipline hanno innanzitutto lo scopo della loro introduzione, infatti, la disciplina degli Atti Persecutori è stata inserita all'interno di una più grande “ristrutturazione” del Codice penale a protezione della donna, mediante varie riforme: quella degli atti persecutori (d.l. n. 38/2009), le modifiche apportate per il reato di violenza sessuale nel '96 legge n.66, e la normativa n. 119/2013 riguardante i femminicidi, infine, la riforma del Codice Rosso n. 69/2019.

Infatti, quest'ultima riforma, ha permesso un inasprimento di pena: originariamente, la condotta in questione era punita mediante la reclusione da sei mesi a quattro anni, oggi, grazie al Codice Rosso, si è passati alla reclusione da un anno a sei anni e sei mesi.

Passando all'analisi dal punto di vista contenutistico, le diverse possibili lesioni dei beni giuridici degli atti persecutori, sono le stesse che poi analizzeremo più nel dettaglio per la condotta di *Revenge porn*.

Innanzitutto, entrambe sono definite come pluri-offensive, quindi ledono una pluralità di diritti: l'onore sessuale, alla reputazione, la privacy, la libera autodeterminazione, l'integrità morale, ma anche fisica, se compromettono lo stato di salute del soggetto passivo.

La Cassazione ha inoltre evidenziato come il delitto di “*stalking*” integri la condotta prevista all'art 612 ter nella parte in cui al comma due si fa riferimento agli strumenti informatici o telematici.

La locuzione che si riferisce a questo tipo di strumenti è stata recentemente aggiunta mediante una modifica, successiva all'introduzione dell'articolo relativo allo *stalking*, nel decreto legislativo poi convertito in legge n.119/2013.

Si prevede infatti che, mediante «l'invio reiterato alla persona offesa di sms, messaggi di posta elettronica o postati sui social network di scritti, fotografie o filmati ritraenti la sfera personale della vittima»¹⁶⁹, si può benissimo parlare di *cyber stalking*.

¹⁶⁶ FLICK G.M., voce *Libertà individuale (delitti contro la)*, in *Enc. dir.*, vol. XXIV, Giuffè, 1974

¹⁶⁷ FIANDACA, MUSCO, *Diritto Penale, parte speciale, i delitti contro la persona*, cit p. 226

¹⁶⁸ MOCCIA S., *La perenne emergenza. Tendenze autoritarie nel sistema penale*, ESI, 2000, spec. 29 ss., ci si riferisce al dl n.11/2009 “Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori” e convertito in l. 23 aprile 2009, n. 38

¹⁶⁹ Cass. Pen. Sez V n 47049/2019

Secondo la Giurisprudenza di Legittimità, ai fini della configurazione del reato di *stalking*, anche in assenza di un incontro fisico tra vittima e imputato, sono sufficienti pochi messaggi via *whatsapp* e una telefonata dal tono minaccioso, i quali conseguono che la persona offesa debba modificare le proprie abitudini¹⁷⁰.

Seguendo l'articolo 612 bis c.p., la Giurisprudenza ha condannato un uomo mediante sentenza¹⁷¹, poiché aveva posto in essere nei confronti della sua ex moglie, molte condotte persecutorie, tra cui la creazione di un profilo *Facebook* appositamente per danneggiarla, chiamandolo «lapidiamo la rovina famiglie», in cui erano postate foto intime, filmati e commenti con riferimenti impliciti ed espliciti alla parte offesa ed alla sua relazione con l'imputato.

La *ratio* del legislatore si deve ricercare nel fatto che, con l'avvento dei *social network* e dei sempre più diffusi strumenti telematici, la vittima potrebbe potenzialmente sentirsi come "circondata" e senza via di scampo.

Per questo motivo l'uso di *Internet* è percepito dal soggetto passivo come *modus operandi* anche più gravoso rispetto allo *stalking* effettuato di persona, fattispecie comune prevista dal comma uno: per tale ragione è stata inserita come aggravante.

Altri punti in comune con l'articolo 612 ter, sono la procedibilità a querela della persona offesa, e un ulteriore aumento di pena se il fatto è commesso dal coniuge o da persona legata sentimentalmente o con relazione di altra natura alla vittima.

Inoltre, entrambe sono costituite da una preventiva clausola di salvaguardia – salvo che il fatto costituisca più grave reato – volto a tutelare quei casi di due norme che si trovano in un rapporto di specialità reciproca; in questo caso, una delle due prevarrà sull'altra in base al principio del concorso apparente di norme.

Contrariamente invece al reato di diffusione illecita di immagini di natura sessuale, solo negli atti persecutori è richiesta l'abitualità, si tratta infatti di un reato istantaneo di mera condotta, la normativa parla di azioni reiterate nel tempo.

Secondo la Giurisprudenza devono essere almeno due¹⁷², devono consistere in minaccia o molestia, in modo da cagionare alla vittima ansia così grave da trovarsi continuamente in uno stato di "allarme" e timore per la propria incolumità o quella dei suoi cari.

Ciò si pone in contrasto con la letteralità dell'articolo 612 ter poiché raramente possono configurarsi condotte reiterate, infatti, in molti altri casi la continuazione dei reati non è presente nella condotta di *Revenge pornography*, per questo motivo si rende difficile la sussunzione per tutti quei reati connotati da una singola azione.

Tuttavia, secondo un orientamento della Suprema Corte non esiste a livello legislativo, un numero minimo di episodi delittuosi che facciano ritenere la fattispecie di atti persecutori integrata¹⁷³.

¹⁷⁰ Cass. Pen. sez. V, sent. n. 61/2019

¹⁷¹ Cass. Pen., Sez. V pen. 28/12/2017, n. 57764

¹⁷² Cass. Pen. Sez V n 30535/2021; Cass. Pen. Sez V n 33842/2018

¹⁷³ Cass. Pen. Sez III, 6 novembre 2018 n 11450

Inoltre, rientrano in quest'ultima disciplina, anche quegli atti indiretti rivolti subdolamente alla persona offesa.

Secondo la Corte Suprema, si può inserire come facenti parte di atti persecutori anche quegli atti di delegittimazione della persona offesa mediante diffamazione o molestie (nel caso di specie erano stati pubblicati su *YouTube* video interviste e vari post su social network a contenuto diffamatorio contro un magistrato) che valica il principio di libera espressione del pensiero, costringendo la persona offesa a cambiare le proprie abitudini di vita¹⁷⁴.

Per quanto riguarda il dolo, nell'articolo 612 bis si ritiene si faccia riferimento a un dolo generico, similmente alla disciplina prevista al reato di *Revenge porn*, al comma primo, in relazione alla mancanza di accettazione da parte della vittima alla diffusione del contenuto.

Tuttavia, al comma secondo del suddetto articolo, si allude alla necessaria presenza del dolo specifico al fine di configurazione di un danno, ponendosi quindi in netto contrasto con la finalità richiesta dalla disciplina di atti persecutori.

4.4 (Segue): Sostituzione di Persona

L'articolo 494 c.p. recita «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». La norma, come abbiamo visto per le precedenti, costituisce una fattispecie di tipo pluri-offensivo, volto a tutelare sia l'interesse della persona che è stata sostituita, la fede pubblica e il destinatario degli effetti del reato posto in essere.

Anche in questo caso, come per il comma secondo dell'art 612 ter, è configurabile il dolo specifico: l'intenzione di procurare per sé o per altri un vantaggio, che può essere patrimoniale o meno, ma anche un danno, a prescindere dalla sua tipologia¹⁷⁵.

La Suprema Corte si è espressa per un caso per cui un uomo creò un profilo su un *social*, con l'immagine della persona offesa, immettendo anche dati personali, con descrizioni dispregiative, condividendo foto della persona offesa senza il consenso e avendo anche contatti con altri utenti del sito¹⁷⁶.

Oltre che la creazione di un profilo falso, è oggetto di tutela mediante questa normativa, anche l'utilizzo di pseudonimo altrui.

¹⁷⁴ Cass. pen. Sez V n. 1813/2021

¹⁷⁵ Trib. di Firenze sez. I penale, 18 agosto 2014 in *Pluris*

¹⁷⁶ Cass. Pen. n. 25774/2014

Fra i due articoli analizzati si potrebbe prevedere una disciplina di concorso oppure un assorbimento, per il quale la sostituzione di persona è il reato "soccumbente", in quanto prevede un edittale di pena minore.

La condotta oggetto dell'articolo 494 c.p. si perfeziona nel momento in cui la persona al quale è indirizzato l'illecito venga tratta in inganno, in mancanza del perfezionamento si configura solo il tentativo¹⁷⁷; mentre nella diffusione illecita di immagini, il reato si perfeziona nel momento in cui l'immagine o il video vengono immessi nel *web*, a prescindere dalla percezione del reato da parte della persona offesa. Molte sono le massime di riferimento, come quella enunciata dalla Suprema Corte nel 2014 che prevedeva come integrato il reato di sostituzione di persona per un soggetto che ha creato un profilo *Facebook* abusando dell'immagine di un soggetto inconsapevole, per comunicare con altri utenti e condividere con loro contenuti e materiali, illecitamente¹⁷⁸.

Altra sentenza è stata emessa dal Tribunale di Trento nello stesso anno, il caso riguardava un uomo condannato per sostituzione di persona per aver creato un profilo *Facebook* con il nome della persona offesa, inducendo in errore gli utenti con cui aveva contatti, condividendo sue foto in atteggiamenti intimi e dettagli personali sulla relazione, in questo caso si è previsto il concorso con il reato di diffamazione¹⁷⁹.

4.5 (segue): Violenza Sessuale

Nel 2018, anno prima dell'entrata in vigore della riforma che ha introdotto l'articolo 612 ter, le sentenze di condanna secondo i dati ISTAT sono stati di 1870, di cui 75 violenza sessuale di gruppo, molti in più rispetto ai 1690 dell'anno prima¹⁸⁰.

Mentre per il servizio studi del Senato¹⁸¹ con l'indagine campionaria sulla "Sicurezza dei cittadini", effettuata nel 2015-2016 su un campione di 50.350 individui di 14 anni e oltre, mostra che il 46,6% sono donne.

Gli autori delle molestie a sfondo sessuale sono in larga prevalenza uomini: lo sono per il 97% delle vittime donne e per l'85,4% delle vittime uomini.

La disciplina che analizzeremo è riportata nell'articolo 609 del cod. pen. e seguenti, che definisce la violenza sessuale come: «Chiunque, con violenza o minaccia o mediante abuso di autorità, costringe taluno a compiere o subire atti sessuali è punito con la reclusione (da sei a dodici anni).

Alla stessa pena soggiace chi induce taluno a compiere o subire atti sessuali: abusando delle condizioni di inferiorità fisica o psichica della persona offesa al momento del

¹⁷⁷ Trib. di Campobasso, 7 novembre 2016 in *Pluris*.

¹⁷⁸ Cass.pen. sez. V, 23/04/2014, n.25774, in *Rivista penale* 2014, 9, 804, in *dejure*

¹⁷⁹ Trib. di Trento, 29/04/2014 n.369 in *dejure*

¹⁸⁰ Min. Giustizia, inchiesta e analisi statistica Istat violenza sessuale, anno 2018

¹⁸¹ Servizio studi del Senato, nota breve N. 232 - settembre 2020 "statistiche sulla violenza di genere"

fatto; traendo in inganno la persona offesa per essersi il colpevole sostituito ad altra persona.

Nei casi di minore gravità la pena è diminuita in misura non eccedente i due terzi».

A causa della evoluzione della sessualità nella società moderna, sempre più fluida e multiforme, ciò ha fatto sì che si verificasse un processo di "smaterializzazione" della condotta, per cui «le stesse formule giuridiche, a dispetto dell'apparente precisione, si rivelano assolutamente incapaci di normare la sessualità»¹⁸².

Per questo, in una recente sentenza della Cassazione si evince che «ai fini della definizione di atti sessuali di cui all'articolo 609-bis c.p., non è indispensabile il requisito del contatto fisico diretto con il soggetto passivo, ma è sufficiente che l'atto abbia oggettivamente coinvolto la corporeità sessuale della persona offesa e sia finalizzato ed idoneo a compromettere il bene primario della libertà dell'individuo nella prospettiva dell'agente di soddisfare od eccitare il proprio istinto sessuale»¹⁸³.

Secondo quest'ultima, la condotta di violenza sessuale sarebbe realizzabile anche mediante modalità telematiche, che siano finalizzate a soddisfare "l'istinto" sessuale e idonei a compromettere la libertà individuale tutelata dalla normativa in esame.

Si considera quindi, ormai di comune accordo, che la violenza sessuale può avvenire anche in maniera "scorporata" dalla sua valenza fisica, considerando il *cyber* spazio come "luogo" sempre più utilizzato per intrattenere relazioni intime, in cui immagini e video diventano il centro della sessualità.

Un esempio di questo fenomeno sono i sempre più frequenti casi di violenza sessuale nella realtà aumentata¹⁸⁴ (*infra*, § cap. 3 par. 3).

Si pensa quindi, che sia possibile una futura integrazione normativa volta a regolamentare l'utilizzo di strumenti telematici per commettere questo tipo di reato, per esempio mediante l'introduzione di una aggravante, come il comma terzo dell'articolo 612ter.

Anche in questo caso, come per il reato di *Revenge porn*, fondamentale per il verificarsi della fattispecie è la mancanza del consenso o la manifestazione del dissenso.

Seguendo questa affinità normativa, potrebbe svilupparsi il concorso nel caso in cui, a seguito della violenza sessuale, vengano scattate immagini o autoprodotte sotto costrizione, sfociando quindi nel sotto-ambito del 612 ter definito come "*sex extortion*", il quale integra la produzione e l'invio di materiale pornografico da parte

¹⁸² GOISIS, *La violenza sessuale: profili storici e criminologici. Una storia di 'genere'*, in www.penalecontemporaneo.it, 31 ottobre 2012, 17.

¹⁸³ Cass., Sez. III, 22 dicembre 2020, n. 36910, in *Dir. pen. e proc.*, 2021, 4, 427; Cass., Sez. III, 2 luglio 2020, n. 25266, in *Diritto di Internet*, 2020, 4, con nota di PICOTTI

¹⁸⁴ Si tratta delle cosiddette "realtà virtuali", per esempio quella sviluppata da *Meta (Facebook)*, tramite tecnologie che coinvolgono in maniera diretta i sensi degli utenti attraverso falsi segnali sensoriali, i quali quindi vivono l'esperienza di una c.d. realtà aumentata. Uno dei più recenti casi di abuso sessuale in una *virtual reality* è quello di Jordan Belamire, ragazza americana che nel 2016 ha subito un palpeggiamento mentre giocava ad un gioco con realtà aumentata (cfr. "Medium, "my first virtual reality groping, 2016, Jordan Belamire"); Cfr. DIBBELL, *A Rape in Cyberspace (Or Tiny society and How to Make One)*, in *Violation: rape in gaming*, a cura di Thorn, 2012, 21 ss.

della vittima al perpetratore, che la minaccia di diffondere materiale della stessa entità, per i quali ne ha già il possesso¹⁸⁵.

Oltre a ciò, occorre precisare che in comune le due discipline avrebbero la tutela dello stesso bene giuridico: la libertà sessuale della vittima e la sua libertà di autodeterminazione.

Perciò questi due articoli vengono associati spesso in concorso fra loro, prevedendo la possibilità dell'autore del reato di: prima minare la libertà sessuale mediante una vera e propria violenza fisica, poi decidere di caricare il contenuto online ledendo la riservatezza sessuale della persona offesa.

Infatti, considerando l'aggressione sessuale nel suo più ampio significato, venivano alla luce una serie di comportamenti che, *strictu sensu*, non venivano ricompresi nell'alveo del reato di violenza sessuale, seppur meritevoli di tutela in quanto lesivi dei suddetti principi.

Tra questi, la diffusione e la produzione non consensuale di materiale di carattere sessuale, la produzione di quest'ultimo sotto costrizione.

Ambiti che poi furono ricoperti dalla riforma del Codice Rosso e dall'articolo 612 ter, per questo motivo possiamo definire i due reati strettamente collegati fra loro.

Molte, infatti, sono le casistiche della Suprema Corte che condividono questa visione¹⁸⁶.

Tuttavia, sebbene questi reati abbiano degli aspetti simili, mentre si considera plausibile un concorso, non è possibile considerare un eventuale “assorbimento” delle due normative, poiché l'oggetto della condotta costituisce un *discrimen* vero e proprio: da una parte la violenza sessuale, dall'altra la diffusione di immagini a sfondo sessuale. Ciò non accade invece con la diffusione di materiale pedopornografico, articolo 600 ter c.p., per il quale sarebbe possibile un assorbimento, ma anche un concorso apparente¹⁸⁷.

Molte, infatti, sono le casistiche della Suprema Corte che condividono questa visione¹⁸⁸.

Di recente, un caso che ha destato preoccupazione nella cronaca e che può essere ricompreso nell'ipotesi di concorso di reati, è avvenuto a Palermo, dove sette ragazzi sono stati indagati per aver violentato una coetanea e per aver ripreso la violenza diffondendo i due video ad altri quattro amici estranei ai fatti.

¹⁸⁵ CITRON, *Sexual Privacy*, in *Yale Law Journal*, 2019, 128, 1895 ss.; LIGGETT O' MALLEY-HOLT, *Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime*, in *Journal of Interpersonal Violence*, 2022, 37, 1-2, 258 ss.

¹⁸⁶ Alcuni esempi, Cass. pen. sez. III, 24/05/2023, (ud. 24/05/2023, dep. 13/10/2023), n.41573; Cass. pen. sez. IV, 05/11/2019, (ud. 05/11/2019, dep. 27/01/2020), n.3205; Cass. pen. sez. III, 11/10/2011, (ud. 11/10/2011, dep. 23/01/2012), n.2681

¹⁸⁷ TAMBORINI L., SIMICICH M., “il revenge porn ad un anno dall'entrata in vigore: prime considerazioni”, ottobre 2020

¹⁸⁸ Alcuni esempi, Cass. pen. sez. III, 24/05/2023, (ud. 24/05/2023, dep. 13/10/2023), n.41573; Cass. pen. sez. IV, 05/11/2019, (ud. 05/11/2019, dep. 27/01/2020), n.3205; Cass. Pen. sez. III, 11/10/2011, (ud. 11/10/2011, dep. 23/01/2012), n.2681

Il processo è iniziato ad aprile scorso: per il più giovane che all'epoca dei fatti era minorenne, è stato utilizzato il rito abbreviato, mediante il quale l'imputato è stato condannato a otto anni e otto mesi di carcere dal Tribunale dei minori.

Per coloro che hanno solamente ripreso con il telefono l'accaduto, sono state previste attenuanti che hanno notevolmente ridotto la pena.

L'Autorità Garante per la Privacy, a tutela della persona offesa, ha rivolto un avvertimento a Telegram, con due provvedimenti d'urgenza, per garantire la riservatezza della vittima¹⁸⁹.

Il Pm, Monica Guzzardi, ha chiesto la condanna per Angelo Flores, a due anni e quattro mesi per la diffusione illecita di immagini e video sessualmente espliciti (prevedendo uno sconto di pena per aver chiesto il rito abbreviato).

Per quanto definito dalla stampa, lo stupro sarebbe stato ripreso dagli stessi protagonisti e le immagini sarebbero state persino messe in vendita online¹⁹⁰; infatti, in duemila su Telegram hanno proposto offerte per arrivare al video: «Se qualcuno ce l'ha pago bene».

Si aspetta la sentenza definitiva il prossimo 18 Marzo.

Secondo una sentenza della Cassazione¹⁹¹, si può condannare per l'articolo 609 bis c.p. anche un minore che filma con il cellulare una violenza sessuale di gruppo nei confronti di una ragazzina, la Corte infatti conferisce a quest'ultimo la stessa responsabilità degli altri membri del gruppo, anche se si è “limitato” a riprendere con il telefonino.

4.6 (Segue): Diffusione di riprese e registrazioni fraudolente

L'articolo 617 *septies* del cod. pen., introdotto dal decreto legislativo n 216 del 2017, si inserisce nel titolo relativo ai delitti contro la persona (Titolo XII), nel capo dedicato ai delitti contro la libertà individuale (Capo III) e nella sezione che prevede i delitti contro l'inviolabilità dei segreti (artt. 616 e ss. c.p.).

La fattispecie prevede che: «Chiunque, al fine di recare danno all'altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di incontri privati o registrazioni, pur esse fraudolente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione, è punito con la reclusione fino a quattro anni.

La punibilità è esclusa se la diffusione delle riprese o delle registrazioni deriva in via diretta ed immediata dalla loro utilizzazione in un procedimento amministrativo o giudiziario o per l'esercizio del diritto di difesa o del diritto di cronaca. Il delitto è punibile a querela della persona offesa».

¹⁸⁹ Comunicato del 23 Agosto 2023, n. 9923426

¹⁹⁰ Cfr. Stupro a Palermo, Il corriere 23 Agosto 2023

¹⁹¹ Cass. Pen. sent.n.11560 del 25.03.2010

Con questa fattispecie si volevano tutelare più aspetti che riguardano la sfera personale della vita della vittima, come l'onore e la dignità ma anche la libertà e segretezza della corrispondenza.

Quest'ultima in particolare, è tutelata dall'articolo 15 della Costituzione «La libertà e la segretezza della corrispondenza e di ogni forma di comunicazione sono inviolabili.

La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge».

Le differenze con l'articolo 612 ter, anche se *prima face* sono minime, in realtà ci sono e costituiscono il motivo di una necessaria introduzione nell'ordinamento della fattispecie in esame.

Dalla prima frase dell'articolo di diffusione di riprese e registrazioni, emerge come obiettivo ultimo quello di recare un danno all'altrui reputazione, costituendone quindi una fattispecie che prevede il dolo specifico.

In quest'alveo normativo, di conseguenza, possono essere ricomprese solo quelle condotte diffusive del contenuto sessualmente esplicito poste in essere con l'unico fine di recare danno alla persona interessata.

Nell'articolo in questione, fondamentale risulta essere il carattere fraudolento della condotta, sottolineata più volte nel comma primo della medesima, con la differenza che l'articolo 612ter parla non di carattere fraudolento, ma in modo più generale, di acquisizione e sottrazione, avente ad oggetto materiale sessualmente esplicito.

Rapportando queste due normative sotto la luce del dolo generico o specifico, si sottolinea ancor di più l'indeterminatezza che caratterizza, fin dai primi momenti in cui si è discusso, l'articolo 612ter.

Questo perché, se il dolo fosse generico allora verrebbe applicato l'articolo 612 ter comma primo, ma i problemi sorgono in relazione al dolo specifico: entrambe le normative pongono dei confini descrittivi delle condotte, non del tutto precisi, per questo potrebbero sorgere delle situazioni per cui la presenza della volontà di arrecare 'nocumento' alla persona offesa, renda possibile l'applicabilità di entrambe¹⁹².

Altra differenza che può essere colta è il *quantum* di pena, che in questo caso risulta essere molto inferiore rispetto alla disciplina di diffusione illecita di immagini sessualmente esplicite.

Infatti, per l'articolo 617 *septies* si prevede la reclusione fino a quattro anni, mentre per le condotte all'articolo 612 ter si prevede la reclusione fino a sei anni.

Quest'ultima non consente l'applicazione della non punibilità particolare tenuità del fatto, proprio a causa della elevata cornice edittale¹⁹³.

¹⁹² PALMIERI G.M., *L'accoglimento del concetto di "genere" come rischio di una tutela penale a binario differenziato, art 612ter e tutela della riservatezza*, 2022

¹⁹³ Il decreto legislativo di attuazione della legge 27 settembre 2021 n. 134 che prevede la delega al governo per l'efficienza del processo penale, in materia di giustizia riparativa, e disposizioni per la velocità di definizione dei procedimenti giudiziari, prevede che l'art. 131-bis c.p. operi quando il minimo edittale non sia in grado di superare i due anni, l'art. 612- ter c.p. rientra quindi adesso nel

La legge delega inizialmente aveva previsto l'introduzione dell'avverbio “solo” (“al solo fine di recare danno alla reputazione o all’immagine altrui”), quindi il fine ultimo di arrecare danno doveva configurarsi come una condotta esclusiva e non alternativa, come invece avviene nella odierna formulazione¹⁹⁴.

Mentre, come abbiamo analizzato in precedenza, nel reato di *Revenge porn* vengono ricomprese anche ulteriori *ratio* che possano aver portato la persona a commettere questo reato.

La locuzione "Diffonde con qualsiasi mezzo riprese audio o video" si riferisce alla divulgazione effettuata adottando qualsiasi modalità (mezzo stampa, *internet*, telefoni, tv o altri mezzi) riprese audio o video, evitando di ricomprendere nella disciplina l'elemento che più caratterizza la diffusione illecita prevista all'articolo 612 ter: le immagini, che diventano elemento imprescindibile per la costituzione della fattispecie in esame.

Tornando a descrivere la natura fraudolenta della condotta, per *natura fraudolenta* si intende la capacità di nascondere in qualsiasi modo la modalità illecita del comportamento a chi la subisce, riferendosi pertanto solamente ad alcuni atteggiamenti ricompresi nell'articolo 612 ter.

Si escludono infatti, nettamente tutti quei casi dove le riprese di immagini audio o video avvengano consensualmente con la persona offesa e poi in un secondo momento, diffuse senza che la vittima abbia accettato tale condotta divulgativa.

In questo modo, vengono meno anche tutti quegli accadimenti per cui soggetti che hanno ricevuto il contenuto da altri, si occupino della mera divulgazione del contenuto; condotta invece tutelata dall'articolo di diffusione illecita di immagini¹⁹⁵.

5.0 (segue): Iter legislativo anteriforma del 2019

L'intervento del Giudice italiano in tema di *Revenge porn* è stato ritenuto come imprescindibile, ai fini di una più ampia cornice di criminalizzazione a livello internazionale.

La diffusione di immagini sessualmente esplicite è una materia che è stata introdotta negli ordinamenti di vari paesi, più o meno tutti nello stesso periodo, come Spagna, Germania, Giappone, Canada, Stati Uniti ecc..; discipline che analizzeremo singolarmente nel prossimo capitolo.

novero dei reati in ogni modo esclusi dalla sfera operativa della non punibilità per particolare tenuità del fatto.

¹⁹⁴ Giurisprudenza Penale Web, 2019, 4

¹⁹⁵ Cfr BRIZZI, *Diffusione illecita di immagini o video sessualmente espliciti: Tra tutela della privacy e Revenge porn* in: *Il penalista*, 2021.

Tuttavia, sebbene questa fattispecie denoti una grande casistica è sempre stata di difficile inquadramento teorico¹⁹⁶.

A fronte del quadro legislativo italiano altamente frammentato in materia, non essendo possibile inquadrare la fattispecie in una specifica norma, era necessario un tempestivo intervento legislativo¹⁹⁷.

Infatti a seguito della triste vicenda di Tiziana Cantone, la ragazza suicidatasi in seguito alla diffusione di immagini sessualmente esplicite che la ritraevano, e la conseguente vera e propria persecuzione ricevuta sia sulle piattaforme social che dal vivo, si è sentita l'esigenza di criminalizzare la pornografia non consensuale.

Infatti, poche settimane dopo il suo suicidio, il 27 settembre 2016 Sandra Savino presentò la prima proposta di legge che aveva come obiettivo ultimo quello di finalizzare l'introduzione di una normativa *ad hoc* per punire le condotte di *Revenge pornography*¹⁹⁸.

La deputata, dichiarò, come introduzione alla proposta di legge:

«Il cosiddetto "*Revenge porn*" è l'espressione anglosassone con cui si indica la pubblicazione sul *web* di foto o video, anche molto intimi ed espliciti, a scopo di vendetta.

Spesso accade che la diffusione di un certo tipo di immagini o video pornografici segua la fine di una relazione sentimentale e venga utilizzata come strumento di vendetta nei confronti delle vittime, che sono prevalentemente donne.

La "vendetta porno" è l'esempio più estremo di come, in certi casi, le nuove tecnologie vengano utilizzate da alcuni uomini con l'unico scopo di esercitare il potere e il controllo sulle donne.

Sono sempre più numerose le vicende di cronaca che vedono protagoniste giovani donne che, senza aver espresso alcun consenso, scoprono *online*, sui *social network*, proprie immagini intime, ormai condivise da un numero molto elevato di utenti, quindi divenute 'virali'.

Si tratta di episodi gravissimi, che hanno ripercussioni a livello psicologico inimmaginabili, spingendo in alcuni casi le vittime fino a gesti estremi.

Negli Stati Uniti d'America il fenomeno del "*Revenge porn*" è riconosciuto a livello giuridico e conseguentemente perseguito, in molti Stati¹⁹⁹.

Le leggi vigenti in Italia non riescono a contrastare adeguatamente il fenomeno dei video privati diffusi per vendetta: per questo serve una normativa adeguata al periodo storico che stiamo vivendo.

¹⁹⁶ per un maggiore approfondimento Cfr. G.M. CALETTI, "*Revenge Porn*". *Prime considerazioni in vista dell'introduzione dell'art. 612-ter c.p.: una fattispecie "esemplare", ma davvero efficace?* in *Diritto penale contemporaneo*, 29.5.19

¹⁹⁷ CADOPPI A. - VENEZIANI P., *Elementi di diritto penale: parte speciale, vol. II, I reati contro la persona tomo II, I reati contro i soggetti deboli*, III edizione Padova, 2023

¹⁹⁸ Proposta di legge n 4055 alla Camera dei deputati, Sandra Savino, 27 settembre 2016

¹⁹⁹ RUVALCABA Y., A. A. EATON, *Nonconsensual Pornography among U.S Adults: A Sexual Scripts Framework on Victimization, Perpetration, and Health Correlates for Women and Men*, *Psychology of Violence*, 10(1), 68–78.

Sarebbe opportuno il riconoscimento di questo reato al pari dell'estorsione, perché si configura come un grave delitto contro la *privacy*, oltre a essere un delitto di genere, perpetrato quasi esclusivamente nei confronti delle donne.

La presente proposta di legge prevede l'introduzione dell'articolo 612-*ter* del Codice penale, concernente il reato che si manifesta attraverso la pubblicazione via *internet* di contenuti pornografici, sia fotografici che video, senza l'esplicito assenso dei soggetti interessati.

La pubblicazione *online* di simili contenuti è punita con la reclusione da uno a tre anni e la pena è aumentata della metà se il fatto è commesso dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa».

5.1 (segue): La prima proposta di legge di *Revenge Porn*

Il testo della proposta di legge, affidato alla II Commissione Giustizia della Camera dei deputati, recita «È punito con la reclusione da uno a tre anni chiunque pubblica nella rete internet, senza l'espresso consenso delle persone interessate, immagini o video privati, comunque acquisiti o detenuti, realizzati in circostanze intime e contenenti immagini sessualmente esplicite, con conseguente diffusione di dati sensibili, con l'intento di causare un danno morale alla persona interessata.

La pena è aumentata della metà se il fatto è commesso dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa». Questa proposta non riuscì ad essere assegnata per l'esame in Assemblea.

Seguentemente, venne anche proposta una petizione *online* per richiedere al Parlamento di intervenire in materia, affinché approvassero una specifica legge per contrastare questo fenomeno.

Dopo pochi giorni, si erano raggiunte le 100 mila firme, la petizione “#Intimità violata” è stata proposta dalle associazioni “Insieme in rete”, “Bossy”, “I Sentinelli” sulla piattaforma *change.org*²⁰⁰.

La richiesta risulta aver raccolto più di 126.000 sostenitori, questa venne consegnata all'ex presidente della Camera Laura Boldrini, la quale dichiarò in un'intervista di aver ascoltato i cittadini, e che avrebbe preparato una proposta di legge in merito²⁰¹.

Durante i primi mesi del 2019, a causa dell'esponenziale crescita di questo fenomeno, la pornografia non consensuale è tornata di nuovo nel centro della scena politica italiana, con il caso della Deputata Giulia Sarti, divenuta anch'essa vittima di porno-vendetta.

Le sue foto private (eseguite molti anni prima) giravano *online* e nelle *chat*²⁰², tanto che la deputata ha deciso di autosospendersi dal Movimento Cinque Stelle, di

²⁰⁰ sito destinato all'attuazione di petizioni da parte dei cittadini.

²⁰¹ “*Revenge porn, arriva una proposta di legge anche in Italia*”, in Wired.it, 28.1.19

²⁰² SARZANINI F., *Giulia Sarti, le foto e i video in rete*, Corriere della Sera (Mar. 14, 2019)

abbandonare la presidenza della Commissione Giustizia, ma non ha rinunciato al suo ruolo in Parlamento²⁰³.

Il Garante della Privacy, allarmato dall'aumento delle condivisioni, ha diffuso una nota in cui richiedeva ai mezzi di informazione di non diffondere «dati riguardanti la sfera intima di una persona per il solo fatto che si tratti di un personaggio noto o che eserciti funzioni pubbliche, richiedendo invece il pieno rispetto della sua vita privata quando le notizie o i dati non hanno rilievo sul suo ruolo e sulla sua vita pubblica».

Nel contempo, molte forze politiche e istituzionali hanno mostrato vicinanza alla deputata, come Roberto Fico, Mara Carfagna, Giuditta Pini.

Matteo Salvini si è espresso in riferimento a questo caso dicendo «È una vicenda disgustosa e molto grave. È nostro dovere proteggere la libertà e la privacy di Giulia Sarti e delle altre persone, spesso giovani, che subiscono e/o hanno subito lo stesso vergognoso trattamento».

Il 19 febbraio 2019 venivano presentati in Senato tre nuovi disegni di legge al fine di rendere meritevole di sanzione penale le condotte oggetto della fattispecie, da parte delle forze politiche M5S, FI e PD, rispettivamente i Ddl. n. 1076, 1134, 1166.

Analizzandoli più dettagliatamente, il decreto-legge n. 1076 prevedeva al primo comma «Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni, chiunque pubblica attraverso strumenti informatici o telematici, immagini o video privati sessualmente espliciti, senza l'espresso consenso delle persone ivi rappresentate, al fine di provocare nelle persone offese gravi stati di ansia, di timore e di isolamento²⁰⁴».

Era stata prevista quindi, come per il successivo 612 ter la clausola di salvaguardia - salvo che il fatto costituisca più grave reato - ma la pena in questo caso è inferiore, rispetto a quella che poi verrà approvata nel nostro Codice penale.

Critica è la differenza che veniva affrontata in relazione alla "pubblicazione e diffusione" del contenuto.

Come si evince dal titolo della norma che il decreto vuole introdurre, si tratta di una distinzione tecnica che voleva rendere effettiva la differenza tra chi diffonde per primo l'immagine lesiva della dignità della persona, e chi, in un secondo momento, quando l'immagine già è online, la divulga ulteriormente.

Tuttavia, questa distinzione rischiava di rendere ancor più ristretto l'ambito applicativo della fattispecie, limitando ai soli casi di "pubblicazione", per esempio, su *Facebook* o *X* (il vecchio *Twitter*), la condotta lesiva.

In questo modo, si eliminavano dalle condotte ivi rappresentate, tutti quei *social network* che non sono soggetti a pubblicazione ma solamente a invio o condivisione, come *whatsapp*.

Nella odierna disciplina è stata mantenuta la digressione per cui si differenziava tra "primi diffusori" e "secondi diffusori".

²⁰³ La repubblica, *Caso rimborsi, Giulia Sarti si autosospende dal Movimento 5 Stelle* (Feb. 26, 2019)

²⁰⁴ testo completo analizzabile sul sito del Senato Della Repubblica, Legislatura 18ª - Disegno di legge n. 1076

In questa proposta di legge però, la pena assegnata per i secondi, era una semplice multa e non aveva quindi, la stessa portata punitiva di quella prevista oggi dal comma secondo dell'articolo 612 ter, poiché poneva, invece, l'attenzione sulla tutela dal punto di vista civilistico.

Altre circostanze mantenute nella normativa di riferimento, sono l'aggravante in caso di persona legata da una relazione affettiva alla vittima, ma anche la procedibilità a querela e la sua scadenza entro i sei mesi.

Elemento particolare nel ddl in esame, è l'aggravante della avvenuta morte della persona offesa, fattispecie mancante nella odierna diffusione illecita di immagini sessualmente esplicite, poiché già ricoperta, nei casi ove fosse possibile, dall'articolo 586 c.p.

In caso di suicidio prevedeva la proposta, che le circostanze attenuanti concorrenti, diverse dall'articolo 94 e 114 c.p., non possano essere ritenute equivalenti o prevalenti. L'articolo due introduceva la facoltà della persona offesa, per il tempestivo intervento di rimozione delle immagini e dei video, di mandare al gestore della piattaforma *online* su cui è stato caricato il contenuto, una richiesta di rimozione del contenuto sessualmente esplicito diffuso senza la sua approvazione, mantenendo in ogni caso i dati originali.

5.2 (segue): La seconda e la terza Proposta di legge

Il ddl n. 1134 volto alla criminalizzazione di “diffusione di video privati” introduceva come aggravante la condotta di "*doxxing*<", ossia la tendenza a rendere note informazioni personali della vittima, oltre che le immagini a carattere sessuale²⁰⁵. Questa non è stata mantenuta nella disciplina di legge vigente.

La Dottrina, in merito alle aggravanti, ritiene sia meno convincente la scelta di prevedere nella proposta di legge, un'aggravante per i casi per cui le immagini siano state tratte di nascosto da chi le abbia successivamente diffuse.

L'ipotesi è già tutelata adeguatamente da altre norme incriminatrici del Codice (v. artt. 615-bis e 617-septies c.p.).

L'iter da seguire in caso di reato di *Revenge porn*, prevedeva che se entro ventiquattro ore dall'avvenuto accoglimento dell'istanza, il responsabile della piattaforma non comunicava di aver accettato l'incarico per la rimozione, e non provvedeva entro un limite di quarantotto ore, allora la vittima poteva proporre reclamo al Garante della privacy oppure ricorrere all'Autorità Giudiziaria, ai sensi di quanto previsto dal Codice della Privacy.

Nel testo di legge viene infatti sottolineata l'importanza, all'articolo tre, della finalità preventiva che detiene la legge in esame; finalità che deve essere portata a termine

²⁰⁵ ddl n.1134/2019, introduzione reato diffusione di video privati, XVIII Legislatura

anche mediante l'introduzione di una "educazione digitale" presente nelle istituzioni scolastiche²⁰⁶.

Tuttavia, questa parte non venne presa in considerazione dal legislatore.

La terza proposta di decreto-legge, n. 1166 prevedeva il collocamento del reato, grazie alla riserva prevista al decreto legislativo 21/2018²⁰⁷, nel Codice della Privacy e non nel Codice penale, come era stato fino a quel momento previsto.

La proposta arrecava il titolo "dati personali idonei a rivelare la vita sessuale".

Si legge nel testo di legge che:

«Chiunque al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, effettua, in assenza del consenso dello stesso, una comunicazione plurima o una diffusione, con qualsiasi mezzo, di dati personali idonei a rivelarne la vita sessuale, è punito con la reclusione da due a cinque anni e si procede d'ufficio». Il dibattito fu molto lungo, e intervenne ancora Giulia Sarti dicendo che il reato di *Revenge porn* non potesse risolversi attraverso l'approvazione di un "mero emendamento".

Si sentiva l'esigenza di una vera e propria discussione non solo di carattere parlamentare ma "giuridico-sociale".

Viste le divergenze sulla questione, la deputata Stefania Ascari decise di proporre un nuovo emendamento in Commissione Giustizia, al disegno di legge, che mirava a mettere d'accordo le opposizioni.

Queste, ai fini della approvazione, hanno rinunciato a proporre sub-emendamenti, con l'obiettivo di stabilire uno schema unitario a tutela della violenza di genere²⁰⁸.

La settimana prima, era stato proposto lo stesso emendamento da Forza Italia al Partito Democratico, ma aveva ottenuto voti contrari dal Movimento Cinque Stelle e dalla Lega.

Quest'ultima aveva anche proposto un ulteriore emendamento, che però è stato successivamente ritirato a causa dei voti negativi del Movimento Cinque Stelle: prevedeva una forma di castrazione chimica per i condannati per reati sessuali, a tre condizioni: che venisse fornito il consenso informato, che ci sia l'assenso del condannato, e che in nessun modo la procedura possa essere reversibile.

²⁰⁶ si legge nel testo di legge "è così previsto che entro 30 giorni dall'entrata in vigore della legge, il ministero dell'istruzione, dell'università e della ricerca, sentito il ministero della giustizia, adotti linee guida per la prevenzione nelle scuole del delitto di pubblicazione e diffusione di immagini e video privati sessualmente espliciti senza il consenso delle persone rappresentate, da aggiornare con cadenza biennale. Il disegno di legge indica già per il triennio 2019-2021 gli interventi mirati alla prevenzione e sensibilizzazione rispetto al delitto di cui all'art 612 ter del Codice penale..."

²⁰⁷ d.lgs. 21/2018 in vigore dal 6 aprile dello stesso anno, sancisce "nuove disposizioni che prevedono reati possono essere introdotte nell'ordinamento solo se modificano il Codice penale ovvero sono inserite in leggi che disciplinano in modo organico la materia". A tal proposito cfr. BENARDI, nel *"il nuovo principio della 'riserva di codice' e le modifiche al Codice penale: scheda illustrativa"*.

²⁰⁸ PITTARO P., *Il c.d. "Codice rosso" sulla tutela delle vittime di violenza domestica e di genere*, in *Famiglia e diritto*, 2020

Il 2 aprile 2019 l'Assemblea approvò con la totalità di voti a favore, l'emendamento "Bipartisan", grazie a ciò finalmente fu possibile l'introduzione nel nostro ordinamento della nuova disciplina che criminalizza le condotte di diffusione illecita di immagini o video sessualmente espliciti, prevedendo proprio quest'ultima locuzione come titolo del nuovo articolo 612 ter del Codice penale²⁰⁹.

Con una nota, Francesca Businarolo del Movimento Cinque Stelle, Presidente della Commissione Giustizia alla Camera, ha spiegato: «Portiamo in Aula un emendamento della Commissione presentato dalla relatrice Stefania Ascari e condiviso da tutte le forze politiche, di maggioranza e opposizione. Felici per aver trovato questa intesa».

CAPITOLO II - IL CODICE ROSSO E L'INTRODUZIONE DELL'ART. 612TER

SOMMARIO:

1. La riforma del 2019 - Il codice Rosso e le novità di recente introduzione. 2. L'articolo 612ter, diffusione illecita di immagini o video sessualmente espliciti. 3. I casi Giurisprudenziali che hanno contribuito alla consolidazione della disciplina. 4. Il *Revenge porn* negli ordinamenti stranieri

una necessaria premessa

Durante questo capitolo, per arrivare a trattare in maniera specifica il reato di diffusione illecita di immagini o video sessualmente espliciti, introdotto dalla riforma, parlerò prima delle novità generalmente inserite in quest'ultima.

Citerò altri reati che sono stati aggiunti insieme all'articolo 612ter, come l'articolo 583 quinquies, che si riferisce ai danni provocati tramite lo sfregio del viso di una persona, oppure la fattispecie all'articolo 558 bis "induzione al matrimonio".

Parlerò anche di tutte quelle modifiche sostanziali al codice di procedura penale, per poi giungere alla descrizione dettagliata della fattispecie del *Revenge porn*, trattando nel dettaglio tutti gli elementi che caratterizzano questo fenomeno, dal punto di vista penalistico: il concetto di nocumento, elemento soggettivo e oggettivo, la clausola di salvaguardia, per citarne alcuni.

Affronterò altri casi giurisprudenziali, tra i più importanti, che hanno segnato la storia del *Revenge Porn* e della violenza di genere in Italia, come il caso di Tiziana Cantone e Giulia Sarti, ma questi non sono gli unici; infatti, negli ultimi anni, c'è stato un incremento di questi casi non solo nel nostro paese, ma nel mondo.

²⁰⁹ CALETTI, *Revenge porn. Prime considerazioni in vista dell'introduzione dell'art 612 ter cp: una fattispecie "esemplare", ma davvero efficace?* in Diritto Penale Contemporaneo, 2019.

Inquadrerò il fenomeno anche dal punto di vista statistico, analizzando anche gli aspetti per i quali, secondo la Dottrina, il legislatore dovrebbe avviare ulteriori riforme, aggiungendo tutte quelle *sub specie* che non sono state previste nella normativa, per questioni di celerità di entrata in vigore del codice.

Infine, mi focalizzerò sul *modus operandi* degli altri Stati, confrontando le decisioni del legislatore europeo ed *extra* europeo, con quelle Italiane, ponendo l'attenzione anche a casi rilevanti che si sono verificati nel mondo, in modo tale da mettere in luce le differenze e le novità della nostra disciplina rispetto a quella straniera.

In questo capitolo, infine, voglio mettere in luce gli aspetti negativi e positivi della Riforma e delle conseguenze dell'introduzione del reato di diffusione illecita di immagini o video sessualmente espliciti, in modo tale da porre le basi per poter comprendere, nei successivi capitoli, come la tecnologia ha influenzato questo tipo di condotta.

1.0 (segue): La riforma del 2019 - Il Codice Rosso e le novità di recente introduzione

Il legislatore italiano ha introdotto, mediante la legge n. 69/2019²¹⁰, il cosiddetto "Codice Rosso" grazie a spinte sovranazionali e all'incessante necessità di regolamentare le condotte di violenza di genere.

Il decreto-legge, il quale prevede «Modifiche al Codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere», entrò in vigore il 9 agosto 2019.

Sebbene già ci fossero nel nostro ordinamento delle tutele generali in grado di fornire un adeguato livello di criminalizzazione dal punto di vista sanzionatorio, con questa Riforma, il legislatore ha voluto introdurre delle novità, su più livelli, in ottica della maggior tutela alle vittime di violenza domestica e di genere.

Si continuano comunque ad applicare, a seconda dei casi specifici, le circostanze aggravanti ad effetto comune, se il soggetto agisce per «per motivi abietti e futili», oppure con «crudeltà verso le persone», «con abuso di autorità o di relazioni domestiche, [...] di coabitazione, o di ospitalità», oppure, tutte, considerando il caso di «minorata difesa» o di persone «vulnerabili».

Inoltre, non bisogna sottovalutare il dato Costituzionale, che valorizza il principio di non discriminazione e uguaglianza, tramite gli articoli due e tre si prevede, rispettivamente «La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale»,

²¹⁰ in merito, ALGERI L., *Il c.d. Codice rosso: tempi rapidi per la tutela delle vittime di violenza domestica e di genere*, in *Diritto penale e processo*, 2019, 10, pp. 1363 ss.; BASILE E., *La tutela delle donne dalla violenza dell'uomo: dal Codice Rocco ... al codice Rosso*, in *Diritto penale e uomo*, 2019

«Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali», questi sottolineano la necessità di garantire uguaglianza tra i sessi, senza discriminazioni di genere, nel rispetto dei diritti inviolabili dell'uomo.

Tuttavia, nella Riforma del Codice Rosso, non sussiste una definizione precisa di "violenza di genere" o "violenza domestica": questo problema tecnico-lessicale è stato risolto da una normativa sovranazionale, la Convenzione di Istanbul, adottata dal Consiglio d'Europa nel 2011, ratificata con legge n. 77/2013²¹¹.

Secondo quest'ultima, «con il termine “genere” ci si riferisce a ruoli, comportamenti, attività e attributi socialmente costruiti che una determinata società considera appropriati per donne e uomini».

Mentre, scendendo più nel dettaglio, il 117° considerando della direttiva n. 29/2012 UE del Parlamento Europeo e del Consiglio²¹², il quale fornisce protezione in materia di diritti e assistenza alle vittime da reato, definisce la violenza di genere come «Diretta contro una persona a causa del suo genere, identità di genere o della sua espressione di genere o che colpisce in modo sproporzionato le persone di un particolare genere²¹³».

Mentre, la violenza domestica come «tutti gli atti non episodici di violenza fisica, sessuale, psicologica, economica che si verificano all'interno della famiglia o del nucleo familiare o tra attuali o precedenti coniugi o persone legate da relazione affettiva in corso o pregressa, indipendentemente dal fatto che l'autore di tali reati condivida o abbia condiviso la stessa residenza con la vittima²¹⁴».

Di recente, è stata istituita la prima organizzazione a livello europeo per tutelare i diritti umani sul *web*, la *Cyber Rights Organization* (CRO), con sede in Olanda. Obiettivo fondamentale di questa fondazione è quello di dare assistenza legale alle vittime di violenza di genere online, *Revenge porn*, *doxxing*, *hate speech*, *cyberbullismo*.

Inoltre, prevedono l'attuazione di campagne di sensibilizzazione alla tutela dei diritti digitali.

Le menti che hanno fondato questa istituzione sono Silvia Semenzin, sociologa e attivista promotrice dell'art. 612ter c.p., Annachiara Sarto, laureata in diritto internazionale all'Università dell'Aja e direttrice della Ong *Protection4kids*, ma anche consulente del Dipartimento delle Operazioni di Pace nella Squadra speciale di protezione dei minori delle Nazioni Unite; Andrea Baggio, CEO di *Reputationup*; Juan Ricardo Palacio, esperto di *cybersecurity* e informatica forense.

Il CEDAW, Comitato per l'eliminazione della discriminazione nei confronti delle donne, ha effettuato un rapporto nei confronti dell'Italia, in cui prevedeva, in relazione alla violenza domestica, la considerazione secondo cui, pur avendo giudicato

²¹¹ POGGI F., *Violenza di genere e Convenzione di Istanbul: un'analisi concettuale*, in *Diritti umani e diritto internazionale*, 2017

²¹² sostituisce la decisione quadro GAI n. 220/2001, (in Gazz.Uff. U.E., 14.11.2012, L 315/57)

²¹³ Direttiva n 29/2012 Parlamento Europeo e Consiglio Europeo, nelle Premesse

²¹⁴ dl n. 119/2013 articolo 3 comma 1; decreto-legge recante disposizioni urgenti in materia di sicurezza e per il contrasto alla violenza di genere.

positivamente l'introduzione della fattispecie di cui all'art. 612 *bis* c.p. con la Legge 11/2009, permangono in ogni caso delle criticità sui fenomeni di violenza domestica e di genere²¹⁵.

Il comitato ha rivolto, pertanto, un avvertimento al legislatore italiano, affinché lo Stato intervenisse per poter garantire una tempestiva protezione nei confronti delle vittime di questi episodi.

Sebbene anche la Convenzione di Istanbul abbia richiesto, all'articolo 8, lo stanziamento di risorse finanziarie al fine di effettuare programmi che possano contrastare tutte le forme di violenza, rientranti nella disciplina prevista dalla Convenzione, il legislatore non ha seguito appieno questo dettato.

Infatti, possiamo notare come l'articolo 18 della legge n.69/2019 in tema di sicurezza e violenza di genere ha abrogato l'articolo 5 bis comma secondo lettera d, legge n. 119/2013 per la parte in cui veniva previsto lo stanziamento di un terzo dei fondi regionali per le "pari opportunità" e per l'istituzione di centri e di case rifugio per contrastare il fenomeno della violenza contro le donne²¹⁶.

Pertanto, si ritiene sia necessario un intervento legislativo per porre una soluzione sì penalistica, ma anche multidisciplinare, nel rispetto dei principi di sussidiarietà e proporzionalità²¹⁷.

In questo contesto si è espressa anche la Corte EDU nel caso *Talpis c. Italia*²¹⁸, con la quale lo Stato italiano è stato condannato per la violazione degli articoli 2, 3 e 14 CEDU in un'ipotesi di violenza domestica che aveva comportato l'omicidio del figlio della vittima e il tentato omicidio della stessa.

Secondo la Corte, la violazione dell'art. 2 CEDU, riguardante il diritto alla vita, è stata rilevata non solo nella parte in cui prescrive allo Stato l'obbligo, in negativo, di astenersi dal pregiudicare la vita altrui, ma anche in riferimento all'obbligo, positivo, riguardante la predisposizione in via preventiva di misure volte a proteggere le vittime di violenza domestica.

Nel caso in esame, è stata evidenziata l'inerzia delle Forze dell'ordine che ha portato al verificarsi dell'evento, avendo perciò contribuito al ripetersi di gravi forme di violenza: le autorità avrebbero dovuto percepire la situazione di pericolo e agire di conseguenza, tempestivamente.

Ancora, la violazione dell'articolo 3 Cedu per il mancato adempimento degli obblighi di intervento, e la violazione dell'articolo 14 poiché il non rispetto dell'obbligo di protezione ha comportato, nel caso di specie, una violazione del divieto di non discriminazione.

²¹⁵ DAVICO A., *stalking, atti persecutori, articolo 612bis c.p.*, 2022

²¹⁶ Si tratta del «Fondo per le politiche relative ai diritti e alle pari opportunità, di cui all'articolo 19, comma 3, del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248, in Gazz. uff. n. 186 del 11.08.2006.

²¹⁷ PORTALUPI, VILLASI, *Presente e futuro della violenza di genere. A che punto siamo dopo il codice rosso*, cit., 89 ss. In *Diritto Penale e Uomo*, 2020

²¹⁸ (udienza del 2.03.2017)

A causa di molti casi come questi, si è sentita la necessità nel diritto interno di una riformulazione nella tutela penale nei confronti delle violenze domestiche e di genere: è in tale contesto che si colloca il Codice Rosso, e in quest'ambito infatti, si alloga l'introduzione della disciplina in esame: il reato di diffusione illecita di immagini o video sessualmente espliciti.

Infatti, anche se i dati suggeriscono il verificarsi di casi di *Revenge porn* anche a danno di uomini nella veste di persone offese (*Infra*, § cap. 2 parag. 4.2), questo tipo di illecito, come in generale quelli introdotti dal nuovo Codice Rosso, colpisce prevalentemente le donne²¹⁹.

La Riforma del processo penale, instaurata con legge n. 134/2021 ha esteso le tutele previste per le vittime di questo tipo di reati, mentre la legge n. 12 del 2023 ha previsto la costituzione di una Commissione bilaterale d'inchiesta su ogni tipo di violenza di genere.

Molti definirono l'entrata in vigore del Codice Rosso come frettolosa e sbrigativa, poiché non ha contemplato, a causa della necessità impellente di tutela e della quasi immediata cristallizzazione della legge, una previsione mirata alla riparazione in termini civilistici delle conseguenze che derivano dal reato.

Secondo molti, era anche necessaria una sistematica sensibilizzazione della società, mediante interventi volti a prevenire la messa in atto di questo reato.

Tuttavia, in conclusione è stato normato solamente l'assetto punitivo della condotta, non considerando misure di carattere preventivo²²⁰.

La legge n.69 del 2019 è stata modificata mediante la legge di recente introduzione, n. 122 del 2023, la quale istituisce un nuovo dovere di vigilanza del Procuratore della Repubblica e del Procuratore Generale in merito al rispetto del termine di tre giorni sull'assunzione delle informazioni dalle vittime.

Se il giudice designato per le indagini preliminari non rispetta il termine, c'è la possibilità da parte del Procuratore della Repubblica di revocargli l'assegnazione del procedimento e assumere immediatamente le informazioni che sono state omesse.

Tuttavia, questo compito viene designato dalla riforma come un potere, non un dovere del Pm, tenendo conto anche del fatto che, di norma è la polizia giudiziaria a occuparsi dell'ottenimento di informazioni e solo raramente il compito lo svolge il Pubblico ministero.

Obiettivo di questa Riforma è velocizzare le tempistiche di messa in atto delle disposizioni al suo interno, che a causa della tipologia di reati introdotti e della loro gravità, necessitano di tempi più ristretti, ma anche assicurare l'effettività dell'intervento del Pubblico Ministero per la tutela dei diritti.

²¹⁹ Report della direzione centrale di polizia criminale, consultabile online, le vittime sono prevalentemente donne, con un'incidenza del 73%; tra queste, l'82% risulta maggiorenne e l'87% è di nazionalità italiana: Ministero dell'Interno, Dipartimento della pubblica sicurezza, Il punto, cit., p. 27.

²²⁰ DOLCINI E., GATTA G.L., *Codice penale commentato*, V^a ed., Milano, 2021

Il Codice Rosso, tramite ventuno articoli, ha apportato varie modifiche al diritto penale sostanziale, processuale, penitenziario e ha introdotto misure in relazione alla giustizia riparativa.

1.1 (Segue): Modifiche e novità introdotte dalla riforma del Codice Rosso, dal punto di vista procedurale

Prima di procedere all'analisi del nuovo reato di diffusione illecita di immagini sessualmente esplicite portato finalmente a realtà dal Codice Rosso, ritengo opportuno effettuare una breve esplicazione riguardante le novità introdotte in relazione alla procedura²²¹.

Al fine di migliorare la tutela effettiva resa alla vittima (anche in previsione dell'articolo 6 e 13 della CEDU, rispettivamente il principio del giusto processo e il diritto a un ricorso effettivo, che prevedono, tra le altre cose, di evitare eccessive lungaggini del processo²²² e tenendo conto anche dei vari Considerando delle direttive Europee²²³) si è voluto dare carattere di celerità per l'avvio del procedimento di alcuni reati tra cui *stalking*, violenza sessuale e maltrattamenti in famiglia.

A livello procedurale la prima novità riguarda l'articolo 347 Cod. Proc. Pen, il quale nella formulazione indica: «Acquisita la notizia di reato, la polizia giudiziaria, senza ritardo, riferisce al pubblico ministero, per iscritto, gli elementi essenziali del fatto e gli altri elementi sino ad allora raccolti, indicando le fonti di prova e le attività compiute, delle quali trasmette la relativa documentazione.

Comunica, inoltre, quando è possibile, le generalità, il domicilio e quanto altro valga alla identificazione della persona nei cui confronti vengono svolte le indagini, della persona offesa e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti.

Qualora siano stati compiuti atti per i quali è prevista l'assistenza del difensore della persona nei cui confronti vengono svolte le indagini, la comunicazione della notizia di reato è trasmessa al più tardi entro quarantotto ore dal compimento dell'atto, salvo le disposizioni di legge che prevedono termini particolari.

Se si tratta di taluno dei delitti indicati nell'articolo 407, comma 2, lettera a), numeri da 1) a 6), del presente codice, o di uno dei delitti previsti dagli articoli 572, 609bis, 609

²²¹ VALSECCHI A., “Codice rosso” e diritto penale sostanziale: le principali novità, in *Diritto penale e processo*, 2022

²²² Secondo la Cedu, sez I, Talpis c. Italia, 2/03/2017 "Il semplice passare del tempo può nuocere alla inchiesta, ma anche compromettere definitivamente la possibilità che questa sia portata a termine"

²²³ Considerando n. 9 della direttiva 2012/29/UE, secondo cui «un reato è non solo un torto alla società, ma anche una violazione dei diritti individuali delle vittime». v. POGGI F., *Violenza di genere e Convenzione di Istanbul: un'analisi concettuale*, in *Diritti umani e diritto internazionale*, 2017, 1, pp. 68 ss.

ter, 609 quater, 609 quinquies, 609 octies, 612 bis e 612 ter del Codice Penale, ovvero dagli articoli 582, 683 quinquies del Codice Penale nelle ipotesi aggravate ai sensi degli articoli 6, primo comma, numeri 2, 5 e 5.1, e 577, primo comma, numero 1, e secondo comma, del medesimo Codice Penale, e, in ogni caso, quando sussistono ragioni di urgenza, la comunicazione della notizia di reato è data immediatamente anche in forma orale.

Alla comunicazione orale deve seguire senza ritardo quella scritta con le indicazioni e la documentazione previste dai commi 1 e 2. Con la comunicazione, la polizia giudiziaria indica il giorno e l'ora in cui ha acquisito la notizia».

Perciò, al comma terzo del suddetto articolo, è stato ampliato il catalogo dei reati per i quali è previsto che una volta che è stata acquisita la notizia di reato, la polizia giudiziaria informa, anche in forma orale, (precedentemente consentita solo per i reati di "particolare allarme sociale"²²⁴), il Pubblico Ministero.

Quest'ultimo, se ritenga di dover procedere per reati di violenza sulle donne, successivamente all'iscrizione della notizia di reato nel registro²²⁵, deve assumere informazioni entro tre giorni e avviare la procedura effettuata da parte della polizia giudiziaria dello svolgimento di atti di indagine, senza ritardo, dalla persona offesa dal reato oppure da chi ne ha denunciato il fatto.

Grazie all'articolo uno della presente legge, l'obbligo di riferire le notizie di reato anche oralmente è stato esteso a tutti i reati che vengono ricompresi nella violenza di genere, conseguentemente, anche per il reato di nuova introduzione, il *Revenge porn*.

Scendendo più nel dettaglio, il Pubblico Ministero dovrà ricevere comunicazione della notizia di reato in maniera immediata, da parte della polizia giudiziaria, in forma orale, prevedendone successivamente anche la forma scritta con indicazione delle informazioni necessarie all'identificazione della persona offesa ma anche del soggetto a cui sono destinate le indagini.

Ciò è stato previsto a fronte di una necessità di maggior speditezza delle indagini ma anche al fine di evitare che la vittima possa subire ulteriori ripercussioni sulla sua salute e sicurezza, considerando anche il fine, secondario, di valutazione da parte del Pubblico Ministero di emettere eventuali misure cautelari.

Dopo che sono passati tre giorni dall'iscrizione della notizia di reato, secondo il Codice Rosso, chi ha presentato la denuncia, querela o istanza, debba essere sentito dal Pubblico Ministero per l'assunzione di informazioni: ciò emerge dalla modifica all'articolo 362 cod. proc. pen., inserita nel comma 1ter.

Questa correzione si ritiene sia di particolare rilevanza poiché innanzitutto si riduce la possibilità di vittimizzazione della persona offesa, *in secundis* diminuisce ampiamente i tempi tra denuncia e vari provvedimenti necessari, previsti per l'aggiornamento sul

²²⁴ sono reati considerati molto gravi dal legislatore, elencati nel secondo comma dell'articolo 407 cpp lett a) n da 1 a 6

²²⁵ Anche se la riforma non si esprime esplicitamente su questa necessità, alcuni non ritengono che sia un potere discrezionale perché ciò "vanificherebbe la ratio dell'intervento legislativo" SORGATO, *"Revenge porn. Aspetti giuridici, informatici e psicologici"*, Milano, 2019

comportamento del soggetto agente, infatti, di solito le tempistiche arrivano fino ad un anno.

Tuttavia, il reato della diffusione illecita di immagini sessualmente esplicite non rientra nel novero legislativo delle discipline per il quale questa riduzione dei tempi è stata programmata: (tra cui per esempio la riservatezza delle immagini e la tutela di minori di anni diciotto) le motivazioni, non esplicitamente enunciate dal legislatore, secondo i giornali, risiedono nella volontà di non rendere eccessivamente gravosa l'attività che il Pubblico Ministero deve svolgere²²⁶.

Al pari di ciò è stata riformata anche la disciplina delle misure cautelari: soprattutto quello riguardante il divieto di avvicinamento della persona offesa, contenuto nell'art 282 ter del cod. di proc. pen., prevedendo l'introduzione di strumenti tecnici come, per esempio, il collaudato braccialetto elettronico, inizialmente ammesso dalla legge solo per gli arresti domiciliari.

L'utilizzo di quest'ultimo è quindi stato consentito anche per i reati agli articoli 600, bis, ter, quater, quinquies, octies, 612, 612bis.

Altra novità riguarda la sospensione condizionale della pena, istituto di recente modificato grazie alla Riforma Cartabia²²⁷, all'art 165 del cod.pen., per il quale si è concesso, in caso di commissione dei reati sopracitati, l'instaurazione di un percorso di recupero presso enti e associazioni per l'assistenza psicologica; tuttavia, la riforma ha escluso dal novero di questa norma la diffusione illecita di immagini di carattere sessuale.

Questa novità, secondo il legislatore è fondamentale, non solo dal punto di vista della repressione delle condotte criminali ma anche della prevenzione del reato.

La riforma ha contemplato l'introduzione di una più dura repressione a livello di pena inflitta, per i reati riguardanti la violenza di genere: per citarne alcuni, per il delitto di atti persecutori la pena prevista è da sei mesi a cinque anni di reclusione, per i reati di violenza sessuale, atti sessuali con minorenne, la cui pena è ulteriormente aumentata se la messa in atto di tali comportamenti avviene in cambio di denaro o altre utilità, anche solo promessi.

Anche per violenza sessuale di gruppo è stato introdotto un innalzamento di pena, sia nel minimo che nel massimo edittale (di almeno un anno).

Inoltre, tra gli altri cambiamenti apportati, al fine ultimo di incrementare il coordinamento tra istituti giudiziari e per ampliare l'esercizio dei diritti di difesa della persona offesa, ci sono maggiori obblighi di comunicazione alla vittima, al giudice civile e al difensore.

Questi devono riguardare: la cessazione della misura detentiva o cautelare e la scarcerazione; l'obiettivo infatti è quello di proteggere massimamente la vittima per una più rapida valutazione del rischio.

²²⁶ Camera, *"Revenge porn escluso dal codice rosso"*, Il Sole24ore, 22 luglio 2019

²²⁷ la sospensione condizionale della pena rientra tra le disposizioni immediatamente precettive, per i casi in cui la condanna abbia ad oggetto reati sessuali, di violenza domestica o di genere. v.d. MARINUCCI G., E. DOLCINI, G.L. GATTA, *Manuale di Diritto Penale*, XI ed., 2022

Con l'articolo tre della presente legge, su spinta internazionale, in base ai dettami della Convenzione di Istanbul contro la violenza di genere²²⁸, sono stati previsti altri due commi all'articolo 370 cod. proc. pen., che inseriscono l'obbligo della polizia giudiziaria di non indugiare e di procedere senza ritardo al compimento degli atti che il Pubblico Ministero gli delega, e di fornirne a quest'ultimo immediatamente la documentazione necessaria.

A sostegno di ciò, alcuni anni dopo è stata approvata dal Parlamento la Direttiva n. 29 dell'Unione Europea che inserisce norme minime riguardanti i diritti, la protezione della vittima in seguito al reato e l'assistenza a quest'ultima²²⁹.

Tale decreto riformò l'articolo 90 del cod. di proc. pen, elencando una serie di informazioni che l'autorità procedente, tramite il commissariato, deve fornire alla vittima mediante un linguaggio che sia a lui comprensibile e chiaro, anche in forma scritta.

Queste informative riguardano il ruolo che la persona offesa assumerà durante il processo, il diritto di venire a conoscenza della data e del luogo del processo e la relativa imputazione, il diritto di costituirsi parte civile e di ricevere notifica della sentenza, la facoltà di avvalersi del patrocinio dello Stato, diritto all'interpretazione degli atti e alla loro traduzione, le misure di protezione di cui potrebbe avvalersi.

La vittima deve essere informata sulle autorità alle quali rivolgersi in merito all'andamento della causa, la facoltà di richiedere risarcimento danni, di richiedere remissione della querela, di conoscere le strutture sanitarie presenti nel luogo ove si trovi.

Può richiedere dove si trovano case-famiglia o centri antiviolenza e la comunicazione, come anticipato in precedenza mediante introduzione del Codice Rosso del comma 1bis al presente articolo, dei provvedimenti di scarcerazione o di cessazione della misura di sicurezza, del divieto di avvicinamento ai luoghi frequentati dalla persona offesa, di revoca o sostituzione di misure coercitive o interdittive o anche di evasione del soggetto sottoposto a indagini.

Queste ultime erano, in via generale, previste solamente su richiesta della persona offesa dal reato, mentre ora, a prescindere dalla volontà della vittima per reati di genere come violenza sessuale, maltrattamenti ecc., sono dovute lo stesso.

Queste informazioni in particolare vengono comunicate sia alla vittima ma anche al difensore che è stato nominato²³⁰.

²²⁸ La Convenzione sulla prevenzione e la lotta alla violenza contro le donne e la violenza domestica – nota come ‘Convenzione di Istanbul’ – adottata dal Consiglio d’Europa, l’11 maggio 2011, è entrata in vigore il 1° agosto 2014. La Convenzione è formata da un Preambolo, di 81 articoli. L’Italia ha ratificato la convenzione con la legge 27 giugno 2013, n. 77. La Convenzione è il primo strumento internazionale considerato vincolante a livello legislativo che si pone come fine quello di definire un quadro normativo a tutela delle donne contro qualsiasi forma di violenza, considerata una violazione dei diritti umani previsti dalla Corte Europea dei Diritti dell’Uomo.

²²⁹ d.lgs. n. 212 entrato in vigore nel 2016

²³⁰ FIANDACA G., MUSCO E., *Diritto penale: parte speciale. I diritti contro la persona*, Vol. II, tomo primo, V ed., 2020

Fra questa lista di reati, è stato escluso il reato all'art 612 ter).

Altra novità è anche il concetto di estensione della "condizione di particolare vulnerabilità"²³¹ regolata dall'articolo 90 del cod. di proc. pen, che si riferisce sia all'età e lo stato di salute psichica, ma anche dal tipo di reato e le modalità di attuazione di quest'ultimo (tenendo in considerazione, per esempio, l'avvenuta violenza o discriminazione o odio razziale²³²) prendendo in esame anche la situazione economica, se la vittima dipende dall'autore del reato.

Può essere chiamato un esperto psicologo o psichiatra che aiuti l'ufficiale di Polizia Giudiziaria nell'interrogare la vittima, e addirittura in casi di estrema necessità si può anche richiedere che la testimonianza della vittima avvenga mediante incidente probatorio, in stanze particolarmente protette, facendo in modo che la persona offesa parli con il giudice, anche durante il dibattimento, e con l'esperto psicologo filtrando le domande, evitando eventuali contatti con l'imputato.

Tuttavia, quest'ultima possibilità è prevista solamente per i reati di maltrattamenti, violenza sessuale, atti persecutori, pedopornografia, non anche per la nuova introduzione del reato di *Revenge porn*.

L'articolo cinque della presente legge ha anche introdotto delle norme che richiedono l'organizzazione, entro dodici mesi, di corsi di formazione relativi a chi esercita un trattamento penitenziario sulla persona condannata, presso la Polizia di Stato, l'Arma dei Carabinieri e il Corpo di Polizia Penitenziaria, in questa disciplina invece viene ricompreso anche il reato di *Revenge porn*.

Si muta anche l'articolo 275 comma 2 bis cod. proc.pen, introducendo il reato all'articolo 612ter, nella lista di quelli per cui il giudice, anche se ha ammesso con sentenza la sospensione condizionale della pena, consente la possibilità di ottenere anche degli arresti domiciliari e la custodia cautelare in carcere.

Secondo una sentenza del 2012, il divieto di applicazione di queste ultime era riferito alle misure di permanenza in casa e di collocamento in comunità, per quanto riguarda il procedimento minorile²³³.

Quindi, per analogia, si arriva alla conclusione che per il reato di diffusione illecita di immagini a sfondo sessuale non si applicava la normativa generale che prevede l'applicazione della misura di custodia cautelare in carcere o arresti domiciliari.

Per l'indagato che potrà disporre della sospensione condizionale, inoltre, non deve essere condotto in carcere se per lui potranno essere disposte misure alternative²³⁴.

²³¹ l'espressione "di particolare vulnerabilità" compare anche a livello europeo nella Raccomandazione R (2006)8 del Consiglio D'Europa, punto 3.4. Per un approfondimento maggiore su questa condizione, si guardi anche VENTUROLI "la vulnerabilità della vittima di reato quale categoria 'a geometria variabile' del diritto penale" in Riv. it. medicina legale 2018,2, 553.

²³² con il decreto legislativo n. 212/2016 il Codice penale è stato integrato di specifiche disposizioni: il diritto della vittima di ricevere informazioni riguardanti il procedimento penale e l'eventuale scarcerazione, e l'istituzione di alcune tutele per la persona affetta da questa condizione di vulnerabilità

²³³ Cass. Pen. Sez. II, 29 novembre 2012 n 48738

²³⁴ Corte di Appello di Roma sez. III 4 luglio 2014

Si dispone anche che, per i reati con violenza di genere, la sospensione condizionale può essere applicata solo se il soggetto venga ammesso a presenziare, grazie ad autorizzazione del Giudice civile, presso specifici percorsi che possano aiutarlo al recupero psicologico, tramite enti e associazioni predisposti a tale fine.

Il Giudice civile si occupa anche, secondo l'articolo 64 bis disp. Att. cod. proc. pen., sempre in attuazione del Codice Rosso, delle ordinanze applicative di misure cautelari personali, le quali devono essere trasmesse senza ritardo a quest'ultimo (compreso il provvedimento di archiviazione).

In ciò viene ricompreso anche il reato all'articolo 612 ter, mentre, antecedentemente alla riforma, questa connessione fra i vari Giudici era consentita solo per i reati di violenza articoli 600, bis, ter, *quinquies*, 609, 612, 572 ecc. al fine di assicurare una maggior tutela e speditezza per i procedimenti riguardanti violenza domestica, prevalentemente su soggetti di minore età.

Per cui, questa estensione introdotta dalla riforma, dovrebbe, *sic et simpliciter*, aiutare i casi di necessario coordinamento fra procedimento penale e civile.

Per quanto concerne le modifiche al Codice penale, sono state immesse anche nuove figure di reato, a causa della necessità riscontrata nella prassi giurisprudenziale di rimediare a vuoti di tutela.

Per completezza, descrivo in breve anche gli altri articoli aggiunti dalla riforma del Codice Rosso: è stato incluso l'articolo 387 bis «Violazione dei provvedimenti di allontanamento dalla casa familiare e del divieto di avvicinamento ai luoghi frequentati dalla persona offesa», introducendo una nuova criminalizzazione per coloro che violano gli obblighi o i divieti previsti mediante la disposizione delle misure cautelari oggetto della normativa, con l'obiettivo di evitare che la vittima si senta turbata dal contatto con il reo.

In precedenza, ciò era possibile solamente per la violazione della custodia cautelare in carcere e agli arresti domiciliari e la violazione della norma sull'evasione.

È stata aggiunta anche la fattispecie di "costrizione o induzione al matrimonio" nell'articolo 558 bis cod. proc. pen., a causa della spinta sovranazionale, della convenzione di Istanbul, che nell'articolo 37, induceva gli Stati firmatari a punire penalmente le condotte di costrizione di un adulto o un minore a contrarre matrimonio. Altre norme che il legislatore ha voluto immettere nel c.p. sono state: in *primis* il reato all'articolo 583 *quinquies* in merito alla deformazione dell'aspetto della persona mediante lesioni permanenti al viso, per il quale la Giurisprudenza di legittimità ha precisato il significato di "deformazione": lo sfregio permanente o una alterazione del viso che determini nell'osservatore ripugnanza o ribrezzo²³⁵.

Questa introduzione trova le sue ragioni nella situazione di allarme sociale che ha avuto una evidente crescita in seguito alla quantità di donne che sono state sfregiate con l'acido, come ulteriore "vendetta" posta in essere dall'autore del reato.

²³⁵ Cass. Pen. n 21394/2016 sez. V; Cass. Pen sez. V n 27564/2020

Infine, sono state aggiunte delle modifiche agli articoli 572 e 612 bis cp inasprendo il trattamento sanzionatorio rispettivamente prima da due a sei anni, a tre a sette anni per maltrattamenti, da sei mesi a cinque anni a un anno fino a sei anni e sei mesi per atti persecutori, e inserendo una circostanza aggravante per danno a un minore o uso di armi.

Soggetti a modifica sono stati anche gli articoli 609 bis, ter, quater, septies, octies, aumentandone le pene e il termine per proporre la querela; sono state altresì aggiunte circostanze aggravanti: se la violenza è attuata da un ascendente o da genitore o tutore, o a danno di un minore, graduando la pena in base alla fascia di età²³⁶.

2.0 (segue): L'articolo 612ter, Il delitto di diffusione illecita di immagini o video sessualmente espliciti

Il legislatore, tra le altre fattispecie introdotte, per l'aumento di casi di persone, in via generale maggiormente donne, che sono state vittima di diffusione di immagini intime senza la loro approvazione, ha sentito la necessità di criminalizzare questa condotta che ha preso sempre più piede nel nostro paese, decidendo quindi di introdurre l'articolo 612 ter Codice penale²³⁷ tramite l'articolo n. 10 della legge 69/2019²³⁸.

Il Presidente dell'Osservatorio *Cyber Security* dell'Eurispes ha dichiarato, in merito alla diffusione a macchia d'olio di questo fenomeno: «il rischio è di una esposizione generalizzata: nessuno è escluso, dagli adolescenti fino ai rappresentanti delle Istituzioni, passando per personalità pubbliche e per cittadini comuni»²³⁹.

Per questo, si è sentito il bisogno di introdurre una fattispecie *ad hoc* che regolasse il fenomeno, tramite l'articolo 612 ter, che recita quanto segue:

«Salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è punito con la reclusione da uno a sei anni e con multa da euro 5.000 a euro 15.000.

La stessa pena si applica a chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocumento.

²³⁶ per ulteriori dettagli sulle modifiche consultare l'articolo 13 della legge 69/2019

²³⁷ è stato inserito nell'Allegato A riferito al C-1455 della seduta in Assemblea del 2 aprile 2019.

²³⁸ BIANCHI M., *L'incriminazione del "revenge porn": il nuovo delitto di "diffusione illecita di immagini o video sessualmente espliciti"*, in *Diritto penale*, Tomo III, *I delitti contro la libertà morale*, A. CADOPPI, S. CANESTRARI, A. MANNA, M. Papa (a cura di), Torino, UTET, 2022

²³⁹ Dichiarazioni del 18 dicembre 2019, Presidente dell'Eurispes, istituto di ricerca privata in temi di politica, economia e sociale dal 1982, consultabile sul sito ufficiale

La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici.

La pena è aumentata da un terzo alla metà se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza.

Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. La remissione della querela può essere soltanto processuale.

Si procede tuttavia d'ufficio nei casi di cui al quarto comma, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio²⁴⁰».

Questo reato si colloca nella sezione del Codice penale dedicata ai reati contro la libertà morale, sezione III, nel Titolo XII dei delitti contro la persona, capo III dei delitti contro la libertà individuale: la volontà del legislatore di inserirlo in questa sezione del Codice è da ritrovarsi nel carattere di continuità che accomuna questa fattispecie con quelle precedenti, per esempio con gli atti persecutori articolo 612 bis.

Inoltre, parte della Dottrina sottolinea la consapevolezza del legislatore della capacità di questo delitto di provocare un grave danno nella vita della vittima, per questo, si giustificerebbe la collocazione tra i delitti della libertà morale²⁴¹.

Il legislatore ha preferito dunque, questa collocazione, rispetto alla proposta iniziale di porre questa disciplina all'interno del Codice della Privacy²⁴².

Alternativamente, L'Unione Camere Penali Italiane (UCPI) aveva portato alla Camera, in sede di discussione di entrata in vigore del Codice Rosso, la proposta di creare un titolo a parte sui delitti che ledono la libertà sessuale²⁴³, ma non è stata presa in considerazione.

Questa disciplina di recente introduzione, per il principio di irretroattività della norma penale, previsto dall'articolo 25 della Costituzione (costituente uno dei corollari del principio di legalità) non può trovare applicazione se il fatto venga commesso prima dell'entrata in vigore della suddetta, in quanto, quei comportamenti tenuti, non potevano essere puniti secondo questa disciplina.

Mettendo in luce alcuni dati, tuttavia, si può vedere che dal momento in cui questo reato è stato introdotto, come definisce il report della Direzione centrale della Polizia

²⁴⁰ BIANCHI M., *L'incriminazione del "revenge porn": il nuovo delitto di "diffusione illecita di immagini o video sessualmente espliciti"*, in *Diritto penale*, Tomo III, *I delitti contro la libertà morale*, A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), Torino, UTET, 2022.; G.M. CALETTI, *Libertà e riservatezza sessuale all'epoca di Internet. L'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale*, in *Rivista italiana di diritto procedura penale*, 2019

²⁴¹ PADOVANI T., *L'assenza di coerenza mette a rischio la tenuta del sistema*, in *Guida dir.*, 2019, f. 37, pp. 51-55

²⁴² CALETTI G.M. *L'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale*, in *Rivista italiana di diritto procedura penale*, 2019; contrario alla collocazione del Revenge porn è SEMINARA S., *Codice penale, riserva di codice e riforma dei delitti contro la persona*, in *Rivista italiana di diritto e procedura penale*, 2020

²⁴³ testo completo disponibile sul sito senato.it

criminale, pubblicato dal Dipartimento della Pubblica Sicurezza del Ministero dell'Interno il 25 novembre 2021, in occasione della Giornata Internazionale per l'eliminazione della violenza contro le donne, è emerso un incremento di casi verificatisi, pari al 45 % rispetto all'anno precedente.

Il monitoraggio ha riguardato, per entrambi gli anni, l'arco temporale di gennaio-ottobre.

È interessante notare che la diffusione del fenomeno prescinde dall'area geografica: difatti il maggior numero di reati, in valori assoluti, è stato registrato in Lombardia, Campania e Sicilia, mentre le regioni meno interessate sono state la Valle d'Aosta, il Molise e la Basilicata²⁴⁴.

La normativa appare "neutra", senza specificare un genere in particolare, poiché altrimenti verrebbe meno il rispetto del "principio di non discriminazione"²⁴⁵ tutelato dall'articolo 3 della Costituzione e 21 della Carta dei Diritti Fondamentali dell'Unione Europea.

Questo principio pone le sue fondamenta sul fatto che è necessario assicurare una adeguata tutela e pari opportunità, senza distinzioni di genere, razza, religione ecc. in quanto la disciplina prevista in materia di violenza di genere non può essere solo riferita alle donne, ma è una violenza di carattere generale basata sul sesso²⁴⁶.

Infatti, anche l'OMS definisce la violenza domestica come il "comportamento abusante di uno o entrambi i compagni in una relazione intima", senza alcun riferimento al genere.

La Dottrina vuole comunque sottolineare l'inadeguatezza della fattispecie a porre rimedio ad una problematica ben radicata nel nostro sistema: la diffusione di immagini a sfondo sessuale senza il consenso della persona offesa.

Secondo gli esperti, questa deve essere valutata attentamente anche a fronte dei casi giurisprudenziali sempre più in crescita.

²⁴⁴ Ministero dell'Interno, Dipartimento della pubblica sicurezza, Il punto. La violenza contro le donne, 25 novembre 2021, Giornata Internazionale per l'eliminazione della violenza contro le donne, pp. 24 ss.; il report è consultabile nel sito ufficiale del governo.

²⁴⁵ Regolato dall'articolo 3 della Costituzione, a livello Europeo, Art. 2,3 TUE. Per l'articolo 157 TFUE, per le pari opportunità tra uomini e donne, non si decide secondo l'unanimità ma la maggioranza qualificata. Il trattato di Amsterdam ha ampliato la base giuridica dell'articolo 12 TCE con altre fattispecie discriminatorie. La Corte di Giustizia Europea ha precisato «il principio generale d'uguaglianza, di cui il divieto di discriminazione a motivo della cittadinanza è solo un'espressione specifica, è uno dei principi fondamentali del diritto comunitario. Questo principio impone di non trattare in modo diverso situazioni analoghe, salvo che la differenza di trattamento sia obiettivamente giustificata» sent. *Überschar*, 8 ottobre 1980, causa 810/79, *ivi*, p. 2747 e ss.

²⁴⁶ Da una ricerca ISTAT del 2018, in Italia nel 2015/2016, tre milioni di uomini hanno subito abusi sessuali, numero inferiore rispetto alle donne ma in ogni caso alto. A Catania nel 2013 è stata istituita l'Associazione Violenza sugli Uomini (AVU). Cass. Pen. n. 29577/21: la cassazione ha ritenuto integrato il reato di violenza nei confronti della p.o. Che ha subito atti di valenza sessuale da una donna, senza che quest'ultimo ricercasse il contatto fisico.

2.1 (Segue): La clausola di salvaguardia e il concorso con altri reati

Partendo la nostra analisi dal comma primo dell'articolo 612ter, questo si apre con una clausola di salvaguardia - salvo che il fatto costituisca più grave reato -, principio contenuto anche nella fattispecie degli atti persecutori all'articolo 612 bis²⁴⁷.

Secondo questa clausola, ad applicazione sussidiaria, nel caso di dubbio tra più fattispecie che astrattamente possono essere applicate, rientranti tutte nella medesima sottospecie comune di reato, la disposizione che il legislatore applicherà fra queste sarà quella che ritiene più grave.

Perciò potrebbe venire ad esistenza il fenomeno di concorso apparente di norme; infatti, l'articolo 15 del c.p. sancisce che «Quando più leggi penali o più disposizioni della medesima legge penale regolano la stessa materia, la legge o la disposizione di legge speciale deroga alla legge o alla disposizione di legge generale, salvo che sia altrimenti stabilito».

Tale questione prevede quindi l'applicazione della norma principale, cioè quella che tutela più interessi rispetto a quella sussidiaria.

Pertanto, il reato di diffusione illecita di immagini a sfondo sessuale verrà meno nel caso in cui ci sia un concorso con una fattispecie ritenuta più grave dal legislatore e in quest'ultima verrà assorbita.

Si consideri, astrattamente, la possibilità che possa avvenire un assorbimento tra il reato di estorsione e quello di *Revenge porn*, considerando la prima fattispecie come più grave, in quanto prevede una pena maggiore.

Ciò si potrebbe verificare in caso di "*sex extortion*", nel caso in cui prima ci sia la minaccia di diffusione e poi l'effettiva divulgazione.

Tuttavia, se la divulgazione non avviene, l'assorbimento non può verificarsi, perché con la sola minaccia, non si violerebbe l'articolo 612ter.

Considerando l'ipotesi in cui l'assorbimento non abbia ad oggetto gli stessi interessi giuridici protetti, ma ci sia una eterogeneità giuridica, si potrà verificare un concorso di tipo formale tra le due norme: si applicheranno quindi entrambe le fattispecie per i quali i reati vengono puniti, anche se si tratta di una sola azione od omissione e per il quale si potrebbe riconoscere l'appartenenza a uno stesso disegno criminoso (e quindi risulterebbe applicabile la continuazione ex art 81 cpv Codice penale²⁴⁸).

Ciò è consentito in quanto la stessa letteralità di questo principio fa riferimento non alla omogeneità della fattispecie tutelata ma a un *quantum* edittale di pena.

Infatti, il legislatore dovrà fare un vero e proprio confronto fra le fattispecie che sono legate da un rapporto di specialità²⁴⁹.

²⁴⁷ Cass. Pen. sez III 14 Novembre 2017 n 14707 in CED Cass Pen rv 239659

²⁴⁸ Cass. Pen., Sez. Un., 28 febbraio 2013 (dep. 13 giugno 2013), n. 25939, Pres. Lupo, Est. Cassano, Imp. C.

²⁴⁹ su questo principio vd. TRAPANI M., *La divergenza tra il voluto e il realizzato*, 2006, cit., spec. 258-260.

Il principio di concorso formale, cioè la continuazione fra reati, viene spesso riconosciuta, tra l'articolo 612 ter e la normativa che disciplina l'accesso abusivo a sistema informatico, articolo 615 ter: nel caso in cui il materiale venga preso da un sistema al quale il soggetto attivo non avesse l'autorizzazione ad accedervi, oppure, molto di frequente, potrebbe concorrervi la commissione di violenza sessuale.

Il concorso formale può avvenire anche fra la disciplina di Atti persecutori e la Diffusione di immagini sessualmente esplicite, perché si tratta rispettivamente di un reato abituale, che quindi consta di condotte reiterate, e di un reato istantaneo di mera condotta.

Secondo parte della dottrina l'articolo 612ter non può coprire l'intera offensività della disciplina degli atti persecutori, mentre altra dottrina ritiene che questo reato possa essere assorbito dall'articolo 612 bis poiché viene considerato sussumibile nel concetto più ampio, di molestia, comune a entrambe le fattispecie, e più in generale ai reati di tipo sessuale²⁵⁰.

Invece, secondo un orientamento Giurisprudenziale, il concorso formale potrebbe essere escluso se il reato di minore gravità venisse assorbito nell'altro sotto forma di circostanza aggravante²⁵¹.

2.2 (Segue): La pluralità di condotte incriminate nell'articolo di diffusione illecita di immagini sessualmente esplicite

Come si evince dal testo letterale della norma, il comma uno dell'articolo 612 ter punisce "chiunque" realizzi le condotte penalmente rilevanti: per questo, viene definito come un reato comune, mono-soggettivo per il quale cioè, è sufficiente l'attuazione da parte di una sola persona ai fini della configurabilità del reato.

Il soggetto attivo è dunque colui che dopo aver realizzato o sottratto il materiale, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito: a differenza dal comma successivo quindi, qui si definisce l'autore della condotta come un "distributore primario" del materiale.

Il legislatore, con la specificazione delle condotte "presupposto", cioè quelle che portano al compimento dell'azione illecita, ha voluto sottolineare, utilizzando i termini "realizzato" e "sottratto", che ci potrebbero essere ipotesi per cui si verifichi la non coincidenza tra il soggetto attivo che realizza il reato e l'autore materiale del contenuto. Infatti per capire bene la disciplina bisogna effettuare una digressione di tipo semantico: nel dizionario italiano realizzare significa far divenire realtà; nel linguaggio

²⁵⁰ In questo senso VIGANO' F., *Il delitto di atti persecutori (art. 612-bis c.p.)*, in *I delitti contro la persona. Libertà personale, sessuale e morale. Domicilio e segreti*, a cura di C. Piergallini, F. Viganò, M. Vizzardi, A. Veri, in *Trattato di diritto penale. Parte speciale*, diretto da G. Marinucci, E. Dolcini, Cedam, 2015, 664, *contra* per tutti v. CAPUTO M., *Eventi e sentimenti nel delitto di Atti persecutori*, in *Studi in onore di Mario Romano*, a cura di M. Bartolino, L. Eusebi, G. Forti, vol. III, Jovene, 2011

²⁵¹ Cass. Pen. Sez I n 12680/2008 in Cass. Pen. 2009,1,200

giuridico, più precisamente, si fa riferimento a una rappresentazione di un caso concreto di una ipotesi di reato.

Tuttavia, il legislatore utilizza questo termine volontariamente non tecnico, con l'intento di ricomprendere nella condotta *sic* la produzione lecita del materiale, mediante il libero intento di fotografarsi (riferendosi anche al dibattito in materia di *selfie* in relazione al fenomeno del *sexting*) *sic* la produzione illecita e fraudolenta, tramite la creazione di materiale pornografico all'insaputa della persona offesa e la sua successiva diffusione.

Si richiama, per maggiore chiarezza, la definizione di fotografia data dal diritto d'autore: all'articolo 87 la definisce come «una immagine di persone o aspetti, elementi o fatti della vita naturale e sociale, ottenute col processo fotografico o con processo analogo, comprese le riproduzioni di opere d'arte figurativa e i fotogrammi delle pellicole cinematografiche²⁵²».

Questa definizione viene considerata ancora del tutto attuale grazie alla precisazione "processi analoghi" per il quale vengono ricomprese anche le fotografie digitali.

Tornando alla norma, "sottrarre" indica ogni condotta che mira a togliere dalla disponibilità del soggetto passivo l'immagine, con l'astuzia e senza il consenso di quest'ultimo, andando così a ricomprendere il dolo specifico, oggetto del secondo comma dell'articolo 612ter.

Secondo parte della Dottrina, appare alquanto contraddittorio il fatto che le due condotte siano connotate da un determinato disvalore nel primo comma, mentre nel secondo, non ci sia distinzione in merito alla condotta diffusiva o al trattamento sanzionatorio, che rimangono invariati: sia dal punto di vista della realizzazione che per la sottrazione del materiale da parte del reo²⁵³.

Di conseguenza, per il secondo comma è necessario che il soggetto attivo, una volta ricevuto il materiale, lo divulghi al fine di recare un nocumento ai soggetti cui il contenuto dell'immagine o video si riferisce.

Si è voluto sottolineare la mancanza di accettazione alla divulgazione/creazione del contenuto da parte della vittima, non solo tramite l'utilizzo del verbo "sottrarre", ma anche usando espressamente la locuzione "senza il consenso delle persone rappresentate" alla creazione dell'immagine o del video, previsto dallo stesso comma primo, poche righe più avanti.

Il legislatore, ponendolo in una accezione positiva come "assenza di consenso"²⁵⁴ e non come dissenso, tramite la letteralità dell'articolo 612 ter, vuole effettuare un riferimento

²⁵² Per un maggiore approfondimento in tema, MONTALDO, "il ritratto fotografico digitale tra diritto d'autore, diritti della persona, e tutela della privacy" in resp. civ. prev. 2010, 11, 2369B s.

²⁵³ LO MONTE E., *L'art. 612-ter C.P.*, cit., p. 122

²⁵⁴ Nel nostro ordinamento, un esempio di questa inversione terminologica è l'art. 1 della l. n. 219 del 2017, a norma del quale «nessun trattamento sanitario può essere iniziato o proseguito se privo del consenso libero e informato della persona interessata». S. CANESTRARI, *Una buona legge buona (DDL recante «norme in materia di consenso informato e di disposizioni anticipate di trattamento»)*, in Riv. it. med. leg., 2017, 975.

alla fattispecie normativa presente negli Stati Uniti (*infra*, cap. 2 parag. 3.1) nel quale si usa il paradigma dell'"affirmative consent"²⁵⁵.

La condotta sottrattiva²⁵⁶ viene ripresa anche in altri reati, tra cui il furto (articolo 624 c.p.), estorsione (articolo 629 c.p.), interferenze illecite nella vita privata (art 615 bis c.p.) e appropriazione indebita (art 646 c.p.).

La norma in esame, al primo comma, definisce il verificarsi dell'azione illecita mediante una lista ampia di condotte, alcune delle quali già analizzate: per la configurazione del reato basta porre in essere anche solo una di queste per definire integrata la condotta di diffusione illecita di immagini sessualmente esplicite.

Sul piano applicativo, tuttavia, queste vengono diversificate: sebbene alcune *a prima face* possano coincidere, il legislatore ha utilizzato la locuzione "o", per questo motivo si ritiene che quest'ultimo abbia voluto lasciare all'interprete la possibilità di definire caso per caso le condotte in base alla situazione a cui si riferisce.

Secondo Padovani²⁵⁷ la fattispecie è stata divisa in due macro-gruppi: la consegna-invio-cessione e la diffusione-pubblicazione.

Con questa classificazione, come vedremo per il comma secondo del presente articolo, si mette in luce la diversa destinazione del contenuto illecito.

Tuttavia, secondo parte della Dottrina, l'elenco di comportamenti non sarebbe tassativo, in quanto, sebbene le condotte descritte siano molte, non si riesce a ricomprendere interamente ogni ipotesi lesiva verso la vittima, per esempio non viene considerato il solo mostrare la foto ad altri, oppure l'estrarne una copia²⁵⁸.

Secondo la Cassazione però, l'estrazione di una copia non rientra nella condotta sottrattiva, anche se la copiatura non è autorizzata²⁵⁹, al contempo, si ritiene che, far vedere l'immagine ad un'altra persona, senza inviarla, ma solo mostrandola, non rientra nella fattispecie in esame, considerando che il soggetto può controllarne la portata diffusiva.

Mentre, secondo altri, la disciplina in questione dovrebbe esser resa più snella, ricomprendendo solamente le condotte di diffusione e rivelazione²⁶⁰.

²⁵⁵ SCHULOFHER SJ, *Consent: What It Means and Why It's Time to Require It*, in *University of the Pacific Law Review*, 2016, 665 ss. Si prevede infatti la definizione di "rape" come «*sexual penetration without consent*», riecheggiante l'articolo 612-ter c.p.

²⁵⁶ AMORE N., *La tutela penale della riservatezza sessuale nella società digitale*, 2020, cit., p. 36 s., propone, sperando in una riforma da parte del legislatore, di modificare l'articolo 612 ter prevedendo anziché la condotta di sottrazione, la sostituzione col termine appropriazione; inoltre, secondo A., sia la formazione che l'appropriazione del materiale oggetto della condotta debba essere punito a sé, indipendentemente dalla successiva diffusione

²⁵⁷ PADOVANI, "l'assenza di coerenza mette a rischio la tenuta del sistema" in *Guida al diritto* 2019, 37, 54

²⁵⁸ PITTARO P., *Il c.d. "Codice rosso" sulla tutela delle vittime di violenza domestica e di genere*, cit., p. 738

²⁵⁹ Cass. Pen., IV sez., 13 novembre 2003, n. 3449

²⁶⁰ LO MONTE E., *L'art 612 ter c.p.*, cit. Pag. 166

Il primo gruppo di condotte presuppone l'esistenza di un rapporto diretto con i destinatari (quindi si sottolinea la loro determinatezza, includendo anche la possibilità che l'invio avvenga da parte di una sola persona²⁶¹), mentre il secondo, allude a una potenziale indeterminatezza degli individui a cui il contenuto potrebbe essere destinato. L'invio ha come destinatario un solo soggetto, e ha una definizione molto simile alla cessione; infatti, anche in questo caso avrà una portata diffusiva bassa, quest'ultima viene delineata come la condotta con cui il soggetto attivo trasferisce materiale pornografico nella sfera della disponibilità della persona.

Molte volte, la Dottrina fa un paragone con la cessione prevista nella norma 600 ter del c.p., comma quarto, in riferimento alla cessione di materiale pedopornografico, qui la cessione può avvenire anche in maniera gratuita e ha carattere residuale, a differenza dell'articolo 612ter²⁶².

La Giurisprudenza di legittimità, in una sentenza, precisa in merito a questo tipo di condotta, che se i file destinati ad essere inviati non sono ancora stati visionati dal moderatore di un gruppo di discussione o "newsgroup", e vengono indirizzati a server "nttp" (*network transport protocol*, servizio che serve per poter leggere i *file* in questi gruppi), ciò non rientra nella cosiddetta "connessione privata".

Questa considerazione si basa sul fatto che l'immagine ricade nella disponibilità di un numero indefinito di utenti, non dando importanza alla presenza del moderatore, che potrebbe essere punibile a titolo di concorso²⁶³.

Leggermente più ampia invece è la portata diffusiva della "consegna", sebbene non possa essere ritenuta alla stregua delle altre due condotte di diffusione e pubblicazione, che ambiscono a un numero ancora più elevato di destinatari.

Infatti, il termine potrebbe indicare sia la consegna ad un singolo individuo ma anche a un gruppo con un numero determinato di persone che ne fanno parte.

Questa parola viene utilizzata sia per descrivere l'atto di inviare il contenuto illecito mediante mezzi informatici, come un gruppo ristretto su *whatsapp* o *Facebook* (sebbene su queste piattaforme, è possibile che il gruppo sia ristretto, l'immagine potrebbe potenzialmente avere portata più ampia a causa della possibilità degli utenti di scaricare il contenuto a loro volta) ma anche per descrivere una effettiva consegna *brevi manu*, e quindi materiale del contenuto.

Proseguendo con l'analisi delle condotte, la norma si riferisce alla "diffusione" e "pubblicazione".

²⁶¹ Cfr. DOVA M., *sub Art. 612-ter*, in *Codice penale commentato*, E. Dolcini, G.L. Gatta (diretto da), Tomo III, *Artt. 452bis-649bis*, V ed., Milano, Wolters Kluwer, 2021, p. 1941; VALSECCHI A., "Codice rosso" e diritto penale sostanziale, 2020 cit., p. 170.

²⁶² Cass. Pen sez. III n 1647/2018 in *Dir & Giustizia*. 2019 16 gennaio, qui si prevede la configurazione del reato all'articolo 600 ter comma 4 c.p., perché il soggetto attivo ha inviato materiale pedopornografico utilizzando il profilo *Facebook* del destinatario, facendo sì che queste rientrassero solamente nella disponibilità di quest'ultimo.

²⁶³ Cass. Pen sez. III n. 30564/2011 in CED Rv. 251260

Queste ultime sembrano all'apparenza assumere la stessa connotazione, tuttavia distinta è la destinazione del contenuto.

Infatti, mentre la diffusione viene considerata dalla maggior parte degli studiosi come una condotta destinata ad essere indirizzata a terzi, ma in numero molto più ridotto (per esempio mediante invio del contenuto in una chat di messaggistica privata), la pubblicazione invece sarebbe un metodo di divulgazione che fa sì che il contenuto sia destinato a un numero potenzialmente indefinito di soggetti.

In quest'ultima ipotesi viene ricompreso nella fattispecie il caso della divulgazione mediante *social network*, che viene definita "*one to many*".

Considerando poi che una volta che il contenuto è stato pubblicato online, è molto difficile eliminarlo totalmente, a causa della possibilità degli utenti di poter scaricare il contenuto e pubblicarlo a loro volta, creando una catena potenzialmente infinita di condivisioni.

2.3 (Segue): L'oggetto della condotta dell'articolo 612ter - cosa si intende per 'immagini a contenuto sessualmente esplicito?'

L'articolo 612ter parla di "immagini o video a contenuto sessualmente esplicito".

Si tratta di una evidente novità nel diritto penale italiano, essendo un concetto presente solamente nella disposizione riguardante la pornografia minorile.

Questa definizione però non ha suscitato pochi dubbi interpretativi nella Giurisprudenza²⁶⁴ a causa della sua vaghezza ma anche della possibile ampiezza della fattispecie, che potrebbe porsi in un'ottica di contrasto con il principio di determinatezza della legge penale²⁶⁵ (articolo uno Codice penale, quattordici delle preleggi, e articolo venticinque, comma due della Costituzione).

Tuttavia, non sarebbe stato meglio definire la disciplina come diffusione "pornografica", in quanto presupporrebbe uno scopo sessuale della rappresentazione, che non sempre è presente.

²⁶⁴ ROMANO V.B., *L'introduzione dell'articolo 612-ter del Codice penale in materia di diffusione illecita di immagini o video sessualmente espliciti* (art. 10, l. 19 luglio 2019, n. 69), in Codice Rosso. Commento alla L. 19 luglio 2019, n. 69, in materia di tutela delle vittime di violenza domestica e di genere, B. Romano, A. Marandola (a cura di), Pisa, Pacini Giuridica, 2020, p. 107; E. LO MONTE, *L'art. 612-ter C.P.*, cit., pp. 99 ss. Il difetto di precisione, già segnalato dall'Unione delle Camere penali nell'audizione in Commissione Giustizia (v. Unione Camere Penali, Audizione Commissione Giustizia del Senato 11.6.2019, cit., p. 2), è stato successivamente rimarcato dall'Ufficio del Massimario e del Ruolo della Corte Suprema di Cassazione: v. la Relazione 62/19, cit., p. 19.

²⁶⁵ Così, cfr. FABOZZO in *"analisi normativa e profili problematici del reato di diffusione illecita di immagini o video a contenuto sessualmente esplicito ex art 612 ter cp"*, in Riv. Pen. 2020, 2, 150; CASALNUOVO, COLELLA, *"il codice rosso. Guida operativa alla legge n 69 del 2019"*, Piacenza, 2019, 42

Perciò, il legislatore ha preferito mantenere questa definizione anche alla luce di un suo possibile intervento negli anni avvenire, al fine di porre maggiore chiarezza, come è successo per la definizione di pornografia minorile, richiamata nel 2012 con l'articolo 600 ter c.p.

La Corte costituzionale si è espressa in merito alla probabile violazione del principio di legalità precisando «l'esigenza costituzionale di determinatezza della fattispecie ai sensi dell'articolo 25, secondo comma della Costituzione non coincide necessariamente con il carattere più o meno descrittivo della stessa, ben potendo la norma incriminatrice fare uso di una tecnica esemplificativa, oppure riferirsi a concetti extra giuridici diffusi ovvero ancora a dati di esperienza comune o tecnica.

Il principio di determinatezza non esclude infatti l'ammissibilità di formule elastiche, alle quali non infrequentemente il legislatore deve ricorrere»²⁶⁶.

Le precedenti versioni dei disegni di legge che non sono entrati in vigore, in particolare il ddl n. 1076, aveva previsto una definizione per la diffusione di immagini a contenuto sessuale: «ogni rappresentazione, con qualunque mezzo, di soggetti consenzienti, coinvolti in attività sessuali, ovvero qualunque rappresentazione degli organi sessuali per scopi sessuali, realizzati, acquisiti ovvero comunque detenuti in occasione di rapporti od incontri anche occasionali», ma non è stata presa in considerazione²⁶⁷, poiché ritenuta superflua.

L'indeterminatezza in questione viene considerata tale anche in relazione all'utilizzo da parte del legislatore della parola "immagini".

Secondo la Giurisprudenza, l'uso di questo termine è volto a ricomprendere nella fattispecie anche le fotografie, al fine di ampliarne la portata applicativa²⁶⁸.

Escluse invece dalla disciplina dell'articolo 612 ter sono le immagini di nudo artistico, le registrazioni audio, quelle foto che vengono caricate sul *deep web*, su motori di ricerca nascosti dai comuni fruitori di *internet*, di foto non esplicite sessualmente ma caricate per esempio sui *social network*, di persone ritenute attraenti o di minori²⁶⁹.

²⁶⁶ Corte Cost. n. 172/2014

²⁶⁷ in particolare, il disegno di legge n 1076, che forniva come definizione "ogni rappresentazione, con qualunque mezzo, di soggetti consenzienti, coinvolti in attività sessuali, ovvero qualunque rappresentazione degli organi sessuali per scopi sessuali, realizzati, acquisiti ovvero comunque detenuti in occasione di rapporti od incontri anche occasionali".

²⁶⁸ per un maggiore approfondimento, LO MONTE E. "art 612 ter c.p. diffusione illecita di immagini o video sessualmente espliciti. Tra buoni propositi, denegato diritto all'oblio e 'morti social'" Torino, 2021, 72.

²⁶⁹ Intervista ad Alessandro Trivillini, responsabile del servizio di informatica forense della Scuola universitaria professionale della Svizzera italiana (SUPSI), secondo cui «Facebook e *Instagram* vengono definite fonti aperte, quando i genitori postano foto di minori online, i malintenzionati possono scaricare le immagini sul proprio dispositivo personale, i contenuti vengono scambiati tramite la rete TOR, che permettono di navigare senza farsi rintracciare. Se il dispositivo è acceso, tramite questa rete verranno scaricate le immagini, altrimenti non ci sarà nessuna traccia della operazione, perché il *deep web* non prevede una archiviazione sistematica dei siti» Articolo di VALENTINA CODA, Corriere del Ticino, 2019

Al contempo però, l'attuale genericità della normativa va a favore del legislatore, potendo ricomprendere nella condotta un più ampio spettro di violazioni, considerando anche la mutevole disciplina, per il quale, in sede di decisione definitiva, si dovrà analizzare caso per caso²⁷⁰.

Una corretta visione potrebbe essere quella fornita proprio in merito all'articolo 600 ter del c.p.: si prevede che ai fini dell'integrazione del reato, per "gli atti sessuali" si intende non per forza una esibizione lasciva degli organi genitali, di soggetti minori di anni diciotto, ma è sufficiente una qualsiasi rappresentazione degli stessi per scopi sessuali²⁷¹.

In questa prospettiva viene ricompresa anche la mera raffigurazione di corpi nudi, e le immagini nelle quali la vittima viene ritratta in un contesto dall'esplicito significato sessuale, ma senza che sia svestita²⁷².

Le immagini infatti, precisa la norma, devono essere 'esplicite' nel senso di contenuti sessuali chiari e diretti.

A conferma di questo orientamento, una più recente sentenza, la quale condanna un uomo per violazione dell'articolo 612 ter, per aver diffuso in rete video della sua ex ragazza in *lingerie*, per questo si evince che per "contenuto sessualmente esplicito" non si fa riferimento solo alla pubblicazione di contenuti con oggetto rapporti sessuali o organi sessuali, ma anche parti erogene del corpo che rimandano a un contesto di tipo sessuale²⁷³.

Tuttavia, altri ritengono che siffatta interpretazione non andrebbe presa in considerazione per il reato di diffusione illecita di immagini a sfondo sessuale, per questi infatti basterebbe una interpretazione restrittiva, considerando solo i contenuti espliciti, di matrice sessuale.

2.4 (segue): Il concetto di 'Nocumento' nel reato di *Revenge porn*

Analizzando l'articolo 612ter, si evince che il secondo comma costituisce una specificazione della condotta per il quale si prevede che la stessa pena, istituita nel comma primo, si applica a chi, avendo ricevuto o comunque acquisito le immagini o i

²⁷⁰ Contra, E. LO MONTE, *L'art. 612-ter C.P.*, cit., p. 166, che propone una clausola definitoria che include finanche l'elencazione delle parti anatomiche da considerare come "contenuto sessualmente esplicito" del materiale diffuso.

²⁷¹ Cass. Pen, sez III, 8 gennaio 2020, n. 9354

²⁷² Contra, SEMINARA S., *Delitti contro la libertà personale e morale*, in R. Bartoli, M. Pelissero, S. Seminara, *Diritto penale. Lineamenti di parte speciale*, Torino, Giappichelli, 2021. Anche G.M. Caletti, *Libertà e riservatezza sessuale all'epoca di Internet*.

²⁷³ Così, A. VALSECCHI, "*Codice rosso*" e diritto penale sostanziale; Id., *Delitti contro la libertà fisica e psichica dell'individuo*

video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza l'assenso delle persone rappresentate, al fine di recare loro "nocumento".

Perciò ai fini della imputabilità del reato, tutti gli elementi contenutistici del primo comma devono essere presenti.

Ciononostante, a differenza del primo comma, qui si fa riferimento a quei soggetti, cosiddetti secondi distributori, che non hanno prodotto direttamente il contenuto sessualmente esplicito, ma comunque avendolo ricevuto, ne aumentano la portata lesiva, diffondendolo a loro volta verso un numero ancora più ampio di persone.

Per questo motivo, rientra all'interno della fattispecie sia colui che semplicemente si occupa di inoltrare un'immagine, sia chi rincara la dose di offensività verso la vittima, contribuendo con insulti e minacce, oppure colui che, dopo che la vittima ha ottenuto, a seguito di un complicato *iter*, la cancellazione delle proprie immagini dalle piattaforme, dopo anni ricomincia la loro distribuzione²⁷⁴.

Appaiono ravvisabili, fra le condotte definite dai due commi, anche diversi obiettivi del soggetto agente.

Nel primo comma, il dolo è generico, mentre nel comma secondo è presente la finalità di arrecare nocumento alla persona offesa, riferendosi quindi a una ipotesi di dolo specifico (e non di dolo diretto, ossia la sola consapevolezza e la volontà di poter arrecare un danno, che rientra nel dolo generico), presupposto che è presente per il distributore del contenuto, (per il quale dovrà essere dimostrata questa finalità attuata nei confronti della vittima) ma non per il realizzatore.

Il termine "nocumento" deriva dal verbo "nuocere" e si riferisce all'esistenza di una lesione concreta della sfera personale e patrimoniale²⁷⁵.

Secondo una recente sentenza, per 'nocumento' quindi, non si intenderebbe solo un danno di carattere patrimoniale, quando dalla divulgazione del contenuto derivi una diminuzione del patrimonio suscettibile di valutazione (per esempio nel caso in cui la vittima venga licenziata dal lavoro a causa del contenuto diffuso), ma anche per il conseguente danno morale alla sua sfera psicologica e relazionale²⁷⁶.

Tuttavia, il dolo specifico viene considerato come di difficile dimostrazione in sede processuale.

²⁷⁴ CITRON D.K, *Hate Crimes in cyberspace*, 2016. Un esempio di questa ultima condotta è stato messo in atto nel Caso Cantone, in America, dove uno sconosciuto ha ripubblicato dopo molti anni le foto a contenuto sessualmente esplicito facendole di nuovo circolare sul web.

²⁷⁵ In tale modo anche Cass. Pen sez. III, n 7504 del 2014; Cass. Pen. Sez. III, n 15221/2016

²⁷⁶ Tribunale di Roma, 27 ottobre 2011 in *Guida Dir.* 2012, 5, secondo questa sentenza il danno è *l'incipit* che ha portato alla necessità di sostegno psicologico che potrebbe condurre alla prova del danno stesso.

Alcuni studiosi²⁷⁷, infatti, suggerivano di modificare l'articolo con una formula che rinvia all'articolo 59 comma 2 c.p.²⁷⁸ «qualora il dissenso delle persone rappresentate era da lui conosciuto ovvero ignorato per colpa o ritenuto inesistente per errore determinato da colpa».

Mentre altri, ritenevano fosse opportuno inserire il *fine di arrecare nocumento* nel terzo comma dell'art 612 ter c.p., come una circostanza aggravante della condotta²⁷⁹.

Inoltre la presenza di dolo specifico farebbe sì che sia possibile l'esclusione, in capo al secondo distributore, della fattispecie di dolo eventuale sulla mancanza di consenso alla divulgazione, alla stregua dello stretto rapporto che intercorre fra il divulgatore stesso e la volontà di arrecare nocumento alla vittima²⁸⁰.

Questa definizione porrebbe come presupposto il fatto che la vittima debba mettere al corrente il *provider* della mancanza di volontà alla diffusione del materiale intimo.

Per la prova del dolo specifico, la Cassazione si è espressa in merito agli atti persecutori²⁸¹, ma la massima può essere applicabile anche alla casistica in esame del reato di *Revenge porn*.

Si prevede che non è elemento imprescindibile l'attuazione di una perizia o consulenza tecnica sulla prova del nocumento, quindi il Giudice potrà valutare la sussistenza degli effetti della condotta illecita sul soggetto passivo e sul suo equilibrio psicologico, anche grazie a massime di esperienza e alla situazione pregressa di stato mentale della persona offesa, tenendo a mente anche il contesto sociale in cui vive, il comportamento del soggetto attivo e altre previsioni circostanziali, ai fini di una analisi più approfondita del turbamento psicofisico della vittima.

Infine, pare ravvisabile da una parte della Dottrina, una sorta di disparità di trattamento fra i primi e i secondi distributori.

Per i primi, il dato letterale istituisce una punizione fino ai sei anni, a prescindere dal fine di arrecare nocumento alla persona offesa, elemento che invece, per i secondi distributori, deve essere dimostrato per assicurare la punibilità e la configurazione del reato²⁸².

²⁷⁷ Di diverso approccio è M. DOVA, Art. 612-ter, cit., p. 1942, che, alludendo alla presenza di una lesione della riservatezza della vittima, pensa che l'accertamento del dolo specifico non contrasti con l'effettività della norma, perché l'art. 612-ter, comma 2, c.p. verrebbe considerato come «un singolare reato di danno la cui realizzazione è sorretta dalla finalità di nocumento» «e in particolare da quelli che restituiscono al dolo specifico una dimensione oggettiva, in termini di idoneità della condotta al fine, che altrimenti si muoverebbe in un'incerta dimensione puramente psicologica». Per quest'ultimo, il carattere oggettivamente lesivo non comporterebbe l'accertata prova del fatto che ci fosse la volontà di arrecare nocumento.

²⁷⁸ Cfr. ROMANO B., L'introduzione dell'articolo 612-ter, cit., p. 109.

²⁷⁹ AMORE, "la tutela penale della riservatezza sessuale nella società digitale" in *Quotidiano Giuridico*, 2019, 37

²⁸⁰ Cass. Pen. Sez V n 30334/2016 in *Dir&giust.* 18 luglio.

²⁸¹ Cass. Pen. Sez. n. 6, n. 20038, 19.3.2014, Rv. 259458

²⁸² CADOPPI A., VENEZIANI P., *Elementi di diritto penale, parte speciale, i reati contro la persona, Tomo II, vol. 2, i reati contro i soggetti deboli*, 2023

2.5 (segue): Le circostanze aggravanti e il maggiore disvalore penalistico in base alla qualità della persona offesa

Il comma tre e quattro dell'articolo 612 ter definiscono alcune circostanze aggravanti: «La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici.

La pena è aumentata da un terzo alla metà se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza»²⁸³.

Questi aumenti di pena sono stati introdotti per far fronte a un aggravamento del disvalore penale dato dall'eventuale condotta realizzata, nei confronti di un particolare rapporto che intercorre con la vittima, oppure per determinate condizioni.

Il comma terzo è volto a regolare quelle ipotesi di rottura del rapporto fiduciario che fa capo a una relazione di tipo affettivo, pregressa o esistente alla commissione del fatto, intesa in modo volutamente generico (al fine di far fronte a una modifica dei costumi della popolazione e anche per ricomprendere tutte quelle fattispecie che non prevedono il rito matrimoniale, come le unioni civili).

Qui il legislatore chiaramente ha voluto evidenziare, mediante questa apposita aggravante, la violenza di genere che di solito viene perpetrata durante un rapporto sentimentale e che il Codice Rosso mira a contrastare.

In questa aggravante, non si potrebbe ravvisare una violazione del principio di determinatezza, in quanto il legislatore ha voluto dare priorità alla tutela dei diritti, ricomprendendo anche tutti quei casi di relazioni interpersonale, che non sono inclusi in un rapporto di tipo sentimentale.

La Cassazione definisce infatti il termine "relazione affettiva" come «non solo la stabile condivisione della vita comune ma anche il legame connotato da un reciproco rapporto di fiducia, tale da ingenerare nella vittima aspettative di tutela e protezione»²⁸⁴.

A fronte di ciò, sarà il legislatore a dover decidere caso per caso.

Il legame affettivo è una circostanza ad effetto comune, per il quale quindi è previsto l'aumento di un terzo della pena; questa disciplina viene ad esistenza anche per il delitto di atti persecutori al comma due dell'articolo 612 bis e anche per il delitto di violenza sessuale al n. 5. quater dell'articolo 609 ter cod. pen.

La seconda parte del comma terzo riguarda l'aggravante a effetto comune dell'utilizzo di strumenti informatici o telematici, che si pongono al centro della condotta offensiva regolata dalla normativa contro il *Revenge porn*, essendo questa oggi il principale metodo di realizzazione della condotta.

²⁸³PIERDONATI M., *La tutela delle persone vulnerabili con particolare riferimento all'analisi della legge 19 luglio 2019, n. 69 (c.d. 'codice rosso')*, in *La Giustizia Penale*, 2020

²⁸⁴Cass. Pen. Sez III n 11920/2018

Come già definito in precedenza, per strumenti informatici si intende, secondo l'articolo 1 lett. a della Convenzione di Budapest, ogni apparecchiatura o insieme di strumenti connesse grazie a un programma, che compiono elaborazione automatica di dati.

Per sistema telematico invece la Dottrina maggioritaria²⁸⁵ intende un metodo di trasmissione e circolazione del pensiero, tramite dati e informazioni che vengono trasmessi a distanza tramite un linguaggio computerizzato che veicola informazioni automatizzate, per esempio la rete *internet*.

Evidente dalla letteralità della normativa è la pericolosità maggiore che deriva dall'uso di questi strumenti che si contrappone al diritto di libera fruizione dei contenuti caricati. Una nota sentenza degli anni duemila definiva *internet* come 'mezzo di pubblicità' ritenendo inapplicabili le normative riguardanti la stampa e la radiotelevisione²⁸⁶; nel caso di specie le informazioni diffamatorie erano state inserite su un sito con il titolo di "*dossier*", questo era gratuito e fruibile da tutti gli utenti di *internet* e quindi maggiormente virulento.

Altra giurisprudenza rilevante in materia, riguarda un uomo e una donna che si sono messi d'accordo per diffondere materiale intimo dei loro ex amanti, pubblicandoli su *Facebook*, per tali fatti vennero condannati per atti persecutori²⁸⁷.

Sebbene possa ravvisarsi questa circostanza dell'uso di strumenti informatici o telematici anche nel reato di atti persecutori, la differenza principale risiede nel fatto che lo *stalking* può anche essere messo in atto senza l'utilizzo di tali mezzi (per questo esiste il termine *cyber stalking*).

Per lo *stalking* quindi, si ritiene giustificata l'introduzione dell'aggravante da parte del legislatore, mentre attualmente, esaminando il reato di *Revenge porn*, l'aggravante appena descritta risulta all'ordine del giorno, in quanto è il *modus operandi* più diffuso per il reato all'articolo 612 ter c.p., trattandosi per l'appunto di un reato propriamente informatico²⁸⁸.

Per questo motivo, potendo esser considerato come elemento costitutivo del reato in questione, questa aggravante viene considerata dalla maggior parte della Dottrina come una specificazione che poteva essere evitata²⁸⁹.

Altra differenza con la fattispecie di *cyber stalking* si sottolinea in merito alla condotta: il *Revenge porn* ha ad oggetto una sola condotta, mentre per l'altra fattispecie sono necessarie una pluralità di condotte (almeno due).

Ulteriore aggravante viene ad esistenza per la diffusione di immagini sessualmente espliciti verso donne incinta, o soggetti affetti da inferiorità fisica o psichica,

²⁸⁵ FROSINI, "*telematica e informatica giuridica*" in *Enciclopedia del diritto*, 1992, XLIV, 60

²⁸⁶ Tribunale di Oristano, 25 maggio 2000 in *riv. it. dir. e proc. pen.* 2001, 1405 con nota Scopinaro.

²⁸⁷ Tribunale di Milano, sez. IX penale, n 13365 14 dicembre 2016

²⁸⁸ FABOZZO M., *Analisi normativa e profili problematici del reato di "diffusione illecita di immagini o video a contenuto sessualmente esplicito" (c.d. "Revenge porn") ex art. 612-ter c.p., in Rivista penale*, 2020

²⁸⁹ GIANMARCO CALETTI, "*'Revenge Porn' prime considerazioni in vista dell'introduzione dell'art. 612 ter cp, una fattispecie esemplare, ma davvero efficace?*" in *Diritto penale contemporaneo*, 23 aprile 2019

quest'ultima precisazione, tuttavia, appare molto generica, tanto da non essere necessaria una valutazione medica.

Al contrario, quest'ultima è fondamentale per il riconoscimento della disabilità prevista nell'articolo 612 bis²⁹⁰.

L'infermità viene correlata alla nozione della minorata difesa, prevista nell'articolo 61 n. 5 c.p.; Dottrina e Giurisprudenza definiscono quest'ultima come lo stato di inferiorità dal punto di vista psichico o fisico che si presenta nel momento in cui la vittima non ha la possibilità di difendersi autonomamente, facilitando il compiersi dell'illecito nei suoi confronti.

Questa circostanza a effetto speciale, non prevede alcune situazioni che invece vengono considerate dal legislatore per il reato di pornografia minorile all'articolo 600 cod. Pen. Una differenza riguarda, per esempio, l'assenza nella disciplina dedicata al *Revenge porn*, di una aggravante in caso di soggetti di minore età, per i quali spetta massima tutela ai sensi dell'articolo 31 della Costituzione.

Infatti, secondo parte della Dottrina, non si ritiene corretto aggiungere i minori nell'alveo dei soggetti a cui si riferisce l'aggravante dell'articolo 612ter, per infermità fisica o psichica²⁹¹.

Tuttavia, questa esclusione da parte del legislatore trova la sua *ratio* nel fatto che in questo caso, grazie al fenomeno dell'assorbimento, il reato di diffusione illecita di immagini sessualmente esplicite espletato nei confronti di minori, venga assorbito dal più grave reato di pornografia minorile, per il quale è previsto un maggiore limite edittale.

La Suprema Corte, in un primo momento, nella sentenza del 2019 affermava che «la disciplina della pornografia minorile è affidata esclusivamente al sistema chiuso degli art. 600-ter e seguenti»²⁹².

Oggi però, con una più recente casistica, la Corte ha escluso, per quanto riguarda la fattispecie di immagini auto prodotte dal minore, che la loro circolazione possa integrare la fattispecie di “distribuzione, divulgazione, diffusione, pubblicizzazione di materiale pedopornografico”.

Quindi la norma in commento potrà essere applicata anche in molte delle ipotesi di pornografia non consensuale in ambito minorile²⁹³.

Per la decisione concernente la gravità del reato²⁹⁴, il legislatore può sia guardare alla pena (gravità in astratto), ma anche considerare la gravità in concreto.

²⁹⁰ articolo 3 legge 104/1992

²⁹¹ in questo senso CAMPAGNOLI M.N., *Social media e information disorder: questioni di ecologia comunicativa in Rete (Parte Terza – Il Revenge porn)*, in *Dirittifondamentali.it*, 2020, III, p. 323; PIERDONATI M., *La tutela delle persone vulnerabili con particolare riferimento all'analisi della legge 19 luglio 2019, n. 69 (c.d. 'codice rosso')*, in *La Giustizia Penale*, 2020, n. 3, c. 189.

²⁹² Cass. Pen, sez. III, sentenza del 21 novembre 2019, n. 5522, punto 10 del Considerato in diritto

²⁹³ Sul mutamento di orientamento giurisprudenziale, BIANCHI M., *Il “Sexting minorile” non è più reato?*, 2016, Cass. pen., Sez. III, 21.3.2016, n. 116755 cit., passim.

²⁹⁴ Art. 133 cp

Infatti, in presenza di una condizione di inferiorità fisica o psichica sarà il giudice a valutare caso per caso le condizioni della persona offesa²⁹⁵.

La Giurisprudenza ha preferito senz'altro l'applicazione della prima.

Per quanto concerne lo stato di gravidanza, la *ratio* dell'aggravante, ripresa anche nell'articolo 612bis, deve essere riscontrata nella volontà di protezione della donna stessa e del feto, per far fronte a un potenziale danno psico-fisico.

Anche se non espressamente previsto dalla norma, si ritiene si faccia riferimento alla sussistenza dello stato particolare, al momento di divulgazione del contenuto, il quale comporterebbe un grave stato di ansia e turbamento alla persona offesa²⁹⁶.

Tuttavia, bisogna prendere in considerazione anche il caso in cui il soggetto attivo non sia a conoscenza dello stato di gravidanza, indi per cui, se ignorasse questa evenienza, la fattispecie in esame non potrebbe trovare applicazione, ai sensi dell'articolo 59 comma 2 del c.p., il quale prevede l'impossibilità di attuazione di questa aggravante, nel caso in cui ignorasse lo stato particolare per colpa o per errore determinato da colpa.

2.6 (Segue): Il regime di procedibilità

L'articolo 612 ter, al pari dell'articolo 612 bis in tema di atti persecutori, a causa della ingerenza che avviene nella vita privata e intima della vittima, prevede la procedibilità a querela della persona offesa mediante richiesta ai Carabinieri, agli uffici di Polizia, alla Procura della Repubblica a mezzo del proprio avvocato.

I termini rispetto alla normativa generale prevista dall'articolo 124 c.p. di tre mesi, sono aumentati a sei, sebbene ci siano state non poche critiche dalla Dottrina²⁹⁷.

Ciò ha il fine di permettere alla vittima di valutare la convenienza e la correttezza della querela.

Per quanto concerne il *dies a quo*, non si segue la disciplina prevista all'articolo 124 c.p. che stabilisce il generale principio di inizio del termine nel momento in cui la condotta costituisce reato²⁹⁸, ma il termine decorrerà dal momento di venuta a conoscenza della vittima della condivisione illecita²⁹⁹.

²⁹⁵ Cass. Pen sez I n 4322/1997 in Cass. Pen 1998,822. FIANDACA-MUSCO, "diritto penale. Parte generale", Zanichelli, Bologna, 2010; vedi anche Cass. Pen. N 15/1997 in *riv. pen.* 1998 n 251

²⁹⁶ Cfr. G.M. CALETTI, *Libertà e riservatezza sessuale all'epoca di Internet*

²⁹⁷ LOMETTI S., *Il delitto di diffusione illecita di immagini o video sessualmente espliciti*, 2021 cit., p. 240.

²⁹⁸ Secondo la Cassazione, la notizia deve essere basata su elementi concreti sia in relazione al fatto oggetto di reato sia in relazione a chi l'ha commesso. Cass. Pen. Sez V n 33466/2008 in *Ced Cass. Pen.* rivista n 241396

²⁹⁹ Cass. Pen., Sez. IV, n. 21527, 21.01.2015 «il termine per la proposizione della querela decorre dal momento in cui il titolare del relativo diritto ha conoscenza certa del fatto di reato nella sua dimensione oggettiva e soggettiva, e cioè dalla data del reato perfetto in tutti i suoi elementi costitutivi».

Sussiste, solo per la fattispecie di diffusione illecita di immagini e per il reato di *stalking*, non anche per il reato di violenza sessuale, la possibilità di remissione.

Quest'ultima deve essere solamente processuale, perciò è irrevocabile³⁰⁰.

La sua irrevocabilità serve ad impedire che la vittima possa essere influenzata o minacciata dal soggetto attivo.

La remissione processuale della querela trova la sua *ratio* nella volontà di affidare all'autorità giudiziaria l'attendibilità della richiesta.

A seguito di questa, l'indagato deve essere rimesso in libertà nell'immediato.

La remissione non può essere tacita³⁰¹, ma deve essere portata a conoscenza del Giudice mediante Procuratore speciale, può essere proposta in modalità scritta od orale e può essere presentata anche da terzi, per esempio i familiari della vittima.

È prevista la procedibilità d'ufficio dalla seconda parte del quarto comma, per i casi di persona offesa incinta o un soggetto in condizioni di inferiorità fisica o psichica, quando il fatto è commesso in connessione ad un altro delitto procedibile d'ufficio.

Il fine ultimo di questa possibilità, è perseguire il delitto in esame il prima possibile³⁰², oppure la protezione di soggetti particolarmente vulnerabili, che a causa della loro condizione, potrebbero avere remore a denunciare l'accaduto; la stessa *ratio* è alla base anche di quella prevista per gli atti persecutori.

La procedibilità d'ufficio segue l'articolo 12 del cod. di proc. pen., stabilendo tre ipotesi: La prima riguarda il reato commesso da vari soggetti in concorso oppure con condotte indipendenti che hanno determinato il verificarsi dell'evento.

³⁰⁰ si segue quindi il principio di irretroattività della legge penale, regolato dall'articolo 25 comma secondo della Costituzione, secondo cui nessuno può essere punito se non in forza di una legge che sia entrata in vigore prima del fatto commesso, principio ripreso anche dall'articolo 7 della CEDU, secondo la Corte Costituzionale questo principio viene considerato uno strumento essenziale di garanzia per il cittadino contro l'eccessiva arbitrarietà del legislatore, e quindi necessario per la libera autodeterminazione individuale: In Corte Cost. N 394/2006; per cui il reato di diffusione di immagini sessualmente esplicite potrà essere applicato solo ai casi successivi all'entrata in vigore della legge che lo prevede. Questo principio è tutelato anche dal Codice penale all'articolo 2 comma 1; inoltre, nei commi seguenti stabilisce l'ulteriore principio di retroattività delle norme penali sopravvenute che siano favorevoli al reo, definendo che, se vi sia stata condanna per un fatto commesso all'epoca della vigenza della norma sfavorevole, cessano gli effetti penali della medesima. Questo principio a differenza della irretroattività sfavorevole trova la sua *ratio* nella necessità di rispettare l'uguaglianza e la ragionevolezza sanciti dall'articolo 3 della costituzione, per evitare l'applicazione di una determinata sanzione che non è più intesa in senso così grave dalla legge, ma più mite. Essendo questa la *ratio*, il legislatore, può derogare a questo principio (a patto che ci siano ragioni di esigenze di tutela di interessi aventi rango almeno pari a quelli per cui si fa riferimento nel principio derogato), cosa che invece non accade col principio di irretroattività, che rimane inderogabile.

³⁰¹ secondo le Sezioni unite, in Cass. Pen. Sez.V n 17756/2008 in *guida al diritto* 2008,23, corrispondendo la disciplina al principio di responsabilità, prevede che la mancata comparizione del querelante non integra una ipotesi di remissione tacita, salvo nel caso previsto dagli articoli 21,28,30 sui procedimenti davanti il Giudice di Pace

³⁰² Cfr. Cass. Sez. III, 30 novembre 2005 (dep. 29 dicembre 2005) n. 47247, CED 233016; Cfr. Cass. Sez.III, 9 luglio 1996 (dep. 8 agosto 1996) n. 3014, CED 206061

La seconda, quando un soggetto è imputato per più reati venuti ad esistenza con una sola azione od omissione o con più azioni od omissioni, ma che fanno parte dello stesso disegno criminoso.

La terza riguarda invece l'ipotesi per cui i reati per i quali si procede sono stati commessi in funzione dell'esecuzione di altri reati.

Tuttavia, in merito alla "connessione" si fa riferimento anche a un collegamento di tipo investigativo, regolato dall'articolo 371 comma 2 cpp.

Per quanto riguarda la procedibilità d'ufficio, infatti, determinata dalla ipotesi di connessione prevista dall'art. 609 septies, 4° co., n. 4 c.p., questa verrebbe ad esistenza non solo quando, come detto poc'anzi, nel caso di connessione di tipo processuale (art. 12 c.p.p.), ma anche quando si verifica un collegamento materiale.

Per "collegamento materiale", si intende tutte le volte che l'indagine sul reato perseguibile di ufficio comporti obbligatoriamente l'accertamento di quello procedibile a querela.

La ricorrenza di una tale forma di connessione "investigativa", dovrebbe considerarsi come l'inizio effettivo delle indagini sul reato perseguibile d'ufficio.

Non deve essere ritenuta quindi sufficiente, secondo la Giurisprudenza, una mera indicazione della connessione tra i diversi fatti, se quest'ultima risulti avvalorata da elementi indizianti rilevanti sotto il profilo investigativo³⁰³.

Successivamente alla denuncia del reato da parte della persona offesa, le indagini in merito alla ricostruzione della vicenda vengono avviate senza ritardo.

Fondamentale è la collaborazione della vittima nel fornire le informazioni necessarie per la ricostruzione dell'accaduto, ai fini di un lavoro semplificato per gli inquirenti.

Infatti, più complesso sarà se la vittima non è capace di fornire dettagli in più circa la diffusione del materiale intimo.

Gli inquirenti dovranno, in questo caso, operare una indagine sulle utenze utilizzate, per trovare chi ha diffuso il materiale in primo luogo.

Nel corso di queste ultime, l'autorità competente potrebbe anche applicare misure cautelari, come l'allontanamento dal nucleo familiare o la custodia cautelare in carcere.

Nel caso in cui avvenga una modifica o una revoca di queste disposizioni, la vittima ha il diritto di essere informata tempestivamente.

³⁰³ Cfr. Cass. Sez.III, 17 novembre 2005 (dep. 10 gennaio 2006) n. 307, CED 233284

2.7 (Segue): *Revenge porn* - una disciplina volta alla tutela dei diritti fondamentali della persona

Il diritto alla riservatezza in relazione alla sfera sessuale

Altro elemento da considerare ai fini di una analisi approfondita sulla condotta³⁰⁴, riguarda i beni giuridici lesi dalla condotta posta in essere dal perpetratore del reato. Uno dei diritti maggiormente a rischio in caso di diffusione illecita di immagini di carattere sessuale è la riservatezza, in quanto il comportamento posto in essere provoca una grave intrusione nella vita privata della vittima.

Il primo comma dell'articolo 612 ter, tutela questo diritto, sia con il riferimento alla mancanza di assenso alla formazione del contenuto, ma anche immettendo nel testo della normativa la locuzione "video o immagini 'destinati a rimanere privati'", che rende implicitamente l'idea che il contenuto venga realizzato in un contesto di coppia o relazione affettiva.

Da una parte, la maggioranza dei casi dà ragione a questa implicazione, dall'altra, però, non considera che il contenuto potrebbe anche essere registrato da un terzo all'insaputa della coppia.

Con questa specificazione il legislatore voleva anche valorizzare il diritto alla riservatezza garantito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea³⁰⁵.

È emblematico il caso sottoposto al Tribunale di Reggio Emilia³⁰⁶: in questa sede, è stata accertata la divulgazione di un video circa un rapporto sessuale avvenuto nei locali dei servizi igienici di una discoteca, la cui porta era stata chiusa a chiave dalla coppia ripresa.

Il video è stato girato da delle persone terze al rapporto, che si sono affacciate dall'alto della porta del bagno, per poter riprendere.

Secondo il Giudice, l'estraneità degli imputati alla relazione della coppia, vittima della diffusione del video, comporta un difetto di tipicità ai sensi dell'art. 612-ter c.p., stabilendo quindi l'assoluzione con la formula «il fatto non sussiste».

La decisione ricalca l'aspetto letterale della norma in esame, per il quale si vuole attribuire rilevanza penale alle sole condotte ivi descritte, esclusivamente

³⁰⁴ Cass. pen., Sez. V, sent. n. 14927 (ud. 22 febbraio 2023, dep. 7 aprile 2023), rel. Brancaccio

³⁰⁵ in merito a questo concetto, CGUE, 7.2.2012, Von Hannover c. Germania; CGUE, 4.12.2015, Zakharov v. Russia.

³⁰⁶ sezione GIP/GUP, sentenza del 22 novembre 2021, n. 528; In commento alla pronuncia BECCARI, *Le prime difficoltà applicative della nuova fattispecie di "revenge porn" in caso di diffusione del materiale da parte di soggetti estranei al rapporto sessuale*, in *Sist. pen.*, 2022, 6, 5 ss.; nonché in *disCrimen*, 7 gennaio 2022, con note di MICHELETTI D., *L'intervento pubblicazione quale elemento costitutivo della fattispecie di Revenge porn*, e C. Paonessa, *Ai confini del c.d. Revenge porn. Tessere di un mosaico normativo* (18 marzo 2022).

nell'eventualità che le immagini o i video siano stati condivisi o realizzati dalla coppia stessa, minando la reciproca fiducia³⁰⁷.

Quindi, in mancanza di una diversa previsione legislativa, secondo la sentenza in esame «non riveste alcuna rilevanza penale» la condotta avente ad oggetto la diffusione di materiale sessualmente esplicito, realizzato e acquisito da un terzo «che evidentemente non faccia parte del contesto relazionale».

Per questo motivo, l'inciso della norma sulla “destinazione privata” del contenuto, esclude dalla fattispecie il caso in cui dei soggetti si espongano volontariamente alla possibilità di essere visti, e vengano ripresi da terzi, estranei al rapporto, senza consenso³⁰⁸.

Peraltro, tramite questa precisazione introdotta al primo comma, si vogliono escludere anche quei contenuti realizzati con il fine di renderli pubblici: come nel caso di video di attori *hard*³⁰⁹, per i quali non c'è una lesione del diritto in esame.

La riservatezza viene posta come fondamento anche della Costituzione, all'articolo 15, istituendo l'inviolabilità della "libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione", all'art 3 della Cost. in riferimento al diritto alla dignità sociale, all'articolo 8 parag. 1 CEDU “diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza” e all'articolo 16 parag. 1 TFUE.

Questa è oggetto di tutela anche degli articoli 617 e 615 bis del c.p. il quale punisce con la reclusione da sei mesi a quattro anni chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'art. 614.

L'obiettivo è quello di garantire all'individuo protezione, rispetto ogni forma di intromissione che non trovi giustificazione in esigenze di ordine generale, debitamente vagliate dall'autorità giudiziaria.

In ultima analisi, la puntualizzazione ‘destinati a rimanere privati’ deve essere letta in chiave soggettiva, considerandola come la volontà consenziente di rappresentazione delle immagini³¹⁰.

³⁰⁷ commento alla pronuncia v. P. Beccari, *Le prime difficoltà applicative della nuova fattispecie di “Revenge porn” in caso di diffusione del materiale da parte di soggetti estranei al rapporto sessuale*, in *Sistema penale*, 2022; D. MICHELETTI, *L'interversione publicationis quale elemento costitutivo della fattispecie di revenge porn*, in *Dicrimen*, 2022.

³⁰⁸ D. MICHELETTI, *L'interversione publicationis quale elemento costitutivo della fattispecie di Revenge porn*, cit., 7, «che chi si apparta maldestramente in preda a furore amoroso, senza premunirsi di non essere visto, non può che imputare a sé stesso l'eventuale cattura e diffusione di immagini che lo riguardano»

³⁰⁹ vedi cfr. CALETTI, *“Libertà e riservatezza sessuale all'epoca di internet. L'articolo 612 ter e l'incriminazione della pornografia non consensuale”*, in *rivista italiana diritto e procedura penale* 2019,4

³¹⁰ *La legislazione penale*, N. AMORE, in *La tutela Penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'articolo 612ter cp 20.1.2020*

Si può ritenere, secondo molti studiosi in Dottrina, fra cui De Cupis, che il diritto alla riservatezza rientri in un più generale alveo di diritti fondamentali tutelati dal legislatore³¹¹.

La Corte costituzionale affronta questo tema in una sentenza³¹², ponendo la riservatezza in un'ottica di bilanciamento³¹³ tra diritti, riconducendone «il proprio decoro, il proprio onore, la propria rispettabilità, riservatezza, intimità e reputazione» e considerando questo bene giuridico come parte dei «diritti inviolabili dell'uomo» all'art. 2 della Costituzione.

Anche la sentenza n. 218 del '94 ha voluto confermare questa visione, definendo che, in ordine al «diritto alla riservatezza sul proprio stato di salute ed al mantenimento della vita lavorativa e di relazione compatibile con tale stato», la dignità umana è «comprensiva del diritto alla riservatezza»³¹⁴.

Manifestazioni di questo principio vengono ad esistenza anche considerando la sfera sessuale dell'individuo: la Cassazione³¹⁵, ha ricondotto tra i diritti inviolabili anche «il diritto di realizzare, nella vita di relazione, la propria identità sessuale, da ritenere aspetto e fattore di svolgimento della personalità».

L'articolo tre, comma uno della Costituzione ha come corollario la dignità sociale, l'onore e la reputazione, per la quale il giudice deve effettuare un bilanciamento con il diritto alla riservatezza e la libertà di manifestazione di pensiero regolato dall'articolo 21.

Tuttavia, queste libertà vengono limitate dall'ultimo comma, dal rispetto del buon costume, che oggi viene definita come pudore sessuale³¹⁶.

De facto, i diritti in questione vengono anche tutelati, non solo dalla disciplina nazionale, ma anche sul piano sovranazionale, grazie alla Convenzione Europea dei Diritti dell'uomo all'articolo 10, e 11 della Carta di Nizza.

In conclusione, in tema di *Revenge porn*, la libertà di espressione deve comunque essere bilanciata dal legislatore con il diritto alla *privacy*.

Per questo il diritto alla riservatezza si pone come corollario di una serie di diritti che devono essere tutelati dal legislatore tramite l'articolo 612ter.

Tuttavia, i *social network* rendono difficile il suo l'operato, poiché coloro che commettono il reato sono convinti di avere una "impunità", a causa della lontananza

³¹¹ PIZZORUSO A., Sul diritto alla riservatezza nella Costituzione italiana, in *Prassi e Teoria*, 1976, p. 32

³¹² Corte Cost. Sent. n. 38/73

³¹³ GIACOBBE G., *Il "diritto alla riservatezza" in Italia*, 1988 cit., p. 709. Il bilanciamento riguarda in particolare il rapporto con la libertà di manifestazione del pensiero

³¹⁴ Cfr. G.M. CALETTI, *Libertà e riservatezza sessuale all'epoca di Internet*

³¹⁵ Cass. Pen. n. 161 del 1985

³¹⁶ la Corte costituzionale ha definito questo limite in riferimento all'«insieme di precetti che impongono un determinato comportamento nella vita sociale di relazione, la inosservanza dei quali comporta in particolare la violazione del pudore sessuale, [...] soprattutto nell'ambito [...] della dignità personale che con esso si congiunge, e del sentimento morale dei giovani» Corte cost., 4 febbraio 1965, n.9

dalla persona offesa e della erronea percezione di mancanza di punizioni adeguate alle condotte commesse *online*³¹⁷.

Il diritto alla privacy e all'oblio: la procedura di deindicizzazione a tutela dei contenuti privati immessi online

Correlato alla disciplina di protezione dei dati personali e alla riservatezza, è il diritto all'oblio³¹⁸, di matrice giurisprudenziale, rientrante nell'alveo dei diritti della personalità.

Infatti, la sua introduzione in questo tipo di diritti trova la *ratio* nel fatto che il contenuto, appena viene immesso sul *web*, diventa di dominio pubblico ed è molto difficile eliminarne ogni traccia.

Si parla di diritto all'oblio sia in relazione a coloro i quali sono stati sottoposti a condanna, che richiedono la cancellazione delle loro informazioni a seguito di vicende giudiziarie, ma anche per coloro le cui informazioni sono già presenti sulla rete.

Queste possono non riguardare condanne, ma informazioni personali che vogliano tenere per sé, a tutela della loro riservatezza e per i quali si può richiedere la procedura di deindicizzazione.

Tuttavia, il diritto all'oblio si differenzia nella sua definizione sostanziale rispetto al diritto alla riservatezza: il primo non preclude la divulgazione di notizie, ma impedisce che fatti già presenti nei database possano essere riportati alla luce a distanza di tempo³¹⁹.

Nel 2008, alla Conferenza Internazionale di protezione dei dati, le autorità si sono riunite per fornire delle raccomandazioni in tema *privacy*, ai fornitori dei servizi di *social network*.

Innanzitutto, fondamentale ai fini di una tutela completa è il consenso dell'utente alla procedura di indicizzazione dei dati a lui appartenenti, successivamente si ritiene di dover dare maggiore rilevanza alla trasparenza delle informazioni.

³¹⁷ ZANI F., *Il difficile bilanciamento fra tutela della libertà di manifestazione del pensiero e diritto alla riservatezza nell'era dei social network*, in *Osservatorio costituzionale*, 2014.

³¹⁸ già previsto dall'articolo 17 del Regolamento UE 679/2016 (c.d. "GDPR") il quale introduce il diritto dell'interessato alla «cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo, il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei seguenti motivi: se i dati personali non sono più necessari per le finalità per i quali sono stati trattati, se l'interessato revoca il consenso su cui si basa il trattamento, se l'interessato si oppone al trattamento, se i dati sono stati illecitamente trattati, se devono essere cancellati per adempiere ad un obbligo giuridico, se sono raccolti ai fini della offerta dei servizi della società dell'informazione»

³¹⁹ Cass. Civ, Sez. I, n. 91437/2020

In secondo luogo, un controllo costante sui dati che riguardano gli utenti, e l'assicurare delle modalità più efficaci e semplici per i cittadini affinché possano autonomamente e senza difficoltà recedere dal servizio.

Necessario è anche un potenziamento delle misure di controllo, per evitare che avvengano accessi abusivi alle informazioni dei cittadini, da parte di terzi malintenzionati.

Una sentenza si è rivelata fondamentale in materia, "*Google Spain*"³²⁰, della Corte di Giustizia Europea³²¹.

La Corte, per la prima volta, con questo caso riconosce il diritto all'oblio sulla base della direttiva 95/46 CE sul trattamento dei dati personali.

Tuttavia, in merito a questa decisione, in Dottrina sono sorti molti dubbi sul bilanciamento del diritto all'informazione della comunità e il diritto alla *privacy* del cittadino; sebbene, molti si sono espressi ritenendola una vera e propria vittoria per la protezione dei dati personali.

Il diritto è esercitabile dal singolo, e tramite questo si ha la facoltà di chiedere la cancellazione dei contenuti riguardanti il cittadino, immessi nella rete, quando questi arrecano danno alla persona³²².

La Cassazione ha definito questo diritto come "Il giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata"³²³.

Il diritto all'oblio è tutelato, seppur in via accessoria e non vincolante, anche dall'articolo 11 comma 1 della Dichiarazione dei diritti di *Internet*, emanata nel 2015, «ogni persona ha il diritto di ottenere la cancellazione dagli indici dei motori di ricerca dei riferimenti ad informazioni che, per il loro contenuto o per il tempo trascorso dal momento della loro raccolta, non abbiano più rilevanza pubblica».

La richiesta di ottenimento del provvedimento di oblio deve pervenire tramite segnalazione della vittima al Garante per la Protezione dei Dati Personali, secondo quanto disposto dall'articolo 144 del Codice della *privacy* e dell'articolo 33 bis regolamento n. 1/2019 del Garante.

³²⁰ MANNA L., "*Diritto all'oblio, le ripercussioni in Italia della Pronuncia Google Spain: primi provvedimenti del garante della privacy*" Gennaio 2015

³²¹ Sentenza Corte di Giustizia 13 Maggio 2014 n. 317, la quale stabilisce che *Google* deve cancellare le informazioni inadeguate e non pertinenti, se il cittadino lo richiede, la Corte, nel caso di specie, era stata invocata dall'Audiencia Nacional di Spagna, Corte nazionale con competenze in materia penale. il ricorso di *Google* contro una decisione dell'Agencia Española de Protección de Datos (AEPD) aveva ad oggetto l'accoglimento della denuncia del sig. Mario Costeja González, che ordinava a *Google* di rimuovere i suoi dati personali dalla rete, i quali riguardavano un'asta di immobili relativa ad un pignoramento per riscossione coattiva di crediti previdenziali.

³²² Regolamento Generale sulla protezione dei dati (UE/2016/679)

³²³ Cass. Ordin. N. 7559/2020

Nel 2021 è stato anche introdotto l'articolo 144 bis, il quale dà la possibilità della vittima di effettuare segnalazioni al Garante o reclami, se ha il fondato sospetto che sia stata diffusa una sua immagine esplicita senza consenso.

Per impedire la diffusione ulteriore di questo materiale³²⁴, se il Garante ritiene fondata la richiesta, emette un provvedimento entro quarantotto ore.

La segnalazione avviene tramite la compilazione di un modulo *online* fornito dal Garante, che deve specificare l'oggetto della richiesta di rimozione, la piattaforma social su cui è stato condiviso il contenuto illecito e le motivazioni.

Grazie a questo sistema di recente introduzione, le segnalazioni dal 2022 al 2023 sono aumentate a dismisura, infatti rispettivamente i casi di intervento del Garante sono duecentosessanta quattro contro i cinquantuno dell'anno precedente; nel 2023 si è anche riscontrato un aumento del 7% di vittime di sesso maschile³²⁵.

Il Garante, una volta ricevuta la richiesta di oblio, la valuterà e la trasmetterà al motore di ricerca, chiedendone la rimozione.

In merito, Tiziana Cantone aveva fatto richiesta di un provvedimento d'urgenza per la rimozione del materiale che la riguardava, ma il legislatore non le ha riconosciuto questo diritto.

Quest'ultimo, ai fini di una semplificazione della procedura di rimozione, ha introdotto una fase propedeutica all'attuazione del diritto all'oblio³²⁶: la procedura di deindicizzazione.

Per dare maggiore rilievo a questa pratica, nel 2017 è stata aggiunta una ulteriore procedura a tutela della persona offesa, che si chiama *'notice and put down'*, introdotta dalla legge n. 71/2017 all'articolo 2, mediante quest'ultima, se si ricerca il contenuto per parole chiave, il contenuto, che è stato oscurato, non sarà più disponibile.

Per "indicizzazione" si intende l'inserimento, all'interno di un sito o in un motore di ricerca, di una notizia; di conseguenza, il sito comparirà tra i primi quando gli utenti cercheranno sul motore di ricerca delle parole o frasi che sono correlate all'argomento. La procedura ha ad oggetto la richiesta dell'interessato, indirizzata al motore di ricerca, di rimozione di ogni riferimento alla propria persona sul sito, in relazione al contenuto dannoso collocato sulla rete.

Successivamente, solo in caso di mancata accettazione da parte del *provider* della richiesta, la vittima in ultima istanza può rivolgersi al Garante o all'Autorità Giudiziaria.

Se verrà accettata, il fornitore del servizio provvederà alla rimozione, tuttavia, la cancellazione non è immediata e di contro, le informazioni potrebbero ancora circolare sul sito.

³²⁴ Garante per la Protezione dei dati personali, provvedimento 5 agosto 2022, n. 9811771, registro dei provvedimenti n. 283 del 5 agosto 2022

³²⁵ Dati presi dalla ricerca del sole24ore, 21 dicembre 2023, articolo di Bianca Lucia Mazzei *"Revenge porn: gli stop decisi dal garante quintuplicati nel 2023"*

³²⁶ vedi IASELLI M., *"Il diritto all'Oblio: un giusto diritto che non può essere riconosciuto"*, Gennaio 2018

L'articolo 8 della Carta dei diritti fondamentali si pone a tutela del principio di protezione dei dati, stabilendo che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano».

Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge.

Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica».

Tuttavia, secondo un recente provvedimento del Garante della Privacy³²⁷, nel caso in cui il richiedente del provvedimento di oblio sia accusato di reati gravi, per i quali la vicenda giudiziaria sia di interesse pubblico e sia da poco conclusa, allora non può essere avviata la procedura.

Il provvedimento riguardava un terrorista che aveva pianificato un attacco (per il quale il soggetto ha scontato due anni di carcere), quest'ultimo chiedeva la rimozione di testate giornalistiche derivanti da fonti qualificate.

Considerando ciò, il Garante ha ritenuto infondata la richiesta di deindicizzazione per detenzione di materiale che faceva riferimento ad Al-Qaida.

Il diritto all'immagine: una duplice tutela – il risarcimento danno e l'azione inibitoria

Fondamentale è anche definire uno dei diritti che si trova alla base della disciplina tutelata dall'articolo 612 ter: il diritto all'immagine.

Infatti, la diffusione di immagini o video sessualmente espliciti senza il consenso della vittima rappresenta un vero e proprio momento di intimità che viene violato, e con la divulgazione si arreca un danno all'immagine, in quanto quest'ultima viene considerata come espressione di una libera sessualità; una sessualità denigrata dal perpetratore del reato a causa di una sua volontà generale di prevaricazione³²⁸.

È regolato dall'articolo 10 GDPR, ma è prevista anche una tutela mediante risarcimento del danno, all'articolo 2043 cc³²⁹, con la funzione non solo di sopperire alla riduzione della capacità economica derivante dalla diffusione illecita di immagini, quindi porre rimedio alla *deminutio patrimonii*, ma anche riportare la vita del soggetto passivo il più possibile simile a come era *ante* illecito.

Ulteriore tutela viene conferita dal Codice civile all'articolo 10, che istituisce la cessazione della condotta lesiva e l'ordine di non reiterazione della stessa, in relazione

³²⁷ Prov. n. 204/2023, 17 maggio 2023, Garante della Privacy, doc. n. 9903127

³²⁸ FLORIO F., “*Non chiamatelo Revenge porn, storie di vittime presunte colpevoli*”, Mondadori, 2022

³²⁹ il diritto al risarcimento segue, nel nostro codice, il principio di tipicità, sancito anche dall'art. 185 del Codice penale, il quale afferma: “Ogni reato obbliga alle restituzioni, a norma delle leggi civili.

Ogni reato che abbia cagionato un danno patrimoniale o non patrimoniale obbliga al risarcimento il colpevole e le persone che, a norma delle leggi civili, debbono rispondere per il fatto di lui”

alla tutela del nome, dello pseudonimo e dell'immagine e in generale per la tutela dei diritti rientranti nell'ambito dell'identità personale.

Come abbiamo fin qui analizzato, fondamentale per la formazione dell'illecito, è l'assenza di consenso della persona offesa, ciò viene considerato come elemento imprescindibile anche dagli articoli 96 e 97 della legge 633/1941 che riguarda il diritto d'autore.

Il Codice civile del 1942 definiva all'articolo 10 recitava «Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni».

Da ciò si evince che, altro elemento fondante ai fini del rispetto del diritto all'immagine, non è solo la mancata accettazione della vittima, ma anche il pregiudizio che viene arrecato alla reputazione.

In merito, il suddetto articolo 97 introduce al comma secondo, un ulteriore limite che riguarda il "pregiudizio al decoro o alla reputazione della persona": si afferma che il ritratto non può essere esposto o messo in commercio se questi comportamenti arrecano pregiudizio all'onore alla reputazione o al decoro della persona trattata.

Per le modalità di prestazione dell'assenso, si richiama una sentenza della Corte di Cassazione «il consenso alla pubblicazione della propria immagine costituisce un negozio unilaterale, avente ad oggetto non il diritto, personalissimo ed inalienabile, all'immagine, che in quanto tale non può costituire oggetto di negoziazione, ma soltanto l'esercizio di tale diritto.

L'accettazione, pertanto, sebbene possa essere occasionalmente inserita in un contratto, resta tuttavia distinta ed autonoma dalla pattuizione che lo contiene, con la conseguenza che esso è sempre revocabile, quale che sia il termine eventualmente indicato per la pubblicazione consentita.

A prescindere dalla pattuizione del compenso, che non costituisce un elemento del negozio autorizzativo in questione, stante la natura di diritto inalienabile e, quindi, non suscettibile di valutazione in termini economici rivestita dal diritto in discussione (Cass. 3014/2004)»³³⁰.

Perciò, secondo la legge sul diritto d'autore, l'unico caso in cui sarebbe possibile derogare al diritto alla tutela della propria immagine e alla riservatezza è l'interesse pubblico prevalente.

È necessario fare riferimento oltre che al danno patrimoniale, anche al danno morale subito dalla vittima le cui immagini vengono diffuse³³¹ (definito dalla Corte come il turbamento psicologico del soggetto leso³³²): viene regolato dall'art.1 lett. b) del d.p.r.

³³⁰ Cass. Pen. n. 1748/2016

³³¹ Corte di Cassazione n. 8177/1994

³³² Corte Cost. n.184/2006

30.10.2009 n.81, che lo definisce come il «pregiudizio non patrimoniale costituito dalla sofferenza soggettiva cagionata dal fatto lesivo in sé considerato».

Esso trova la sua *ratio* nell'ingiusto, seppur momentaneo, turbamento dello stato d'animo, a seguito della violazione della *privacy* subita.

Il Giudice potrà ricorrere a una valutazione degli effetti, riferendosi a criteri circostanziali: come la sofferenza psichica ottenuta, lo stato di turbamento ecc.³³³, e dovrà motivare il percorso logico alla base della sua decisione.

Il danno non patrimoniale è tutelato dall'articolo 2059 cc, riconoscendo la tutela ai diritti personali costituzionalmente garantiti e che non vengono considerati danno patrimoniale.

Secondo un filone di Dottrina³³⁴, la quantificazione del danno morale viene individuata in base al danno biologico³³⁵.

Tuttavia, non sempre nel reato di diffusione illecita di immagini sessualmente esplicite, quest'ultimo viene ad esistenza, rendendo quindi il compito del Giudice di determinare il *quantum* della offesa arrecata, molto difficile.

La Giurisprudenza invece, ritiene che il *quantum* del danno e il danno biologico, siano autonomi, per questo il soggetto leso dovrebbe provare la sofferenza morale causata dalla condotta illecita³³⁶.

Anche la Suprema Corte si è espressa in tal senso, «il danno non patrimoniale da lesione di diritti fondamentali, “quale tipico danno-conseguenza”, non coincide con la lesione dell'interesse (ovvero non è *in re ipsa*)³³⁷.

Pertanto, deve essere allegato e provato da chi chiede il relativo risarcimento, anche se, trattandosi di un pregiudizio proiettato nel futuro, è consentito il ricorso a valutazioni prognostiche ed a presunzioni sulla base di elementi obbiettivi che è onere del danneggiato fornire»³³⁸.

Il diritto all'immagine rientra anche in quei diritti per i quali può essere richiesta l'azione inibitoria.

Quest'ultima è una forma di tutela, nella quale si richiede la cessazione della condotta lesiva mediante l'emissione del provvedimento di inibitoria, che contiene il divieto di reiterazione della condotta.

L'onere probatorio deve pervenire da chi ha subito il danno.

Oltre all'inibitoria può essere richiesto un altro provvedimento cautelare, che è molto comune per il reato all'articolo 612ter, in quanto vengono sequestrati i materiali e gli

³³³ ROSSETTI M., *Il danno da lesione della salute*, CEDAM, 2001.

³³⁴ PENTA A., *Il danno morale, Danno e Resp.*, 2017, 1, 115.

³³⁵ dlgs n. 209/2005 definisce il danno biologico “lesione temporanea o permanente dell'integrità psico-fisica della persona, suscettibile di valutazione medico legale, che esplica un'incidenza negativa sulle attività quotidiane e sugli aspetti dinamico relazionali della vita del danneggiato, indipendentemente da eventuali ripercussioni sulla sua capacità di produrre reddito”.

³³⁶ Cass.n. 14846/2007

³³⁷ T.A.R. Roma, Sez. I, 15/10/2018, n.9984, Cass. n. 7471/2012, Cass. 10527/2011, Cass. 20558/2014, Cass. n. 13614/2011

³³⁸ Cass. Civ., sez. I, 16/04/2018, n. 9385/2018

oggetti che potrebbero contenere elementi di prova, come i *computer*: si tratta del sequestro giudiziario.

Tramite quest'ultimo il Giudice si assicura di preservare tutto ciò che potrebbe essere fonte di prova, togliendo il bene dalla disponibilità del soggetto, prima che ci sia una decisione di merito che accerti la mancanza di consenso alla diffusione delle immagini.

3.0 (segue): Casi Giurisprudenziali - risoluzione degli episodi di *Revenge porn* nella prassi

Il 22 febbraio 2023 si tenne l'udienza per la prima pronuncia di legittimità della Corte di Cassazione sull'articolo 612 ter c.p.

Il caso di specie aveva ad oggetto una donna molestata e minacciata ripetutamente dal suo ex amante (tanto da esser costretta a bloccare il numero di telefono di lui): quest'ultimo non ha retto la fine della loro relazione, dichiarava di voler raccontare tutto alla famiglia di lei (condotta poi successivamente messa in atto).

Ha avuto un comportamento persecutorio anche nei confronti dei figli, inviandogli messaggi ripetuti su *Facebook*, compresi insulti e foto della madre a contenuto sessualmente esplicito, mandandole anche a una amica della donna.

A causa di ciò la vittima, come si legge dal testo della sentenza, ha dovuto modificare radicalmente le sue abitudini di vita andando a vivere dalla madre e interrompendo il vincolo coniugale con l'altro uomo.

Alla fine, decise di sporgere querela nei confronti dell'ex amante.

L'uomo viene indagato dal Tribunale di Latina per reato di atti persecutori articolo 612 bis e diffusione illecita di immagini sessualmente esplicite articolo 612 ter c.p., quest'ultimo verrà poi condannato all'esito di giudizio abbreviato per entrambi i reati.

Alla stessa conclusione aderisce la Corte d'Appello di Roma mediante sentenza, avverso la quale poi l'imputato ha proposto ricorso.

La Corte, in merito all'ambito applicativo della fattispecie, analizza vari aspetti: anzitutto si chiede se possa esser ritenuto integrato il reato mediante l'invio a una singola persona del materiale illecito, essendo in via generale più volte verificatasi il delitto in questione mediante la diffusione "virale" del contenuto (per il quale si ritiene ci sia un maggior disvalore).

Questo argomento si trova alla base dello schema difensivo dell'imputato, poiché la difesa sosteneva che l'invio al figlio dell'immagine e all'amica presupponesse la certezza che questi non avrebbero ulteriormente diffuso l'immagine.

Tuttavia, sono anche molti i casi per i quali l'invio è mirato ad una singola persona o a specifiche persone, in modo da creare uno specifico danno, e questo è il caso di specie (si pensi per esempio all'invio della immagine al datore di lavoro³³⁹).

³³⁹ casistica DI D.K. CITRON, *Hate crimes in Cyberspace*, Cambridge Massachusetts-Londra, 2014, 56 ss.

Si è riflettuto anche se la condotta integri il comma secondo dell'articolo 612 ter, ritenendo presente quindi la finalità di arrecare nocumento alla persona, e se la foto in questione (che rappresentava la donna a seno nudo) potesse essere considerata sessualmente esplicita.

Già in questo primo caso, emerge la finalità, nella maggior parte dei casi presente, di vendicarsi della vittima e della volontà di generare un grave e perturbante stato di ansia con le condotte ripetute di atti persecutori, ma viene confermato anche dall'ambito nella quale viene ricompresa questa condotta, ossia la violenza di genere³⁴⁰, andando a includere anche il sotto-insieme della violenza domestica³⁴¹.

Proprio grazie a questo episodio, ci si è resi conto che è lecito ritenere congrua la scelta del legislatore di inserire il reato di *Revenge porn* nei delitti contro la libertà morale, proprio dopo il reato di atti persecutori, al fine di sottolineare lo stretto contatto fra le due fattispecie.

Infatti, non è stato oggetto di appello da parte della difesa, il riconoscimento della continuazione fra i due reati ex articolo 81 cp.

Durante il ricorso effettuato contro la sentenza di Appello, la difesa eccepisce la generale carenza del quadro indiziario a suo carico, soprattutto per il reato oggetto d'esame, in quanto non è d'accordo con la scelta del legislatore di primo grado, di non considerare valida la perizia effettuata sui dati informatici telefonici per verificare l'effettiva esistenza di questi messaggi inviati ai figli e alla amica dell'ex amante, poiché non la considerava una prova integrativa.

Per questo, non si ritiene neanche rispettata la presunzione all'articolo 533 del cod. di proc. pen. (secondo argomento avanzato dalla difesa) secondo cui «Il giudice pronuncia sentenza di condanna se l'imputato risulta colpevole del reato contestatogli al di là di ogni ragionevole dubbio».

Infatti secondo la difesa, le uniche prove contro il loro assistito sarebbero le dichiarazioni della vittima (poiché il telefono era stato distrutto dal marito e il figlio

³⁴⁰ PECORELLA C., *Violenza di genere e sistema penale*, in *Dir. pen. proc.*, 2019, 1181 ss.; CEDU Volodina c. Russia, 9 luglio 2019, e Volodina c. Russia (n. 2), 14 settembre 2021, sentenza che definisce la divulgazione non consensuale di immagini intime come una forma di “violenza contro le donne”. Per un commento delle due pronunce, ELÖSEGUI M., *The Case Law of the European Court of Human Rights on Violence Against Women and the Intimate Image Abuse*, in G.M. CALETTI, K. Summerer (a cura di), *Criminalizing Intimate Image Abuse. A comparative perspective*, Oxford, 2023 (in corso di pubblicazione). La comunità Europea ha previsto una proposta di direttiva, in particolare della Commissione europea (dell'8 marzo 2022) con il fine di combattere la violenza di genere e rendere più armonica la legislazione degli Stati membri. Fondamentale l'art. 7 che prevede che gli Stati debbano garantire l'incriminazione delle condotte di diffusione di immagini intime, anche manipolate. In proposito, si veda l'approfondito commento di RIGOTTI C., C. MCGLYNN, *Towards an Eu criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse*, in *New Journal of European Criminal Law*, 2022, vol. 13(4), 452 ss.

³⁴¹ BERTOLINO M., *Violenza e famiglia: attualità di un fenomeno antico*, in *Riv. it. dir. proc. pen.*, 2015, 1710 ss.; BRASCHI S., *La nozione di “violenza domestica” tra tutela dei diritti umani e sistema penale*, in *Criminalia*, 2022, anticipato su disCrimen, 3 luglio 2023.

aveva immediatamente cancellato la foto, mentre l'invio all'amica era stato effettuato dalla sorella della vittima e non direttamente dall'imputato), non considerate precise e attendibili.

I motivi del ricorso vengono definiti come inammissibili e quindi manifestamente infondati, poiché si ritiene che durante tutto il procedimento di primo e secondo grado, le prove addotte al giudice siano di tipo dichiarativo e tutte coerenti tra loro.

I Giudici della Corte d'Appello chiariscono inoltre che la persona offesa viene ritenuta attendibile anche grazie all'assenza di interesse economico all'accusa, non essendosi costituita parte civile.

Inoltre, si ritiene che la stessa richiesta posta dalla difesa nel ricorso, ammetta l'oggetto del reato, quindi l'invio ai figli del suddetto materiale.

Perciò, la condotta messa in atto dall'imputato integra il reato di atti persecutori, per le evidenti manifestazioni di molestia e pressione attuati dal ricorrente.

Si ritiene presente anche la volontà di arrecare un male ingiusto, considerato come la rivelazione della relazione extra coniugale al marito e ai figli, al fine di danneggiare espressamente la persona offesa.

In conclusione, è integrato l'articolo 612 ter, grazie al verificarsi di anche solo una condotta censurata nell'articolo in questione³⁴².

All'imputato viene riconosciuta l'attuazione del reato di diffusione illecita di immagini a sfondo sessuale, senza il consenso della vittima, avendo ricevuto le immagini direttamente da quest'ultima nell'ambito di un rapporto sentimentale, ponendo in essere la condotta divulgativa "verso chiunque".

La norma oggetto d'esame, infatti, comprende anche l'invio a una singola persona, non essendo necessaria quindi, ai fini della condotta diffusiva, la viralità del contenuto.

Questo perché, l'articolo 612 ter non fa riferimento a una quantificazione della portata divulgativa, ma si considera reato già dal primo invio ad un destinatario, indipendentemente dal rapporto che intercorre tra i due.

È stata quindi riconosciuta la finalità di arrecare nocumento, concretizzatasi nella volontà di arrecare un danno alla reputazione e nella volontà di vendetta.

È quindi configurabile secondo la Corte la presenza del dolo specifico³⁴³.

Il Tribunale di Siena nel 2023³⁴⁴ ha emesso una sentenza rilevante per la disciplina in esame: il caso riguardava due imputati, i quali accordandosi hanno deciso di filmare la persona offesa durante un rapporto sessuale con gli stessi, senza il suo consenso.

Il video era poi stato mostrato successivamente, mediante la diffusione del video agli amici tramite *whatsapp*, con l'aggravante di aver commesso il fatto con strumenti informatici o telematici.

Con questa sentenza il Tribunale ha voluto affermare alcuni principi di diritto:

³⁴² Cfr. Cass. Pen. Sez V 43085/2015 A. Rv 265231

³⁴³ Cass. Pen. Sez. V, sent. n. 654/2023 in *Sistema Penale*

³⁴⁴ Tribunale di Siena, sezione penale in composizione monocratica, 18 dicembre 2023 n.771

Innanzitutto, il reato di diffusione di immagini a sfondo sessuale all'articolo 612ter non è integrato, se, in caso di rapporti sessuali con più persone, le immagini o i video vengano inviati da un soggetto facente parte dell'atto sessuale ad un altro, sempre partecipante all'atto, con il fine di mantenerli privati.

Inoltre, la condotta oggetto di esame, ossia quella del "mostrare" il video ad un numero determinato di persone, non rientra nell'alveo delle condotte previste dal legislatore per l'integrazione del reato, bensì rientra nella fattispecie di diffamazione.

Ancora, il Tribunale sottolinea che non si può ritenere applicabile neanche il reato di interferenze nella vita privata (articolo 615bis).

Infatti, la fattispecie non è integrata se l'immagine o il video è stato girato in una abitazione in cui la presenza dell'imputato è ritenuta lecita oppure se questi ultimi riguardino immagini di vita privata tra cui atti sessuali, in quanto il reato all'articolo 615bis ha ad oggetto la condotta di un terzo, estraneo al domicilio, che viola l'intimità della persona offesa.

La sola assenza di consenso alla registrazione del video o dell'immagine non è sufficiente per ritenere integrato il reato di *Revenge porn*, perché ai fini del perfezionamento della fattispecie, è richiesto l'assenza di consenso alla divulgazione dell'immagine o video sessualmente esplicito.

Recentemente a Verona, si è verificato un episodio per cui alcuni ragazzi, atleti, che facevano girare foto e video delle loro compagne mentre si cambiavano nello spogliatoio, in una *chat whatsapp* di gruppo che in realtà aveva lo scopo di comunicare gli avvenimenti e gli orari degli allenamenti.

Sotto inchiesta anche l'allenatore, sollevato successivamente dall'incarico, il quale invece di incitarli a interrompere questo tipo di condotta, commentava le foto delle ragazze.

In merito a ciò sono state aperte tre inchieste, tra cui una di tipo militare, poiché l'allenatore faceva parte dell'esercito, per violazione degli articoli 2 del codice di comportamento sportivo del Coni e articolo 6 dello Statuto Fisi, ovvero i doveri di rettitudine, e una sportiva per i quali si è arrivati a una sentenza³⁴⁵.

Tra i dodici sotto accusa (fra questi anche minorenni), sei sono stati scagionati a causa del fatto che erano solo presenti nella *chat*, per questo non hanno commesso un illecito sportivo (infatti si legge dalla sentenza che il Tribunale ritiene che la mera partecipazione passiva non fosse rivolta alla diffusione di materiale pornografico ma aveva principalmente scopi "goliardici" e informativi sull'attività di gruppo, e quindi per questi non si ritiene integrata la condotta in esame).

Mentre, altri quattro sono stati ammoniti, due squalificati a causa della loro partecipazione attiva alla diffusione di contenuti illeciti anche di ragazze minorenni e senza il loro consenso.

³⁴⁵ Trib. Federale, n. 117/2024, procedimenti riuniti 001-002/2023

Uno dei ragazzi in particolare, viene proprio aggiunto alla *chat* con lo scopo di inviare foto intime delle ragazze, e come si legge dal quotidiano nazionale, uno dei presidenti della Federazione Fisi commenta «Familiare questa».

Vengono inviati anche dei video, in particolare uno dall'allenatore, di una ragazza inquadrata di schiena mentre si allena.

Quest'ultimo allegato al video aggiunge il commento «Io ho fatto la mia parte oggi», la *chat* contiene anche l'album fotografico di una ragazzina seminuda.

Un messaggio emblematico della gravità della faccenda viene inviato dall'allenatore nel momento in cui la questione diviene di pubblica conoscenza, questo, lasciando la *chat* scrive: «A me fa piacere che siete affamati di f... e non siate una manica di fr..., malati buonisti pro neg..., comunisti ed ebrei.

Detto questo penso capiate che la mia presenza nel gruppo è un po' borderline. Io esco, meglio evitare possibili casini. Tranquilli non ce l'ho con nessuno. Finiamo bene le gare e poi andiamo a fare caccia grossa».

La divulgazione di fotografie in biancheria intima delle ragazze, avvenuta senza consenso è sufficiente per ipotizzare l'attuazione del reato previsto all'articolo 612 ter. Il procuratore sostituto Gabriele Pezzano individua sia la presenza della violazione di quest'ultima fattispecie, ma anche per alcuni, la diffusione di messaggi con riferimenti al fascismo e all'odio razziale.

A tutti i partecipanti alla conversazione, contesta l'aggravante «per aver agito per motivi futili e per aver cagionato una lesione della dignità delle atlete, l'immagine dello sport e della Fisi».

Tuttavia, il Tribunale ha riconosciuto le attenuanti, al pari delle aggravanti, poiché i soggetti che hanno condiviso fotografie di intimo hanno prontamente riconosciuto il carattere inadeguato della loro condotta e si sono scusati con le atlete e con la Federazione, cercando di attenuare le conseguenze del reato.

Il Tribunale ha escluso la responsabilità del Presidente e del vicepresidente della Federazione, poiché questi si sono attivati immediatamente per rimuovere l'allenatore dall'incarico.

Il presidente del *club* ha commentato dicendo che i ragazzi "non si sono resi conto" della gravità del fatto.

Questo episodio conferma nuovamente quanto il reato di diffusione illecita di immagini a sfondo sessuale venga preso sottogamba e considerato "meno grave" dalla maggior parte dei perpetratori, solo perché l'utilizzo dello strumento informatico altera la percezione offensiva del reato.

Vendendo alla sentenza oggetto di esame, il Tribunale Federale ha ritenuto la condotta di detenzione delle immagini come assorbita dalla più grave fattispecie di diffusione di queste ultime.

Inoltre, gli imputati hanno violato anche l'articolo 58 lettera d del Regolamento di Giustizia Fisi per aver cagionato un danno alla dignità delle atlete coinvolte e violato le norme che riguardano la rettitudine sportiva, dato anche il mancato rispetto degli obblighi di lealtà, correttezza, non violenza e non discriminazione.

Tuttavia, specifica il Tribunale, che le sanzioni disposte nei confronti degli atleti sono state commisurate all'attività concretamente svolta da ognuno di essi.

Famoso è anche il Caso di Dalia Aly, ora ventenne, vittima del fidanzato che ha deciso di pubblicare un loro video *hard*, a seguito di cui ha subito anche bullismo dai suoi, all'epoca dei fatti, compagni di classe; infatti, in quel momento la vittima aveva quindici anni.

Il video era stato divulgato tramite *Telegram* e gira ancora in rete; tuttavia, Dalia non si è potuta avvalere delle tutele conferite dal Codice Rosso in quanto i fatti sono avvenuti nel 2018, quindi sono precedenti all'entrata in vigore di quest'ultimo, ma rientrano pienamente nella fattispecie oggetto d'esame.

Dalia fa presente che nel periodo in cui è stato divulgato il contenuto, doveva essere in lizza per essere eletta rappresentante di istituto del suo liceo.

Ciò mette in luce la volontà di ridicolizzazione e umiliazione ma anche il fine di vendetta perpetrata dall'ex, tipico della condotta di *Revenge porn*.

In una intervista la ragazza spiega «Il mio è proprio un caso di condivisione non consensuale di materiale intimo, ma ho potuto solo denunciare contro ignoti, esponendo i fatti e senza indicare un particolare capo d'accusa.

Ho scoperto che il mio ex fidanzato aveva avuto lo stesso comportamento con altre ragazze di Cosenza, con lo stesso copione: fingeva amore per convincere le fidanzate a farsi filmare e diffondere i video tra gli amici.

Io e le altre siamo state usate solo per questo scopo³⁴⁶». Gli anni seguenti Dalia ha proseguito la battaglia legale, la denuncia per *Revenge porn* è stata presentata nel dicembre 2018; quattro anni dopo il processo è ancora in corso.

Oggi, si è rivolta a un centro antiviolenza di Cosenza grazie al quale è venuta in contatto con una psicoterapeuta e un avvocato.

4.0 (segue): La fattispecie negli ordinamenti stranieri - Come viene regolamentato il *Revenge Porn* all'estero?

L'Inghilterra non è l'unico Stato estero che ha deciso di criminalizzare la condotta di diffusione illecita di immagini sessualmente esplicite e le procedure sono alquanto diverse considerando i singoli ordinamenti.

Molti sono gli Stati che hanno deciso di introdurre una disciplina *ad hoc*, come gli Stati Uniti, Germania, Israele, Regno Unito, Francia, Giappone, Australia e molti altri.

³⁴⁶ Intervista a “*La Stampa*”, 11 gennaio 2022

L’Australia, di recente, si è appositamente dotata di un ente pubblico per la vigilanza di *internet*: l’*Esafety Commissioner*, autorità indipendente di natura amministrativa istituita nel 2015 dall’*Enhancing Online Safety Act*³⁴⁷.

Quest’ultima, ha il compito di sensibilizzare l’educazione dei giovani in materia, spiegando come comportarsi sulla rete per evitare determinate situazioni legate all’abuso delle immagini *online*, ma si occupa anche della ricerca per la prevenzione di questi reati.

Il primo Paese che si è dotato di una legislazione apposita è stata la Repubblica delle Filippine inserendo una pena di reclusione che va dai tre ai sette anni, con l’ “*anti photo and video voyeurism act*³⁴⁸” del 2009.

Anche San Marino ha introdotto, a tutela delle persone offese da diffusione illecita di questi contenuti, una proposta di legge da parte dei Giovani Democratici Cristiani (GDC), la cui disciplina è molto simile a quella italiana, prevede infatti una pena per coloro che creano e diffondono il contenuto, di reclusione dai sei mesi ai due anni e una sanzione che può raggiungere anche i dieci mila euro.

A differenza del nostro sistema, si introduce una attenuante se il soggetto attivo ha esclusivamente diffuso il contenuto senza produrlo, mentre in comune con l’articolo 612ter è l’introduzione di una aggravante in caso di relazione affettiva con la vittima, di donna in stato di gravidanza o di vittime con infermità psichica o fisica.

Sul fronte comunitario, nel 2022 è stata portata dalla Commissione Europea una proposta di legge sulla violenza di genere³⁴⁹, al fine di armonizzare le normative degli Stati Membri.

All’articolo 7 di suddetta proposta viene riportato il caso di “condivisione non consensuale di materiale intimo o manipolato” (comprendendo anche la fattispecie del *deep fake*).

L’articolo enuncia che Gli Stati membri provvedono affinché siano punite come reato le condotte intenzionali seguenti: primariamente, quella di rendere accessibile a una pluralità di utenti finali, tramite tecnologie dell’informazione e della comunicazione, immagini, video o altro materiale intimo ritraente atti sessuali di un’altra persona senza il suo consenso.

³⁴⁷ Testo consultabile sul “*Federal Register of Legislation; Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992*”, in *communications.gov.au*, 15.2.2020

³⁴⁸ Republic Act n. 9995/2009 Il voyeurismo, nella sua veste digitale, si è servito di vari strumenti, tra cui le “*wireless spy cameras*”, ma anche di strumenti di *hacking*, spesso utilizzati in dispositivi elettronici di persone, famose o meno, al fine di rubare materiali intimi. Secondo quest’ultimo, sono punite le condotte che abbiano ad oggetto foto o video di natura sessuale che siano stati ripresi senza il consenso della persona coinvolta e in circostanze nelle quali questa abbia una ragionevole aspettativa di privacy. Sono dunque punite la materiale ripresa, la copia o la riproduzione, la vendita o la distribuzione, la pubblicazione o la diffusione, la esposizione o la esibizione, così come aver agevolato le precedenti condotte.

³⁴⁹ Proposta di direttiva del Parlamento Europeo e del Consiglio, sulla lotta alla violenza contro le donne e alla violenza domestica. Strasburgo, 8.3.2022 COM (2022) 105 final 2022/0066 (COD)

La seconda condotta prevista è quella di produrre o manipolare e successivamente rendere accessibile a una pluralità di utenti finali, tramite tecnologie dell'informazione e della comunicazione, immagini, video o altro materiale in modo da far credere che un'altra persona partecipi ad atti sessuali, senza il consenso dell'interessato.

Infine, quella di minacciare i comportamenti di cui alle lettere a) e b) al fine di costringere un'altra persona a compiere un determinato atto, acconsentirvi o astenersi dallo stesso.

L'anno presunto di entrata in vigore di questa normativa è il 2025/2026.

La collocazione di questo reato nella proposta contro la "violenza di genere"³⁵⁰ viene anche supportata dalla Giurisprudenza, in particolare le sentenze Cedu Volodina vs. Russia del 2019 e del 2021 la quale individuano il reato di diffusione illecita di immagini sessualmente esplicite come una forma di violenza contro le donne³⁵¹.

La Corte di Strasburgo, nel caso di specie, ha sottolineato l'importanza dell'obbligo per gli Stati facenti parte della Convenzione di garantire un sistema che preveda una effettiva punizione per i perpetratori dei crimini di violenza domestica, commessi sia *offline* che *online*, introducendo altresì un meccanismo di effettiva protezione per le vittime, condurre indagini consapevoli nei casi di violenza e prevenire il rischio di trattamenti inumani.

La Corte inoltre, in questa sentenza, ribadisce come la Russia non sia dotata di sistemi di protezione per le vittime di violenza, come per esempio, ordini di allontanamento

³⁵⁰ ROMANO B., A. Marandola (a cura di), Codice Rosso. Commento alla L. 19 luglio 2019, n. 69, in materia di tutela delle vittime di violenza domestica e di genere, Pisa, Pacini Giuridica, 2020

³⁵¹ caso n 1. 41261/2017 decisione finale nel 2019; caso n 2. 40419/2019 decisione finale nel 2021.

I casi hanno ad oggetto il ricorso della signora Volodina, che ha denunciato l'ex marito per aver subito nel corso degli anni varie violenze fisiche, minacce e molestie, oltre che per *Revenge porn*.

Vi è stato l'accertamento della violazione da parte delle autorità russe dell'art 3 della Cedu (divieto di tortura e trattamenti inumani) e dell'articolo 14 (divieto di discriminazione) dell'articolo 8 (diritto al rispetto della vita privata) all'unanimità, riconoscendo alla vittima un equo risarcimento secondo l'articolo 41 della Cedu. Le autorità russe non avevano in alcun modo punito il perpetratore né protetto l'incolumità della vittima. Il soggetto attivo aveva utilizzato foto intime e dati personali di Volodina per creare un profilo falsi *su social network*, aggiungendo tra gli amici anche l'insegnante e i compagni di classe di suo figlio. L'inchiesta dalle autorità russe venne aperta solo dopo due anni, poiché il giudice russo eccepiva la sua incompetenza territoriale e la mancanza di un illecito. Secondo la Corte, la legge russa è venuta meno all'obbligo di una previsione di tutela per le vittime di violenza domestica in quanto non esiste alcuna misura di prevenzione attuabile dalla legge russa. La corte EDU è arrivata a questa decisione anche mediante l'utilizzo di fonti internazionali, come le conclusioni del Comitato della Convenzione sull'eliminazione di ogni forma di discriminazione della donna (CEDAW *Committee's conclusion*) in cui si afferma che il divieto di violenza di genere fa parte del diritto internazionale consuetudinario. La Corte ha anche utilizzato come fonte il report dello *Special Rapporteur on Violence against Women* a seguito della sua missione in Russia nel 2004; Yuri Colombo, "Russia, «la violenza di genere non esiste»", Il Manifesto, 22 novembre 2019

dell'aggressore, ma che anzi, avrebbe continuato a permettere che queste violenze si verificassero, e non è l'unico caso per cui ciò è avvenuto³⁵².

Il legislatore Europeo auspica alla creazione di una disciplina unica che possa fronteggiare il fenomeno del *Revenge porn*, date le grandi differenze che ci sono fra gli ordinamenti.

4.1 (segue): La criminalizzazione negli Stati Uniti

Il *Revenge porn* negli Stati Uniti è un fenomeno che ha iniziato a prendere piede a partire dal 2010 grazie ai Mass Media e alle autorità giudiziali, a causa della comparsa di siti *online* che incentivavano il caricamento di contenuti e foto private di donne senza il loro consenso³⁵³.

La disciplina è molto complessa e variegata e manca di uniformità per quanto riguarda la sua categorizzazione e lo scopo, a seconda dello Stato a cui si fa riferimento.

Per alcuni andrebbe catalogato in quei reati detti "*result crimes*" (come ha fatto il Colorado nel 2014 categorizzandolo come oscenità) i quali richiedono un danno determinato al fine della configurazione del reato, altri invece, come il Kansas, lo collocano come un "*conduct crime*" facendo allusione esclusivamente alla condotta posta in essere³⁵⁴.

Molti studiosi inseriscono il *Revenge porn* all'interno degli "*hate Crimes*"³⁵⁵ a causa dei molti elementi che questi crimini hanno in comune, come per esempio l'accessibilità dei materiali senza limiti di tempo o spazio, l'anonimato degli autori e la correlazione ai dati personali della vittima (tutelati anche dall'articolo 5 della Dichiarazione dei Diritti di *Internet*).

Al momento sono quarantasette gli Stati che hanno introdotto una apposita legislazione³⁵⁶, con l'auspicio del legislatore americano di introdurre una legge federale unitaria che possa criminalizzare queste condotte.

³⁵² Causa Buturga vs Romania, ric n. 56867/15, 11 febbraio 2020, nel caso di specie una cittadina rumena aveva denunciato l'ex marito per violenza domestica, oltre che per accesso abusivo sui suoi account, tra cui quello di Facebook, averla stalkerata via web e aver acquisito immagini e dati. Il Tribunale di primo grado aveva applicato una misura "restrittiva" che sarebbe durata sei mesi, ma che i giudici di Strasburgo hanno definito poco efficace.

³⁵³ FRANKS M.A., "*Revenge Porn*" Reform: *A View from the Front Lines*, 69 FLA. L. REV. pag. 1255

³⁵⁴ COFFEY G., "*Codifying the Meaning of 'Intention' in the Criminal Law*" October 2009 *Journal of Criminal Law* 73(5):394-413; 73(5):394-413

³⁵⁵ D.K. CITRON, *Hate Crimes in Cyberspace*, Cambridge Massachusetts, 2014

³⁵⁶ (tra questi, per completezza, vi sono: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Massachusetts, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, West Virginia, Washington, Wisconsin, Wyoming) *Nonconsensual Pornography Laws*, Cyber CIV. RTS. INITIATIVE

Nonostante la presenza di parte della Dottrina americana che critica questa volontà ipotizzando una contrarietà con il primo Emendamento della Costituzione³⁵⁷, il quale sancisce il principio di libera manifestazione del pensiero, per il divieto per il Congresso di emanare leggi contrarie a quest'ultimo, altra parte della Dottrina considera il contenuto dell'immagine o video che viene divulgata senza consenso come una lesione limitata alla riservatezza del singolo individuo, non della collettività³⁵⁸.

Sul tema si è interrogata anche la Dottrina italiana, ritenendo che il principio di libera manifestazione di pensiero, che tutela in via generale la libertà di espressione³⁵⁹ senza avere alla base un rapporto tra mittente e destinatario, non possa ledere il diritto alla non diffusione illecita delle proprie immagini sessuali, tutelato dall'articolo 612ter poiché si ritiene che la divulgazione non sia una condotta che ha alla base un pensiero giuridicamente rilevante e quindi tutelabile³⁶⁰.

Tornando al tema oggetto d'analisi, secondo parte della Dottrina americana, affinché possa il *Revenge porn* esser riconosciuto come reato di matrice sessuale a tutti gli effetti (*sex offence*) si dovrebbe considerare la violazione dell'autonomia della vittima come interesse fondamentale da proteggere; quindi, potrebbe essere giustificabile una espansione dei confini del reato, anche a costo di violazione del "*freedom of speech*". Per alcuni Stati, infatti, al fine di ovviare a una violazione del primo Emendamento, andrebbe considerato il dolo specifico della diffusione delle immagini come elemento fondante della *mens rea* (elemento psicologico del crimine).

In alternativa, questo potrebbe essere valutato come conseguenza del danno, facenti quindi parte dell'*actus reus*, con lo scopo di ridurre al minimo la possibilità di intrusione alla libertà di pensiero³⁶¹.

La maggior parte degli Stati aderiscono alla prima ipotesi, mentre per alcuni è sufficiente il dolo eventuale.

Secondo la Dottrina³⁶², in particolare John Humbach, professore della facoltà di Legge della Pace University, il problema potrebbe venir meno mediante l'attuazione di una legislazione che non si riferirebbe espressamente al *Revenge porn*, ma agli effetti derivanti da esso, come il disagio emotivo provocati da quest'ultimo.

³⁵⁷ Snyder v. Phelps, 562 U.S. 443, 458 (2011) "The government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable"

³⁵⁸ HUMBACH "the constitution and revenge porn" in Pace Law Review 2015 vol 35,1, 202 ss.

³⁵⁹ PACE A. – M. MANETTI, *Rapporti civili. Art. 21 – La libertà di manifestazione del proprio pensiero*, in BRANCA G. (a cura di), *Commentario della Costituzione*, Bologna: Zanichelli, 2006, 11.

³⁶⁰ LOTTA C., *Prime osservazioni sul rapporto tra il reato di "Diffusione illecita di immagini o video sessualmente espliciti" e le libertà di corrispondenza e di manifestazione del pensiero*, 1 luglio 2019, Fasc. II.

³⁶¹ ROSEMBERG R., HADAR DANCIG-ROSEMBERG, *Journal of constitutional law: "Revenge Porn in the shadow of the First Amendment"*

³⁶² vedi KOPPELMAN A., *Revenge Pornography and First Amendment Exceptions*, 65 EMORY L. J. 661, 684- 90 (2016) (quest'ultimo sostiene che il *Revenge porn*, essendo una situazione che potrebbe produrre effetti e danni collaterali a livello mentale, non dovrebbe essere considerato come rientrante nella libertà di pensiero)

In questo modo, sarebbe possibile perseguire chi diffonde la foto o il video sessualmente espliciti, infrangendo solo in via incidentale e non direttamente, la libertà di pensiero.

Il suo punto di vista è stato ampiamente criticato, poiché è sì possibile identificare come elemento fondamentale della condotta incriminata, l'effetto particolarmente gravoso sulla vittima, ma ciò non lo differenzia dagli altri reati di tipo sessuale; e questo porterebbe alla violazione del principio fondamentale delle leggi Americane, del "*fair labeling*"³⁶³.

Tuttavia, nel 2016 è stata portata all'attenzione del Congresso una proposta: *Intimate Privacy Protection Act (IPPA)* 204³⁶⁴, la quale avrebbe ad oggetto la previsione di una legge federale: questa porrebbe rimedio anche al problema, radicato, di impunità dei *provider* (tranne per il tema del diritto d'autore).

Negli Stati Uniti questi soggetti detengono una vera e propria protezione; tuttavia, quest'ultima verrebbe meno in caso di crimini federali.

La differenza fra i vari Stati può essere ravvisata sia da un punto di vista contenutistico, in base alla gravità della condotta, ma anche in base al trattamento punitivo.

Nel sistema statunitense i crimini si dividono in tre categorie: *felonies*, *misdemeanors*, *infractions*: alcuni Stati, come per esempio l'Alabama e l'Arizona, caratterizzano il *Revenge porn* come "*felony*" ossia un crimine punito con la reclusione a non meno di un anno oppure la pena di morte (negli Stati in cui è ancora presente), altri, come l'Alaska e il Colorado, lo considerano un "*misdemeanor*" cioè una offesa punibile solo con una multa o un breve periodo di detenzione nelle carceri locali, altri ancora lo ritengono una mera invasione di *privacy*³⁶⁵.

In ogni caso, molte vittime non riescono a portare la causa in Tribunale a causa degli elevati costi, e come si evince da uno studio condotto dalla *Yale University*, il caso dovrebbe essere aperto con i nomi reali delle vittime, ma molte non vogliono esporsi a tale risonanza³⁶⁶.

Facendo riferimento alla diversità di criminalizzazione, un caso che ritengo sia importante citare è accaduto nello Stato di *New York*, di recente infatti, la Corte ha archiviato le accuse contro un uomo a seguito della pubblicazione di contenuti sessualmente espliciti della sua ex ragazza su X³⁶⁷, e dell'invio degli stessi alla sorella e al datore di lavoro.

La *ratio* del legislatore si trova nel sostenere che l'uomo non aveva inviato le foto di nudo a lei stessa ma ad altri.

³⁶³ CHALMERS J., LEVERICK F., *Fair Labelling in Criminal Law*, 71 MOD. L. REV. 217 (2008).

³⁶⁴ FRANKS A.M., "*Revenge porn*" reform, cit., 1256; BURRIS A., *Hell hath no fury like a woman porned: revenge porn and the need for a federal nonconsensual pornography statute*, in *Florida Law Review*, 2014, vol. 66, 2325 ss.

³⁶⁵ Del. Code Ann. tit. 11, § 1335(a)(9) (2017); S.D. Codified laws § 22-21-4 (2021)

³⁶⁶ CITRON D.K., FRANKS M.A., *Criminalizing Revenge Porn*, 2014, documento consultabile sul sito dell'Università

³⁶⁷ *People v. Barber*, 42 Misc.3d 1225(A) N.Y. Crim. Court. Feb 2014

Nello Stato in questione, infatti, non costituirebbe una violazione di legge sulle molestie il pubblicare su siti terzi questo tipo di contenuti, in quanto mancherebbe un diretto contatto con la vittima³⁶⁸, a differenza di molti casi della stessa fattispecie avvenuti qui in Italia e condannati a seguito dell'articolo 612ter.

Il soggetto in questo caso è stato condannato per molestie aggravate ed esposizione in pubblico di materiale sessuale offensivo. Camala Harris, nel novembre 2017, con il supporto dei più importanti social network come X e Facebook, ha voluto introdurre il "*Ending nonconsensual online user graphic Harassment (ENOUGH) Act*"³⁶⁹ sia presso il Senato che alla Casa Bianca, il quale fornirebbe la possibilità di portare davanti a un Tribunale Federale la condivisione di immagini esplicite senza il consenso.

Gli unici Stati che prevedono una espressa criminalizzazione del *Revenge porn* sono: New Jersey, California, Alaska, Texas, Virginia, mentre altri Stati hanno proposto dei "*Revenge porn Bills*"³⁷⁰.

Tra questi, il sistema penale a cui vorrei dare maggiore rilevanza è quello del New Jersey, il quale è stato il primo Stato a criminalizzare questo reato, nel 2004 all'interno del *New Jersey Law Criminal Justice*, nel Title 2C207 (New Jersey Code of criminal justice).

L'articolo prevede³⁷¹ che il soggetto attivo commette un reato di terzo grado se, sapendo di non avere la licenza o il privilegio di farlo, fotografa, filma, registra (caso non letteralmente considerato dal legislatore italiano, ma per il quale si potrebbe applicare l'articolo 612ter per analogia delle condotte previste) o riproduce in altro modo l'immagine di un'altra persona le cui parti intime sono esposte o che è impegnata in un

³⁶⁸ DONAGHUE E., *Judge Throws Out New York Revenge Porn Case*, CBS (Feb. 25, 2014, 4:42 PM),

³⁶⁹ SCHOR E., *Lawmakers target 'revenge porn' in bipartisan bill*, Politico (Nov. 28, 2017)

³⁷⁰ atto normativo dei paesi di *common law* che non ha concluso l'iter di approvazione, può essere istituito da ogni membro dello *U.S. Congress* (Congresso degli Stati Uniti d'America) per cui sia dai membri dello *U.S. Senate* (Senato degli Stati Uniti d'America) che dalla *U.S. House of Representatives* (Camera dei rappresentanti degli Stati Uniti d'America): l'iniziativa può provenire sia dagli stessi membri del Congresso, dal governo federale o da singoli individui o gruppi privati. I *bills* federali in America possono essere denominati *private bills* riguardanti singoli individui o società e *public bills*, validi per l'intera collettività o a determinate categorie di persone. Per maggiori informazioni in merito: Libreria online dell'università di Melbourne consultabile al sito University of Melbourne Library "United States of America Law, introduction to federal legislation", Jen. 2025

³⁷¹ «An actor commits a crime of the third degree if, knowing that he is not licensed or privileged to do so, he photographs, films, videotapes, records, or otherwise reproduces in any manner, the image of another person whose intimate parts are exposed or who is engaged in an act of sexual penetration or sexual contact, without that person's consent and under circumstances in which a reasonable person would not expect to be observed. An actor commits a crime of the fourth degree if, knowing that he is not licensed or privileged to do so, he photographs, films, videotapes, records, or otherwise reproduces in any manner, the image of the undergarment-clad intimate parts of another person, without that person's consent and under circumstances in which a reasonable person would not expect to have his undergarment-clad intimate parts observed.» New Jersey Statutes Title 2C. The New Jersey Code of Criminal Justice 2C § 14-9 Amended by L.2016, c. 2, § 1, eff. May 5, 2016; DEL VECCHIO, K., *New Jersey's code of criminal Justice, a practical guide*, 2025

atto sessuale, senza il consenso di quella persona e in circostanze in cui una persona ragionevole non si aspetterebbe di essere osservata.

La particolarità di questa fattispecie è specificata alla lettera D, che enuncia il principio secondo cui viene considerato consentito dalla legge, se il contenuto venga pubblicato con uno scopo legittimo, oppure se la vittima era stata preventivamente avvisata della volontà di pubblicare il contenuto specificato alla lettera a,b,c,e.

La pena prevista è pecuniaria: trenta mila dollari di sanzione.

All'interno della norma viene anche chiarito il significato di "*disclose*", visto il suo significato molto ampio, definendolo come dare, fornire, prestare, commerciare, consegnare, trasferire, pubblicare, distribuire, far circolare, condividere o rendere disponibile tramite l'uso di *internet* o con qualsiasi altro mezzo, sia a scopo di lucro che non.

Di recente, il governatore del *New Jersey Andrew Cuomo* ha approvato una legge che categorizza il *Revenge porn* come una "*Class A misdemeanor*", introducendo anche varie novità: la possibilità di agire anche civilmente nei confronti del perpetratore e la facoltà del Giudice di richiedere alle piattaforme su cui il contenuto è stato pubblicato, la rimozione del contenuto stesso dal sito, come avviene anche in Italia, tramite il procedimento di deindicizzazione.

Secondo quanto definito dal *New York Post*³⁷², alcune aziende capeggiate da *Google* hanno sostenuto che questa nuova disciplina contrasterebbe con il "*Communication Decency Act*", atto federale che esclude una qualsivoglia responsabilità del sito *web* per il contenuto immesso da terzi.

Il giornale chiarisce però che non si tratta di una volontà di ascrivere la responsabilità al *social network*, ma di permettere al giudice di richiedere la rimozione del *post*.

Tuttavia, molti ritengono che i rimedi attuali non siano sufficienti a dare una tutela completa, sebbene in molti Stati possa anche essere oggetto di denuncia civile, per richiedere risarcimento danno, ma questo non protegge la vittima da una eventuale ricondivisione futura e non garantisce la rimozione della fotografia dal *web*.

Il processo di rimozione, infatti, può essere molto lungo e insidioso, come mostra anche la serie *Netflix "The most hated man on the Internet"*, dove una donna si batte per far rimuovere le foto della figlia da un sito di *Revenge porn*, lanciando una campagna *online* contro il fondatore.

³⁷² *New York Post*, By Post Editorial Board pubblicato il 24 luglio 2019

4.2 (segue): La Criminalizzazione in Germania e Francia: i casi più rilevanti

La Germania si è dotata di una normativa anti *Revenge porn* nel 2014, la quale istituisce la pena della reclusione fino a due anni e multa fino a sessanta mila euro.

Precedentemente a questa disciplina, le controversie relative alla diffusione di immagini a sfondo sessuale venivano regolate solo sul piano civile, con una legge che riguardava il *copyright*.

Di recente però nella città di Coblenza, nella Germania Centrale, la Giurisprudenza tedesca ha fatto scalpore per una sentenza³⁷³ per la quale si imponeva all'ex partner di una donna di cancellare le sue foto intime alla fine della relazione, anche se l'imputato non aveva nessuna intenzione, a detta della difesa, di divulgarle online.

Il divieto comprendeva: foto svestita, foto parzialmente svestita con zone intime visibili, con biancheria intima, prima dopo o durante il rapporto sessuale, mentre tutte quelle foto che non la ritraggono in atteggiamenti intimi sono rimaste in possesso dell'accusato e non rientrano nell'ordine di cancellazione.

Si legge nella sentenza, infatti, che la Corte statuisce la possibilità per la persona offesa di revocare il consenso dato per la produzione delle immagini.

Gli argomenti della difesa riguardavano la violazione del principio alla "libertà artistica" in quanto l'accusato era un fotografo professionista; tuttavia, questo principio non si ritenne violato, a fronte di un bilanciamento con i diritti di *privacy* e autodeterminazione della persona offesa.

Secondo Mayer-Schönberger, professore di *Internet Governance and Regulation* alla Università di Oxford «La sentenza di Coblenza non riguardava la protezione dei dati, ma il "diritto alla propria immagine", che è una costruzione speciale della Giurisprudenza dell'Europa continentale, [...] ma ciò che si può dire è che queste due sentenze potrebbero rendere sempre più persone consapevoli dei propri diritti personali nella sfera digitale.

Come minimo, dovrebbero incoraggiare i futuri ricorrenti che vogliono prevenire in modo proattivo il *Revenge porn*»³⁷⁴.

Il consenso, quindi, può anche essere revocato dopo anni rispetto alla produzione della fotografia.

Invece, In Francia venne introdotto l'articolo 226 nel loro Codice penale, poi di recente modificato con decreto n. 247/2024, il quale punisce quelle condotte di trasmissione o diffusione di immagini video di carattere sessuale di una persona senza il suo consenso, consenso che invece era presente al momento della registrazione del contenuto.

In comune con l'articolo 612 ter c'è l'aggravante per fatti commessi a danno di un minore, o commessi da un parente o coniuge o persona legata sentimentalmente, le pene sono aumentate fino a due anni con multa di sessanta mila euro.

³⁷³ 20 Maggio 2014 (Az 3 U 1288/13), Il terzo senato civile del Tribunale Distrettuale Superiore di Coblenza (Oberlandesgericht)

³⁷⁴ Intervista su *The Guardian*, Philip Oltermann, 22 maggio 2014

Quest'ultimo aumento viene ricompreso anche per il caso in cui i fatti vengano commessi nei confronti di un Pubblico Ufficiale, incaricato di pubblico servizio o titolare di un pubblico mandato elettivo.

Questo è proprio quello che è avvenuto, in un recente caso del 2020, al candidato politico *Benjamin Griveaux* che ha subito quello che oggi si definisce "*shitstorm*" ossia una pioggia di insulti, minacce di morte e commenti offensivi, tale da doversi ritirare come candidato a sindaco di Parigi.

Una ex amante del politico avrebbe diffuso le immagini intime della vittima mandandole all'artista russo *Pyotr Pavlensky*, il quale dopo averle ricevute, le avrebbe pubblicate in un portale *online* pornografico³⁷⁵.

L'obiettivo dell'artista era di denuncia politica: colui che si dimostrava molto attivo nel supporto alle famiglie, che aveva moglie e figli, aveva anche una amante.

In migliaia hanno condiviso queste foto sui social, senza che ci fosse una smentita da parte del politico sulla attuale veridicità di quei contenuti, commentando con insulti di ogni tipo.

A conseguenza di ciò, risulta esiguo il numero di condanne rispetto alle denunce presentate nello stesso anno, secondo quanto riporta Juliette Sanchez-Lambert.

L'ex amante e l'artista sono stati sottoposti a processo a giugno davanti il Tribunale Penale di Parigi, al termine dell'udienza la pubblica accusa ha chiesto sei mesi di reclusione per entrambi, la pena dell'artista è poi stata ridotta ed è stato sottoposto all'uso del braccialetto elettronico.

Secondo quanto riporta un articolo di giornale molto conosciuto in Francia³⁷⁶, risulta che da uno studio statistico attuato dall' SSMSI, il servizio statistico Ministeriale per la sicurezza interna, le violazioni della privacy di natura sessuale avrebbero portato solo a poco più di tremila vittime nel 2020, questo a causa delle difficoltà del sistema giudiziario francese ad affrontare questo problema, molte volte, infatti, i casi vengono sminuiti dai giudici.

³⁷⁵ Cfr. GINORI A., "*Il candidato di Macron a Parigi spazzato via da un video porno*", in *la Repubblica*, 14 febbraio 2020.

³⁷⁶ Le journal du Dimanche, 27 giugno 2023, Articolo di Cecile de Seze. Condannati l'11 ottobre 2023.

4.3 (Segue): Come viene trattato il *Revenge porn* in Spagna? Evoluzione normativa ed esperienze giurisprudenziali

In Spagna l'evoluzione normativa si è verificata nel 2015, attraverso la modifica dell'articolo 197 comma settimo del c.p. il quale prevede la reclusione da tre mesi a un anno (in forma alternativa alla sanzione pecuniaria, infatti in alternativa si può agire in sede civile con un procedimento sommario che è più veloce) chi, senza autorizzazione diffonda, riveli o dia a terzi immagini o riprese audiovisive presso il domicilio o qualsiasi altro posto al di fuori della vista di terzi, quando la diffusione leda gravemente l'intimità della persona.

Questa fattispecie sembrerebbe richiamare i cosiddetti secondi distributori, per i quali il legislatore italiano dedica il secondo comma dell'articolo 612 ter: si riferisce quindi a quelle persone che una volta ricevuto il contenuto registrato da terzi, si occupano di diffonderlo.

Nella normativa spagnola viene espressamente definito il fine di arrecare nocumento, e quindi il dolo specifico, tramite la precisazione "quando la diffusione lede gravemente l'intimità della persona", tuttavia questa espressione potrebbe risultare fuorviante per tutti quei casi, comunque meritevoli di tutela, dove il legislatore non ritenga che possa essere lesa in modo molto grave l'intimità del singolo, sarebbe quindi di difficile quantificazione.

Il primo comma invece fa riferimento ai primi distributori: la pena comprende la reclusione da uno a quattro anni per coloro che registrano, trasmettono o diffondono immagini private senza il consenso della persona.

Inoltre, viene mantenuta, al comma quinto, l'aggravante di pena se il reato viene commesso nei confronti di minori o di una persona con particolare vulnerabilità.

Mentre, alla fine del comma settimo viene citata l'aggravante che riguarda i fatti che vengono commessi da un coniuge o persona legata da relazione affettiva, ma si aggiunge, rispetto alla normativa italiana, la fattispecie secondo cui i fatti avrebbero finalità lucrativa.

L'articolo 197 criminalizza anche altre tipologie di reati, legati alla scoperta e alla divulgazione di segreti attraverso *Internet* e altri mezzi tecnologici di comunicazione, come la ricezione di messaggi di posta elettronica "senza consenso".

Nel 2022 la Corte Suprema spagnola ha precisato che nella modifica rientra non solo la nudità totale, ma anche quella parziale: «il diritto alla *privacy* è leso quando la foto mostra la nudità completa della persona interessata, ma anche se fosse parzialmente nuda, purché si riferisca a zone intime come il torso completamente nudo»³⁷⁷.

Tuttavia, la normativa spagnola *ante* modifica, non era molto efficace sul piano repressivo, in quanto risultava sproporzionata rispetto alla gravità delle condotte poste in essere.

³⁷⁷ Corte Suprema n 699/2022, 11 luglio

Nel 2022 la *Ley Organica* n. 10 ha revisionato completamente il sistema dei delitti contro la libertà sessuale, ponendo l'attenzione su una unica definizione di aggressione sessuale non distinguendola dall'abuso sessuale, più ampia della precedente, ricomprendendo ogni atto di tipo sessuale verificatosi senza il consenso della vittima³⁷⁸. Più nel dettaglio, la Riforma interviene sia dal punto di vista repressivo e di contrasto alla violenza di genere, ma anche preventivo, potenziando lo sviluppo economico e la ricerca, si impegna anche a definire in maniera più precisa, a livello normativo, il consenso, come «atti che, con riferimento alle circostanze del caso, esprimano in maniera chiara la volontà della persona»³⁷⁹.

L'anno dopo, con una successiva *Ley Organica* il legislatore spagnolo ha voluto regolamentare i limiti edittali di pena modificati dalla riforma del 2022, attribuendo alla "violación" una pena da sei a dodici anni.

Un caso che ha fatto scalpore in Spagna per la mancanza di una adeguata tutela e che ha poi portato alla necessità di una maggiore criminalizzazione del *Revenge porn*, attraverso un inasprimento di pena, come è avvenuto anche nel caso di Tiziana Cantone, è stato quello di *Olvido Hormigos*³⁸⁰.

Una donna, si è suicidata a Madrid a seguito della diffusione fra i suoi colleghi di lavoro di un suo video intimo; *Hormigos* ha sporto denuncia davanti al Giudice per violazione della sua intimità, tuttavia quest'ultimo ritenne che non potesse configurarsi suddetta violazione poiché per essere tale, l'accusato avrebbe dovuto accedere al suo telefono per rubargli il video, cosa che non è accaduta perché è stata proprio lei a inviare il video all'accusato.

Il giudice, *María del Carmen Neira*, ha indetto l'archiviazione provvisoria e l'archiviazione del procedimento contro i due imputati: un calciatore accusato della diffusione del video, e il sindaco di *Los Yébenes*, *Pedro Acevedo*, con il quale la donna aveva avuto una relazione, esonerandoli da un delitto contro la *privacy*.

³⁷⁸ DE URBINA GIMENO I.O., Adesso davvero hispanica societas delinquere non potest, *Criminalia*, 2010

³⁷⁹ MERENDA I., *La "ley del solo sí es sí": la controversa riforma dei delitti contro la libertà sessuale nell'ordinamento spagnolo. Spunti per il legislatore italiano?* Archivio Penale 2024, n.1

³⁸⁰ FERNÁNDES O., DELGADO L., "El nuevo delito contra la intimidad en el proyecto de reforma del Código Penal de 2013 y el "caso Olvido Hormigos". En: *Revista de Derecho y Proceso Penal*. 2014, núm. 35, pp. 183-220. ISSN 1575-4022. P. 184.

4.4 (Segue): La criminalizzazione in Giappone

Nel 2014 Il Giappone tramite il “*Diet*”, la Camera dei consiglieri giapponese, ha voluto criminalizzare con una proposta di legge la condotta di *Revenge porn*, mediante il “*Revenge Porn Victimization Prevention Act*” cioè “Legge per la prevenzione dei danni causati dalla distribuzione di immagini sessuali private” il quale prevede fino a tre anni di reclusione o una multa di cinquecento mila *yen*, per chi diffonde immagini senza il consenso della persona interessata, di carattere sessuale.

In merito alla diffusione, è importante sottolineare la distinzione che la normativa fa tra delitto di divulgazione e delitto di offerta con l'intento di divulgazione: con quest'ultima si intende l'atto di consegna di immagini sessuali o video attraverso un circuito di comunicazione elettronica oppure l'indurre altre persone a commettere delitto di divulgazione; questa condotta è punibile con un anno di reclusione e multa fino a 300.000 *yen*³⁸¹.

La legge in questione prevede anche la criminalizzazione della conservazione e della circolazione di suddette fotografie, ma anche il ritocco di immagini volto a far sì che la persona sembri coinvolta in atti sessuali.

In seguito alla sua entrata in vigore, è stato condannato un uomo per aver posto una telecamera nei bagni pubblici e aver condiviso i video, ripresi di nascosto, su un sito di intermediazione vendite, violando così la suddetta normativa per la prevenzione del *Revenge porn*, quindi anche per questa fattispecie, come in Italia per il caso portato all'attenzione del Tribunale di Reggio Emilia nel 2021 (*Infra*, § cap. 2 par. 2.2), la normativa è applicabile, pur non trattandosi di un ex partner o una persona vicina alla vittima, bensì uno sconosciuto.

La fattispecie si riferisce anche ai minori, punendo anche chi riprende dei bambini in pose sessuali allusive; precedentemente, queste condotte seguivano la legge sul disturbo della quiete pubblica.

Altra novità di questa riforma, è l'aumento dell'età del consenso dai tredici ai sedici anni, considerando che il Giappone è uno dei paesi facenti parte del G7 con la soglia dell'età del consenso più bassa in assoluto.

Uno degli ultimi casi di *Revenge porn*, che ha fatto più scalpore, ha riaperto i riflettori su questo reato portando all'introduzione di una nuova legge per la quale si prevede la possibilità dei *service provider* di cancellare le immagini che si pensa siano legate a questo tipo di reato, pubblicate *online* senza il consenso dei soggetti ritratti.

Inoltre, oltre che dal punto di vista normativo, novità vengono anche dall'uso della tecnologia: molto innovativa infatti è la volontà di Tokyo di installare un *software* in grado di bloccare a monte la possibilità dei possessori di *smartphone* di scattarsi foto intime compromettenti, ai fini di prevenire un possibile danno.

³⁸¹ Legge Giapponese sulla prevenzione del *Revenge porn*, Articolo 3, Paragrafo 3, “Legge per la prevenzione dei danni causati dalla distribuzione di immagini sessuali private”, Monolite law office, 2024

Già nel 2020 *Tone Mobile*, azienda che produce cellulari, aveva pensato di immettere sul mercato un telefono che potesse rilevare grazie all'Intelligenza Artificiale (*Infra*, § cap. 3 parag. 2) la presenza di parti intime nelle foto e bloccarle prima dell'invio, eliminandole direttamente dalla galleria, perché comparirebbe “errore di messaggio”. Ciò ha suscitato non poche polemiche nella popolazione: essi si interrogano su chi debba decidere cosa viene ritenuto censurabile e cosa no, tornando di nuovo al problema relativo alla libertà di pensiero.

Sono state anche introdotte, come si voleva fare in Italia con il Codice Rosso, iniziative rivolte ai giovani e programmi nelle scuole per informare i più a rischio, sui pericoli di queste pratiche³⁸².

Un'altra differenza fondamentale con il sistema italiano, è che in caso di contenuti che ledano la reputazione della persona, come il reato in esame, non avviene una procedura di deindicizzazione.

Gli unici abilitati, secondo la legge giapponese, a rimuovere pagine *web* o *post* con contenuti diffamatori, sarebbero gli avvocati; coloro che non hanno qualifiche legali, o persone giuridiche come le aziende, non ne hanno la facoltà.

Aspetto in comune fra i due sistemi è il collegamento con il reato di diffamazione: infatti secondo l'articolo 230 del Codice penale giapponese, si può essere accusati anche di diffamazione se si pubblicano o sono già state pubblicate, immagini o video a carattere sessuale verso un numero indeterminato di persone, con una condanna a pena detentiva fino a tre anni.

Secondo il Rapporto della National Police Agency nel 2022 il numero dei casi di *Revenge porn* in Giappone è salito a 1.728 casi, ottenendo un incremento del 20%³⁸³.

³⁸² SHIMBUN Y., via Otakomu; Articolo di Giornale su Japan Today, maggio 2021, Cristina Gauri; Articolo di giornale su *Japan Times*

³⁸³ report completo visualizzabile al link

https://www.npa.go.jp/bureau/safetylife/stalker/R4_STDVRPCAkouhousiryoku.pdf

CAPITOLO III – COME L'INTELLIGENZA ARTIFICIALE PUO' INSINUARSI NEL REATO DI REVENGE PORNOGRAPHY – NUOVE PROSPETTIVE APPLICATIVE DI PREVENZIONE E MODALITA' DI COMMISSIONE DEI REATI

SOMMARIO

1. Intelligenza Artificiale – nozioni generali e normative applicabili 2. AI come mezzo di prevenzione e repressione dei reati - applicabilità al *Revenge porn* 3. AI come mezzo di commissione dei reati

1.0 (segue): – Intelligenza Artificiale – nozioni generali e normative applicabili

Una necessaria premessa

Come per il primo capitolo, prima di procedere ad analizzare in che modo l'Intelligenza artificiale potrebbe essere utilizzata nell'ambito dei reati contro la persona, in particolare nel reato di *Revenge porn*, sia dal punto di vista di commissione del reato, che preventivo, ritengo sia necessario precisare il significato dell'Intelligenza artificiale e spiegare i suoi albori, al fini di costruire un cappello introduttivo alla ricerca oggetto d'esame.

Innanzitutto, mi occuperò di identificare come l'Unione Europea, attraverso i suoi atti, ha dato una definizione a questo nuovo strumento, in particolare, gli organi che si sono occupati di più del tema sono la Commissione Europea e il Parlamento Europeo.

Nei prossimi paragrafi spiegherò come viene regolato dal punto di vista legislativo questo nuovo sistema automatizzato di gestione dei dati, cogliendone sia i lati positivi che negativi ed evidenziando anche i rischi per i diritti dei cittadini, specificatamente mettendo in luce le problematiche che comporterebbe per i diritti fondamentali, il diritto alla privacy e la sicurezza dei propri dati.

Scenderò nel dettaglio descrivendo il periodo storico nel quale l'Intelligenza Artificiale si è sviluppata, le modalità, le innovazioni e i pensieri di studiosi che hanno portato all'utilizzo dell'IA come noi la conosciamo.

Analizzerò accuratamente il primo Regolamento Europeo sviluppatosi sull'Intelligenza Artificiale, in modo da illustrare un quadro completo per lo studio che affronterò nei prossimi capitoli, fornendo le basi per comprendere la disciplina.

Successivamente, tratterò dell'utilizzo dell'*Artificial Intelligence* come metodo di prevenzione del verificarsi dei reati, specificatamente quelli contro la persona.

Andrò a descrivere anche tutte quelle procedure che con il tempo i grandi colossi di *Internet* hanno messo in atto per far fronte alla diffusione illecita di immagini sessualmente esplicite.

Nel terzo paragrafo, invece, mi occuperò del tema opposto: ossia di come *l'IA* possa essere utilizzata dai perpetratori al fine di commettere reati sulle piattaforme digitali, parlerò anche delle nuove sfide per le normative vigenti, per i quali c'è bisogno di una trattazione specifica, come il caso del *Revenge porn* utilizzando sistemi *Deepfake*.

Trovo necessario effettuare questa digressione anche a fronte di un sempre più crescente uso della *IA* sia nel campo lavorativo che nella vita di tutti i giorni, per questo motivo, è utile recuperare delle informazioni anche di informatica base, che servono per comprendere appieno questi sistemi molto avanzati.

1.1 (segue): *L'Artificial Intelligence* – uno strumento in rapida ascesa

L'artificial Intelligence è un ramo della *computer science*, la quale rappresenta un tema di grande interesse per la comunità scientifica, in quanto l'idea di riprodurre le caratteristiche tipicamente umane su una macchina ha da sempre affascinato l'uomo. Infatti, molte sono state anche le riproduzioni cinematografiche in merito, come il film di *Steven Spielberg* "*Ai-intelligenza artificiale*".

In Italia il mercato dell'*Ai* secondo uno studio dell'*Osservatorio Artificial Intelligence*³⁸⁴, ha avuto una crescita del 32%, anche grazie ai fondi stanziati dall'Europa con vari regolamenti³⁸⁵, tra cui uno del 2024, con cui sono stati stabiliti 3,1 miliardi di euro per la *deep tech*, tra cui l'intelligenza artificiale.

Tuttavia, prima di procedere a una introduzione sulla sua storia, bisogna prima interrogarsi sul suo significato.

L'intelligenza Artificiale (*AI*) è una tecnologia informatica attraverso cui viene simulata l'intelligenza umana, analizzando gli effetti delle azioni precedenti e le esperienze passate, per adattarsi a tutte le situazioni e risolvere quelle più complesse autonomamente³⁸⁶.

Ma esiste una definizione legislativa di questo fenomeno?

³⁸⁴ Secondo questa stima, ha raggiunto il valore di 500 milioni di euro. *L'Osservatorio Artificial Intelligence* è stato fondato nel 2017 dal Politecnico di Milano con l'obiettivo di chiarire e indagare sulle reali opportunità dell'intelligenza artificiale ed è patrocinato ad AIXIA, Associazione Italiana per l'Intelligenza Artificiale, Anitec-Assinform, Assintel, FAIR, Lab CINI.

³⁸⁵ Regolamento 2024/795, istituisce il programma denominato "Step" (*Strategic technologies for Europe platform*),

³⁸⁶ *High-Level experts Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, Bruxelles*, 8 aprile 2019, 45; definizione di IA contenuta nel documento proposto dalla COMMISSIONE EUROPEA, *Comunicazione su L'Intelligenza artificiale per l'Europa*, Bruxelles, 25 aprile 2018, COM (2018) 237 final, 1.

Il Parlamento Europeo, la definisce come «l'abilità di una macchina di mostrare capacità umane come il ragionamento, l'apprendimento, la pianificazione e la creatività³⁸⁷».

Tuttavia, la terminologia viene ritenuta "opaca", in quanto utilizzata in diversi ambiti, con significati diversi che potrebbero portare a delle incomprensioni a livello giuridico³⁸⁸.

Un decreto-legge³⁸⁹ recentemente approvato dal Consiglio dei ministri, chiarisce che l'Intelligenza Artificiale è «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve, come generare output quali previsioni, contenuti, raccomandazioni, decisioni che possono influenzare ambienti fisici o virtuali».

Mentre, sempre nello stesso decreto, i modelli di AI si illustrano come «modelli che identificano strutture ricorrenti attraverso l'uso di collezioni di dati, che hanno la capacità di svolgere una ampia gamma di compiti distinti e che possono essere integrati in una varietà di sistemi o applicazioni».

Nella quotidianità, l'AI è già presente da svariati anni, grazie alla sua utilità, basti pensare ai *software* di riconoscimento facciale o vocale, ma anche l'utilizzo di droni, veicoli autonomi con pilota automatico e molti altri.

Questi tipi di sistemi vengono spesso utilizzati nell'ambito della sicurezza pubblica, potenziando o rendendo più semplici le indagini; per esempio, il riconoscimento facciale può servire per riconoscere all'interno del sistema un ricercato le cui caratteristiche fisiche sono già note, confrontando *identikit* e informazioni.

Viene utilizzata anche in campo sanitario, soprattutto a seguito della pandemia del 2020³⁹⁰, si parla infatti di tele-medicina³⁹¹; tuttavia, il legislatore deve assicurarsi che avvenga un bilanciamento tra il rispetto del diritto alla salute e il principio di autodeterminazione del paziente, affinché le decisioni automatizzate non prendano il sopravvento³⁹².

³⁸⁷ Parlamento Europeo, 3 Settembre 2020

³⁸⁸ v. GIUFFRIDA I., LEDERER F., N. VERMEYS, *A legal perspective on the trials and tribulations of AI: how artificial intelligence, the Internet of Things, Smart Contracts, and other technologies will affect the Law*, in *Case Western Reserve Law Review*, 2018, pp. 747 ss., in specie a p. 751.

³⁸⁹ Comunicato Stampa Consiglio dei ministri n. 78, 23/04/2024, Palazzo Chigi

³⁹⁰ EUROPEAN COMMISSION, *State of Health in the EU*, Companion Report 2021

³⁹¹ Il Ministero della Salute nel 2012 ha utilizzato questo termine, coniato negli anni '70 da Thomas Bird definendolo una "modalità di erogazione di servizi di assistenza sanitaria, tramite il ricorso a tecnologie innovative, in situazioni in cui il medico e il paziente non si trovano nella stessa località. Con la Telemedicina, quindi, avviene una trasmissione sicura di dati di carattere medico tramite testi, suoni, immagini; vedi *Linee di Indirizzo nazionali sulla Telemedicina*, 10 luglio 2012, approvate dall'Assemblea Generale del Consiglio Superiore della Sanità.

³⁹² Le decisioni interamente automatizzate sono vietate dall'articolo 22 dal Regolamento n. 679/2016.

In campo medico quindi, potrebbe esser utilizzata mediante la semplificazione della ricerca medica o il rendere ancora più avanzate quelle tecnologie che permettono alle persone con delle gravi disabilità di avere un “corpo digitale”³⁹³.

Persino in ambito automobilistico l’IA ha portato grandi innovazioni, si pensi i veicoli a guida assistita³⁹⁴, ma stanno circolando anche i primi veicoli *driverless*³⁹⁵, commercializzati su ampia scala, ossia veicoli interamente guidati da un sistema di Intelligenza Artificiale.

I legislatori, sia nazionali che internazionali, si sono prontamente attivati per regolamentare questo fenomeno³⁹⁶.

L’Ai potrebbe anche essere utilizzata per scopi sociali: uno studio *McKinsey*³⁹⁷ ha considerato l’uso di questi sistemi nel sociale, dimostrando come ciò potrebbe migliorare il raggiungimento degli obiettivi di sviluppo sostenibile delle Nazioni Unite. *Microsoft*³⁹⁸ ha contribuito a questo fine, con il progetto “*Ai for Humanitarian Action*” per facilitare le azioni umanitarie nei paesi più bisognosi, oppure in caso di guerre o eventi naturali, con l’obiettivo di rispondere tempestivamente ai disastri naturali, proteggere sfollati e rifugiati e infine, analizzare le situazioni critiche per i diritti umani. L’intelligenza Artificiale è stata anche oggetto di grandi dibattiti nella letteratura, con grandi autori come Italo Calvino, il cui pensiero è stato oggetto di studio nel “*Il visconte cibernetico*”, libro che tratta della IA e delle sue implicazioni, della visione che aveva l’artista in merito e dell’evoluzione tecnologica che caratterizza questo periodo storico³⁹⁹.

In quest’opera si illustra come Calvino elabori le visioni di un possibile futuro, ragionando sul rapporto tra scrittura e tecnologia⁴⁰⁰.

Principalmente la funzione più importante è la processazione e la memorizzazione di dati, sia in ambito commerciale, per migliorare gli inventari e la logistica, sia in ambito di *cyber sicurezza*, utilizzando dati riferiti agli attacchi precedenti, per prevenirne di nuovi, ma anche per imparare a riconoscere le immagini.

L’intelligenza artificiale viene oggi utilizzata in vari ambiti della vita quotidiana: Innanzitutto di recente, *Open Ai*, fondazione *non-profit* che ha come obiettivo quello

³⁹³ FONTANA S., *I deepfake stanno diventando una cosa seria*, 10 marzo 2023, in *facta.news*

³⁹⁴ COMPOSTELLA, *Auto a guida autonoma e diritto penale. Profili di responsabilità individuale e collettiva*, Università di Trento, 2024

³⁹⁵ LIEVORE, *Self driving cars: pericoli alla prossima curva? Profili assicurativi, etici e giuridici della mobilità intelligente*

³⁹⁶ FERRARI I., *Analisi comparata in tema di responsabilità civile legata alla circolazione dei veicoli a guida autonoma*, in S. SCAGLIARINI (cur.), *Smart Roads and Driverless Cars: tra diritto, tecnologia, etica pubblica*, Torino, 2019, pp. 97 ss.

³⁹⁷ MCKINSEY & COMPANY, “*AI for social good: Improving lives and protecting the planet*”, Maggio 2024, Medha Bankhwal, Ankit Bisht, Michael Chui, Roger Roberts, and Ashley van Heteren, representing views from McKinsey Digital

³⁹⁸ Microsoft ha investito più di 115 milioni di dollari, il programma fa parte di “Microsoft, Ai for Good”, 2021

³⁹⁹ PRENCIPE A., SIDERI M.” *Il visconte Cibernetico. Italo Calvino e il sogno dell’Intelligenza Artificiale*”, 12/2023

⁴⁰⁰ MARIA CHIARA CARROZZA, curatrice della prefazione del libro di Italo Calvino

di rendere l'uso dell'*Artificial Intelligence* sicura ed etica⁴⁰¹, ha sviluppato un *software*, *Chat GPT*, in grado di simulare una conversazione con una persona in carne ed ossa, ma riesce anche a scrivere testi e generare immagini.

Questo *software* fa parte della categoria delle “*chatbot*”⁴⁰², appositamente progettati per simulare una conversazione umana.

Il formulare delle conversazioni con questo algoritmo, da una parte massimizza le probabilità di combinazioni tra parole e quindi aiuta a ripetere ogni tipo di stile linguistico⁴⁰³, dall'altra, si incorre nel problema che aveva già sottolineato Italo Calvino: l'astrattezza del linguaggio e la pochezza delle emozioni, problemi che si concretizzano con l'Intelligenza Artificiale.

Calvino diceva: «Alle volte mi sembra che un'epidemia pestilenziale abbia colpito l'umanità nella facoltà che più la caratterizza, cioè l'uso della parola, una peste del linguaggio che si manifesta come la perdita di forza conoscitiva e di immediatezza, come automatismo che tende a livellare l'espressione sulle formule più generiche, anonime, astratte, a diluire significati, a smussare tutte le punte aggressive, a spegnere ogni scintilla che sprizzi dallo scontro delle parole con nuove circostanze⁴⁰⁴».

Questo nuovo utilizzo viene chiamato Intelligenza Artificiale Generativa.

Il Garante della *Privacy*, nel 2023, ha disposto per questa applicazione, un blocco provvisorio del trattamento dei dati degli utenti italiani, a causa della perdita di informazioni sensibili che ha subito l'applicazione, violando la disciplina della *privacy* in relazione ai dati personali degli utenti.

Il Garante ha sottolineato la mancanza di comunicazione agli utenti di questo evento di *data breach* (violazione di sicurezza dei dati personali), dati che vengono raccolti da *Open Ai*, ma soprattutto mette in evidenza la mancanza di basi giuridiche che consentano la raccolta e la conservazione di una così ampia quantità di dati, per il fine di apprendimento della macchina⁴⁰⁵.

Come il Garante ha sentito la necessità di proteggere i dati personali degli utenti che utilizzano *chat GPT*, temendo quindi un imminente pericolo per il loro utilizzo illecito, così anche nella vita di tutti i giorni i cittadini temono che l'Intelligenza Artificiale possa, in futuro, superare il concetto di macchina, arrivando ad essere un pericolo per l'uomo.

Alla formazione di questa idea ha contribuito anche la grande quantità di film su questo tema, come per esempio *Odissea* nello spazio di *Stanley Kubrik*, o *A.I. Intelligenza Artificiale*.

⁴⁰¹ OpenAI ha ricevuto finanziamenti iniziali da Elon Musk e Peter Thiel, e aziende come Amazon Web Services e Infosys. Nel 2019, Microsoft ha investito un miliardo di dollari in OpenAI LP, instaurando una partnership di ricerca. Questo investimento è stato oggetto di una verifica della Commissione Europea nel 2024 per valutare l'impatto sul mercato.

⁴⁰² Termine coniato da Michael Mauldin nel 1994, che ha creato *chatbot verbot*

⁴⁰³ *Il visconte cibernetico. Italo Calvino e il sogno dell'Intelligenza Artificiale*, 2023, LUISS UNIVERSITY PRESS

⁴⁰⁴ ITALO CALVINO, “*Lezioni Americane, sei proposte per il prossimo millennio, esattezza*”, 1988

⁴⁰⁵ Roma, 31 marzo 2023, Comunicato del Garante della protezione dei dati personali

Anche *Google* ha deciso di creare una sua AI Generativa, il sistema *Gemini*⁴⁰⁶, che ha come peculiarità il fatto di potersi collegare ad altri servizi *Google*, raggiungendo un numero elevato di informazioni e dati.

In seguito, si consideri anche che i grandi colossi di *Internet*, come *Amazon*, *Google*, *Netflix* ecc. utilizzano l'AI per tenere traccia delle ricerche dell'utente, delle sue preferenze, comparandole con altri utenti in modo tale da raccomandare all'utente delle inserzioni che saranno più di suo gradimento: questo sistema viene chiamato *Recommendation System*.

L'uso dell'IA è sempre più frequente anche nei Tribunali, poiché potrebbe garantire un grado maggiore di imparzialità ed efficienza⁴⁰⁷, tuttavia ci potrebbero essere anche dei pericoli per i diritti dell'individuo⁴⁰⁸, come il rischio di discriminazione.

Anche la CGEU utilizza l'IA, tramite un sistema *NLP* per predire alcuni esiti giudiziari, mentre in Brasile la Corte Suprema utilizza un sistema in grado di ordinare i ricorsi giudiziari.

Il legislatore ritiene sia necessario l'uso di linee guida per garantire maggiore trasparenza e un utilizzo responsabile.

In Italia, la IA durante i processi non è largamente diffusa come da altre parti del mondo, inoltre viene applicata molto spesso in modo rudimentale, solo occasionalmente in modo più avanzato⁴⁰⁹.

Infatti, possiamo evidenziare il fatto che il nostro sistema Costituzionale non permette, tramite l'enunciato all'articolo 101 comma primo, che il giudice possa essere vincolato alla decisione di una macchina, definendo, che le loro decisioni sono soggette solo alla legge.

La sostituzione della decisione del giudice-persona con quella dell'Intelligenza Artificiale, in conclusione, comprometterebbe anche il diritto alla difesa, anch'esso costituzionalmente garantito⁴¹⁰.

Si specifica, inoltre, tramite l'articolo 25 della Costituzione, che durante il procedimento è assicurata la presenza del giudice precostituito per legge, riferendosi, di fatto, a una persona e non ad una macchina.

Il legislatore italiano, infatti, nutre ancora dei dubbi in relazione all'affidamento alle macchine, di compiti che richiedono il necessario apprezzamento del giudice, sia dal punto di vista strutturale, a causa di caratteristiche intrinseche e tecniche della AI, sia per ragioni di natura giuridica, sebbene in futuro il legislatore auspica a un più corretto e maggior utilizzo⁴¹¹.

Per questo, ha deciso comunque di puntare su una maggiore trasparenza delle decisioni.

⁴⁰⁶ Precedentemente si chiamava Google Bard, disponibile in Italia da luglio 2023

⁴⁰⁷ COLAPIETRO C., A. Moretti, *L'intelligenza artificiale nel dettato costituzionale*, cit., 371

⁴⁰⁸ GROPPI T., *Alle frontiere dello Stato costituzionale*, cit., 673.

⁴⁰⁹ NIEVA J., FENOLI, 2019, *Intelligenza artificiale e processo*, cit., 7

⁴¹⁰ Cfr. LUCIANI M., *La decisione giudiziaria robotica*, 2018 cit., 89 ss

⁴¹¹ Cfr. COVELLI M.L., *Dall'informatizzazione della giustizia alla "decisione robotica"? Il giudice di merito*, in A.Carleo (a cura di), *Decisione robotica*, 2019 cit., 125 ss

Per raggiungere questo obiettivo, il Presidente della Terza Sezione civile della Corte d'Appello di Bari, "ritenuto che la prevedibilità delle decisioni costituisce un valore ormai riconosciuto nel nostro ordinamento" ha istituito un progetto mediante l'uso dell'IA, con l'obiettivo di rendere accessibili ai cittadini schede online⁴¹² sulla Giurisprudenza consolidata della Sezione, su materie ricorrenti, per poter prevedere gli esiti della disciplina in questione.

Un caso molto famoso in America, il caso "Compas", riguardante l'uso della IA nei Tribunali ha suscitato molti dubbi nella Dottrina Americana.

Infatti, secondo alcuni studi, le problematiche e i pregiudizi che il cervello umano si pone possono essere anch'essi riprodotti dalla macchina⁴¹³.

Per "Compas" si intende l'algoritmo che si occupa di vagliare il rischio di recidiva e pericolosità sociale, valutando i precedenti e i dati statistici⁴¹⁴.

Nel caso di specie, un imputato era stato condannato a sei anni di reclusione, la pena era stata calcolata mediante questo *software*, le cui modalità di decisione devono rimanere segrete e non possono essere portate a conoscenza dell'imputato.

In linea generale, è avvenuta una comparazione tra le informazioni del reato dell'imputato con altri condannati con caratteristiche simili: sulla base di queste era stato considerato ad alto rischio di recidiva.

L'imputato, non conoscendo il funzionamento di questo *software*, ha fatto ricorso alla Corte Suprema del *Wisconsin*.

Nel 2016 il ricorso è stato rigettato dalla stessa Corte, confermando la legittimità della procedura e sostenendo che non si è verificata alcuna violazione del diritto a un giusto processo.

La Corte ha inoltre evidenziato che la valutazione del rischio, in ogni caso, non può scaturire solamente dal risultato ottenuto dal COMPAS, ma quest'ultimo deve essere ritenuto solo come uno dei tanti elementi che il Giudice dovrebbe prendere in considerazione ai fini di una decisione ponderata⁴¹⁵, quindi non può essere l'unico elemento determinante per il giudizio⁴¹⁶.

Questa argomentazione è stata confermata dalla Corte Suprema USA nel 2017⁴¹⁷.

Il rischio di errori o discriminazione deve, in conclusione, essere considerato come una probabilità, che può derivare da due principali problemi: in primo luogo, gli errori potrebbero essere intrinseci nelle informazioni di cui la macchina si "nutre" in fase di apprendimento (*training data*), per questo i risultati potrebbero non essere

⁴¹² Progetto "*Prevedibilità delle decisioni*", decreto 5 ottobre 2016 del Presidente della Terza Sezione civile della Corte di Appello di Bari, consultabile sul sito ufficiale della Corte d'Appello

⁴¹³ CALDERS T.-I.L. ZLIOBAITÈ, *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, in *Discrimination and Privacy in the Information Society*, Springer, 2013, 43 ss.

⁴¹⁴ SIMONCINI A., *L'algoritmo incostituzionale*, 2019 cit., 71.

⁴¹⁵ Loomis, 881 N.W.2d, 749 (Wis 2016) par. 99

⁴¹⁶ nella decisione si legge "*a COMPAS risk assessment is only one of many factors that may be considered and weighed at sentencing*"

⁴¹⁷ CELOTTO A., *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Riv. Analisi Giuridica dell'Economia*, 1/2019, 47.

attendibili⁴¹⁸; oppure l'inesattezza potrebbe derivare dall'erronea considerazione di dati statistici⁴¹⁹.

Un episodio simile a quello verificatosi in America con il sistema COMPAS, è accaduto in Italia, quando nel 2015 il Ministero della pubblica istruzione ha utilizzato un *software* per gestire una procedura ministeriale in relazione alle richieste di prima assegnazione e mobilità per quell'anno scolastico.

Molti insegnanti hanno presentato ricorso per poter conoscere i criteri di valutazione. Il TAR Lazio, ma anche il Consiglio di Stato, a differenza del caso americano, ha riconosciuto il diritto dei ricorrenti alla conoscibilità delle modalità decisionali.

Il procedimento deve essere conoscibile per rispettare il principio di trasparenza, trattandosi comunque di un atto amministrativo informatico, per il quale si riconosce la "piena conoscibilità della regola, espressa in un linguaggio differente da quello giuridico"⁴²⁰.

Sebbene l'Intelligenza artificiale possa aver portato evidenti benefici alla società, d'altro canto molti studiosi si sono interrogati sulla sua sicurezza e sulla eticità, considerando anche gli aspetti negativi, come la "deresponsabilizzazione" dell'essere umano e delle aziende, ma anche l'eventuale responsabilità in caso di danni commessi dalla AI, a causa della maggiore collaborazione tra uomo – macchina.

Le decisioni automatizzate prese dalle macchine, infatti, non sono esenti da imprevedibilità, si parla di "*unpredictable by design*" per tre motivi: *In primis*, si considera la capacità di questi sistemi di prendere decisioni indipendentemente dal fatto che le informazioni primarie siano complete o meno, completando questo *vulnus* con l'apprendimento.

In secundis, potrebbero essere generati degli *output* diversi, vista la capacità della IA di interagire con altri sistemi e venire a contatto con numerosi input.

Infine, il problema del "*black box*" cioè l'impossibilità della macchina di spiegare il ragionamento causale che sta alla base di un determinato risultato⁴²¹.

Stephen Hawking paventava il rischio che la tecnologia diventi talmente avanzata e automatizzata da migliorarsi da sola, creando una sorta di super intelligenza, con capacità che vanno al di fuori del controllo umano, infatti quest'ultimo precisa che il rischio più grande, non è la malvagità, ma la competenza⁴²².

Nel suo saggio, *Hawking* precisa «Un'AI super intelligente sarà estremamente brava a raggiungere i suoi obiettivi, e se questi non saranno allineati ai nostri, saremo nei guai».

⁴¹⁸ HACKER P., *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law*, in *Common Market Law Review*, 2018, 1146 ss.

⁴¹⁹ cfr. CALDERS T.-ZLIOBAITE I., *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, 2013

⁴²⁰ Cons. Stato, sent. n. 2270/2019, V. TAR Lazio Roma, n. 3769/2017

⁴²¹ FRAGASSO, *La responsabilità penale del produttore di sistemi di intelligenza artificiale*, in *Sistema Penale*, 13 giugno 2023

⁴²² HAWKING S., *Brief answers to big questions*, 2018

Infine, si è considerato anche l'ambito lavorativo, per il quale un eccessivo utilizzo dell'IA può portare a una sostituzione dell'uomo, in base al tipo di mansioni⁴²³.

D'altro canto, soprattutto a livello economico-statale, potrebbe essere, secondo il Parlamento Europeo⁴²⁴, un sottoutilizzo dell'Intelligenza Artificiale, rispetto ad altri paesi, creando una situazione economica stagnante e provocando una minor crescita in questo settore.

La ricercatrice *Kate Crawford*, specializzata nelle implicazioni politiche della AI, ha affermato che «L'AI non è né intelligente né artificiale. Piuttosto, l'intelligenza Artificiale è sia incarnata che materiale, composta da risorse naturali, combustibili, lavoro umano, infrastrutture, logistica, storie e classificazioni»⁴²⁵.

In conclusione, si può dire di poter descrivere l'IA in vari modi, tuttavia non si può affermare di conoscere completamente il suo funzionamento, possiamo, in via generale, parlare degli effetti, positivi e negativi, ma nel dettaglio ancora non sono chiari tutti i passaggi, questo fenomeno viene definito “oscuramento”⁴²⁶.

1.2 (segue): Come nasce l'Intelligenza Artificiale?

È opinione comune ritenere che l'Intelligenza Artificiale sia nata grazie alla conferenza del 1956 a Dartmouth College, nel quale questi due termini, Intelligenza e Artificiale, vennero associati per la prima volta.

Tuttavia, la “cibernetica” era conosciuta già nel 1947 grazie al matematico americano *Norbert Wiener*, che la definisce, nell'omonima opera, come lo studio dei processi che riguardano la comunicazione e il controllo nella macchina⁴²⁷.

Uno dei protagonisti il cui contributo è stato fondamentale ai fini della nascita di questa tecnologia è stato *Alan Turing*, che in quel periodo si interessò di questi sistemi non solo a livello teorico ma anche pratico, applicandolo nell'ambito della crittografia.

Egli ha anche parlato per la prima volta di un sistema che, embrionalmente, ricorda il concetto di *software*, tramite la macchina di *Turing*, una macchina in grado di eseguire ogni sequenza computabile.

Dopo di lui ci furono altri studiosi che arrivarono alla stessa conclusione, ossia a una macchina in grado di “pensare”, come per esempio il filosofo statunitense *Hilary Putnam*, che ha teorizzato il fatto che parole come “pensare, comprendere, vedere” (termini che indicano attività tipicamente umane) non costituiscono una facoltà di tipo spirituale ma sono azioni che anche la macchina può compiere⁴²⁸.

⁴²³ LAMBERTUCCI P., *Intelligenza artificiale e tutela del lavoratore: prime riflessioni*, in *Argomenti di diritto del lavoro*, n. 5/2022, 897 ss.

⁴²⁴ Articolo pubblicato il 29 settembre 2020 sul sito del Parlamento Europeo.

⁴²⁵ CRAWFORD K. “*Atlas of AI*”, pubblicato dalla Yale University Press, 6 aprile 2021

⁴²⁶ BRINDLE., *Nuova era oscura*, 2019

⁴²⁷ WIENER R., *Cybernetics or Control and Communication in the Animal and the Machine*, Cambridge, 1948; V. Frosini, *Cibernetica, diritto e società*, Milano, 1973.

⁴²⁸ PUTMAN. H., “*Mind, Language and reality: philosophical papers*” Cambridge Mass, 1975, pg. 291

Al contrario, il filosofo statunitense *John Searle* contrastava queste due opinioni, ritenendo che l'Intelligenza Artificiale riproduce degli atteggiamenti umani, ma non ne è l'autore, perché sono calcoli che riproduce mediante algoritmi, non ha una coscienza nel senso biologico⁴²⁹.

Negli anni a seguire, vennero sviluppati molti programmi in grado di risolvere problemi matematici, ma negli anni 70 si raggiunse una prima "crisi" a causa della riduzione dei finanziamenti per la ricerca sulla AI.

I dispositivi di ricerca a disposizione non erano molto avanzati, quindi si crearono due teorie distinte: l'Intelligenza artificiale forte, e quella debole.

La prima ipotesi riguarda il caso secondo cui la macchina sarebbe in grado di ottenere coscienza rispetto alle attività che attua, la seconda, si limita a teorizzare una risoluzione delle problematiche ma senza avere coscienza di quanto svolto⁴³⁰.

Negli anni 2000 grazie all'avanzare della tecnologia e alla sua diffusione, fu utilizzato sempre di più il *machine learning* (un sotto-insieme dell'intelligenza artificiale che si occupa di creare sistemi che utilizzano i dati per migliorare la performance) per il riconoscimento delle immagini.

Mediante quest'ultimo, si consente al *software* di adattarsi e di comprendere il compito o l'attività per il quale sono stati programmati, è quindi un metodo di apprendimento che può esser messo in atto con una supervisione didattica (tramite degli esempi l'IA capisce come comportarsi) oppure senza, tramite una analisi dei risultati.

Questi due sistemi, infatti, vanno di pari passo: una categoria del *machine learning* che viene utilizzata molto spesso in relazione alla *artificial intelligence* è il *deep learning*, un insieme di tecniche che simulano il modo in cui il cervello umano apprende delle nozioni, mediante reti neurali artificiali.

Il *deep learning*, per simulare il *modus operandi* della mente umana, deve fare uso di reti neurali artificiali progettati appositamente (*deep artificial neural networks*)

In questo modo la macchina impara autonomamente un procedimento senza il bisogno di processarne prima i dati.

Attraverso quindi il continuo apprendimento di dati la AI può prendere decisioni, senza essere preventivamente preparati per svolgere una determinata attività.

Questa autonomia, secondo la Risoluzione del Parlamento Europeo, avverrebbe indipendentemente dal controllo umano⁴³¹.

In futuro si pensa che l'AI possa continuare ad espandersi anche in altri settori rispetto a quelli utilizzati finora, con l'auspicio del legislatore di regolamentare sempre più l'uso di questi sistemi in ogni ambito.

Sono state introdotte normative europee in materia già da qualche anno: nel 2018 la Commissione si è impegnata a sviluppare progetti sulla AI, in collaborazione con le

⁴²⁹ SEARLE J., *Intentionality. An Essay in the philosophy of Mind*, Cambridge Mass, 1983 p. 312

⁴³⁰ cfr. CASONATO J., *Intelligenza artificiale e giustizia: potenzialità e rischi*, in DPCE online, 3, 2020, 3369 ss

⁴³¹ Parlamento europeo, Risoluzione del 16 febbraio 2017, 2015/2103(INL)

parti interessate all'interno della Alleanza per l'IA, formata da un gruppo di esperti, al fine di potenziare le imprese che utilizzano questi sistemi in Europa⁴³².

In questo atto non vincolante, l'Ue si impegna ad assumere un ruolo guida nello sviluppo della Intelligenza Artificiale, sulla base dei propri valori.

Inoltre, l'Europa sempre nel 2018 istituì un ulteriore Piano di Cooperazione Europeo, che costituisce una dichiarazione di intenti non vincolante, con cui gli Stati membri si impegnano a collaborare per un quadro normativo europeo più uniforme sulla Intelligenza Artificiale.

A quest'ultimo parteciparono anche Norvegia e Svizzera.

L'ultimo aggiornamento è stato previsto nel 2021; il piano mira a massimizzare i vantaggi di essere una delle prime potenze a regolamentare sulla materia, allineando la politica degli stati ed evitandone la frammentazione⁴³³.

Il fine è quello di, primariamente, implementare gli investimenti nella ricerca e nell'innovazione in modo tale da aumentare la competitività dell'Europa sul mercato in tema IA, incentivando gli sviluppi tecnologici e incoraggiandone l'adozione sia nel settore privato che in quello pubblico.

La Commissione europea si è messa d'accordo con gli Stati Uniti al fine di una collaborazione che implementi la ricerca e sfrutti il potenziale dell'intelligenza artificiale⁴³⁴.

Oltre a ciò, la Commissione stessa, ha previsto anche altre collaborazioni: quest'ultima insieme al Ministero dello Sviluppo Digitale e dell'Informazione di Singapore hanno istituito un accordo amministrativo, affinché l'Ufficio dell'UE per l'Intelligenza Artificiale e l'Istituto per la Sicurezza della IA di Singapore, cooperino, per promuovere l'innovazione e lo sviluppo antropocentrico della IA.

Quest'accordo costituisce un importante pilastro per il partenariato digitale UE-Singapore⁴³⁵.

Nel 2024 la Commissione Europea ha presentato una "comunicazione sulla promozione delle *start-up* e dell'innovazione in una IA affidabile" in vista degli ultimi sviluppi tecnologici in materia.

Questa ha il fine di ampliare la proposta originaria della stessa, nel 2021: si vuole arricchire l'ecosistema europeo innovativo di IA, collaborare con *start-up* e fornire maggiore accesso a dati e algoritmi.

⁴³² *Eu commission, communication from the commission, "Artificial Intellingence for Europe", 25.04.2018, 237 final.*

⁴³³ *"Communication from the commission to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions, "coordinated plan on artificial intelligence", COM (2018) 795 final.*

⁴³⁴ *E.U-- U.S. Research Alliance in AI for the Public Good, 5 aprile 2024, consultabile sul sito ufficiale della Commissione Europea*

⁴³⁵ *Eu and Singapore Digital Partnership, 1° febbraio 2023, documento consultabile sul sito ufficiale della Commissione Europea*

Obiettivo è anche quello di aiutare le imprese PMI ad adottare sistemi che aderiscano ai valori europei, alle normative sulla privacy e sulla protezione dei dati⁴³⁶.

Tutto ciò per il fine generale della modernizzazione dell'istruzione e fornire pari opportunità ai cittadini, preparandoli ai cambiamenti socioeconomici che risultano essere un effetto della introduzione della IA nel sistema.

Questi devono essere raggiunti rispettando, parallelamente, il un quadro etico e i valori dell'Ue ma anche un quadro giuridico adeguato.

1.3 (segue): *L'AI Act*: Il primo regolamento al mondo sull'Intelligenza artificiale

L'Unione Europea ha previsto l'entrata in vigore del cosiddetto "*Artificial Intelligence Act*"⁴³⁷: la prima regolamentazione europea sull'Intelligenza Artificiale, composta da norme *self executing*⁴³⁸.

L'AI act prevede un tipo di approccio normativo "orizzontale", in quanto tratta l'Intelligenza Artificiale considerandola in un modo non eccessivamente specifico, ma fissando regole di carattere generale.

Il progetto è stato presentato ad aprile 2021, approvato dal Parlamento europeo il 13 marzo 2024, in vigore dal 1° agosto, tuttavia, la maggior parte delle norme verrà applicata a partire da agosto 2026.

Durante questo periodo di transizione, prima della completa attuazione del regolamento, la Commissione ha deciso di varare il "*l'AI Pact*", volto a promuovere l'adozione anticipata di misure etiche.

Questa iniziativa è su base volontaria, ed è destinata ad organizzazioni pubbliche e private, che utilizzano questa tecnologia all'avanguardia.

Lo scopo è quello di colmare il vuoto di tutela che si crea a seguito del divario temporale tra la continua crescita tecnologica di questi sistemi e l'attuazione di un quadro normativo adeguato e completo.

Inoltre, quest'ultimo fa parte di una più generale volontà del legislatore europeo di creare un unico sistema normativo applicabile in tutta Europa, mediante la cosiddetta "Strategia Europea sui dati 2030", emessa dalla Commissione Europea⁴³⁹, al fine di prevenire rischi e abusi delle piattaforme online.

⁴³⁶ *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the regions on boosting startups and innovation in trustworthy artificial intelligence*, Brussels, 24.1.2024 COM (2024) 28 final

⁴³⁷ Regolamento (UE) 2024/1689 Del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)

⁴³⁸ CARANTANI (2024), *IA Act: l'Unione Europea approva la proposta di Regolamento sull'intelligenza artificiale*, in "*Ius in itinere*", 3 maggio 2024C

⁴³⁹ Commissione europea, *Una strategia europea per i dati*, COM (2020)66, 19 febbraio 2020

L'Europa, insieme all'America e alla Cina è una dei *competitor* maggiori su scala mondiali sul tema, a differenza degli altri competitor però, l'UE pone l'accento sulle tematiche etiche e sociali che riguardano l'Intelligenza Artificiale, dandone una visione antropocentrica⁴⁴⁰.

Infatti, quest'ultima ha sempre considerato che l'IA dovesse integrare le capacità dell'uomo e non sostituirle⁴⁴¹.

Tuttavia, non mancano le lacune: per esempio, la Cina ha una disciplina lacunosa in materia di trasparenza della IA e di protezione dei dati personali⁴⁴².

Mentre gli Stati Uniti hanno puntato la loro ricerca sulla IA sulla base dell'autonomia privata e non sull'intervento pubblico (tuttavia, ci sono movimenti in grado di influenzare l'opinione pubblica americana, che chiedono delle specifiche regole in tema di protezione dei diritti dalla IA).

La Cina, d'altro canto, si è posta l'obiettivo di diventare il centro mondiale dell'innovazione entro il 2030.

Quest'ultima, mette in atto la strategia opposta, puntando su un incremento degli investimenti pubblici.

L'*AI act* è indirizzato sia a fornitori dei servizi (persone fisiche o giuridiche che immettono sul mercato un servizio⁴⁴³) che a utilizzatori (coloro che sfruttano i sistemi di IA⁴⁴⁴), importatori, distributori, anche se non hanno stabilità nell'Unione Europea, ma non crea diritti in capo ai singoli individui.

Nell'articolo 3 n. 1 dell'*AI act* si definisce l'Intelligenza Artificiale come «un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

Il Regolamento dà una nozione volutamente ampia, mantenendo la linea con la definizione proposta dall'OCSE (Organizzazione per la Cooperazione e lo sviluppo Economico)⁴⁴⁵, ma non poche sono state le critiche da parte della Dottrina⁴⁴⁶.

⁴⁴⁰ Commissione Europea, *Eu Commission: shaping Europe's digital future*, 2020

⁴⁴¹ Risoluzione del Parlamento Europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla Robotica, C 252/239, Gazzetta Ufficiale Unione Europea

⁴⁴² *New Generation Artificial Intelligence Development Plan (AIDP)*, China State Council, 2017

⁴⁴³ Articolo 3 n.3 del Regolamento

⁴⁴⁴ Articolo 3 n. 4 del Regolamento

⁴⁴⁵ «*Machine based system that can, for a given set of human defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. It uses machine and/or human based inputs to perceive real and/or virtual environments; abstract such perceptions into models (in an automated manner e.g. with ML or manually); and use model inference to formulate options for information or action. AI systems are designed to operate with varying levels of autonomy*», in OECD 2019

⁴⁴⁶ vd. SCHERER M.U., *Regulating Artificial Intelligence Systems: risks, challenges, competencies, and strategies*, in *Harvard Journal of Law and Technology*, Vol. 29, Number 2, 2016, p. 354 ss.

Restano escluse dalla definizione i *software* meno complessi, ma anche i sistemi di IA utilizzati con finalità di difesa, militari, di innovazione⁴⁴⁷.

La Commissione Europea, nel febbraio 2024 ha promulgato una decisione volta a introdurre l'“*AI Office*”, l'ufficio sull'Intelligenza Artificiale⁴⁴⁸, che farà parte della struttura amministrativa della Direzione Generale per le Reti di Comunicazione.

L'*AI Office* ha il compito di promuovere l'*AI Act* e regolarne l'attuazione, monitorare l'andamento del mercato digitale, consigliare l'utilizzo di sistemi affidabili, ma anche valutare metodologie innovative per verificare la presenza di rischi e indagare sulla violazione delle norme.

In caso di violazione di norme dell'*AI act*, secondo l'articolo 72 lett. a del regolamento Eu sull'AI, è la stessa Commissione Europea a irrogare sanzioni, secondo determinati criteri, per tutti gli altri casi spetterà ai singoli Stati Membri.

Si consideri in ogni caso, che questo organo non andrà ad interferire sui poteri e sulle competenze decisionali delle singole autorità nazionali.

Le basi che hanno portato alla costituzione dell'*AI act* vennero poste già nel 2018 dal GDPR, ma anche dal *Digital Markets Act*, *Data Act* e *Digital Services Act*, Regolamenti che hanno come obiettivo quello di rendere il mercato digitale più sicuro, garantendo parità per le imprese e la tutela dei diritti degli utenti.

Con questi atti, si voleva porre come fondamento la responsabilità delle piattaforme di gestione dei contenuti che vengono caricati sulla rete, e l'obbligo per questi ultimi di fornire all'utente le informazioni riguardanti il *quomodo* del funzionamento dei loro algoritmi per garantirne la trasparenza.

Scendendo più nel dettaglio, il *Digital Markets Act* si occupa di regolamentare quelle imprese cosiddette “*gatekeeper*” cioè grandi piattaforme *online* che hanno una elevata competitività sul mercato.

Mentre, il *Digital Services Act*⁴⁴⁹ si occupa della protezione dei consumatori, per evitare contenuti potenzialmente dannosi per la collettività e della responsabilità.

Il fine principale di questo atto è proteggere diritti fondamentali come il diritto alla *privacy* e la libertà di espressione.

Questi due atti vengono considerati generalmente come un *unicum* perché operano in modo complementare per assicurare un servizio digitale equo.

Tornando all'*AI Act*, gli obiettivi finali di questo atto sono vari: limitare i rischi dell'IA per la salute, la sicurezza e la dignità dei cittadini, rispettando i diritti fondamentali e i valori europei, sostenere l'innovazione tramite finanziamenti, aumentare la fiducia dei cittadini verso l'utilizzo di questi sistemi, creare un mercato unico al fine della libera circolazione della IA nel mercato europeo.

⁴⁴⁷ DURANTE M., PAGALLO U., *Manuale di Informatica Giuridica e diritto delle nuove tecnologie*, 2017

⁴⁴⁸ Commission Decision, Brussels, 24.1.2024 C (2024) 390 final

⁴⁴⁹ lo snodo centrale è il rischio, prevede obblighi appositi in base ai destinatari della regolazione. Su questi aspetti v. DE GREGORIO G., DUNN P., POLLICINO O., *A partire dalla Strategia per il Mercato Unico Digitale, l'approccio basato sul rischio è stato applicato in tutte le principali normative UE: analizziamo le analogie e le differenze tra GDPR, DSA e AI Act*, 15 Settembre 2022.

L'articolo 14 dell'*AI act* chiarisce anche che, in base ai fattori di rischio previsti nel medesimo atto che andrò ad analizzare in seguito, l'essere umano dovrà essere in grado di riconoscere potenziali fattori di rischio per i diritti fondamentali, per poter rilevare anomalie e interrompere tempestivamente la macchina.

Tuttavia, il testo finale verrà approvato ad aprile 2024 dal Parlamento Europeo e il Consiglio.

Secondo Mathieu Michel⁴⁵⁰, «l'adozione del regolamento sull'IA rappresenta una pietra miliare per l'Unione europea.

Questo atto legislativo storico, il primo del suo genere al mondo, affronta una sfida tecnologica globale che crea anche opportunità per le nostre società ed economie.

Con il regolamento sull'IA l'Europa pone l'accento sull'importanza della fiducia, della trasparenza e della responsabilità nell'utilizzo delle nuove tecnologie, insieme alla garanzia che questa tecnologia in rapida evoluzione possa prosperare e stimolare l'innovazione europea».

Inoltre, la scelta del tipo di atto legislativo non è casuale: è un Regolamento e non una direttiva per limitare la generale flessibilità sulla regolamentazione dell'AI in Europa. Infatti, l'articolo 114 TFUE conferisce la possibilità alle istituzioni di adottare misure che possano avvicinare, a livello teorico, le discipline interne, che incidono sul mercato comune⁴⁵¹.

L'obiettivo è quello di disciplinare l'emissione sul mercato e l'uso dei sistemi di Intelligenza Artificiale in tutta Europa⁴⁵².

Questa regolamentazione ha previsto vari livelli di rischio con cui classificare i sistemi, mediante una struttura piramidale, se il livello non è previsto come accettabile dalla regolamentazione allora non potrà essere utilizzato.

Viene considerato a rischio elevato, secondo l'articolo 6 del Regolamento sull'Intelligenza Artificiale, se la tecnologia AI è utilizzata nei seguenti ambiti: formazione scolastica, infrastrutture critiche (come i trasporti), servizi pubblici e privati essenziali, amministrazione della giustizia (per esempio l'utilizzo per prendere decisioni giudiziarie), ma anche l'uso di sistemi di identificazione biometrica remota (per i quali serve l'autorizzazione di un organo competente).

⁴⁵⁰ Dichiarazione del Sottosegretario di Stato belga per la digitalizzazione, all'annuncio del lavoro legislativo iniziato nel 2021 dall'Unione Europea

⁴⁵¹ ADINOLFI A., *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europea tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini Giuridica, Pisa, 2020, p. 13 e ss.; CLEYNENBREUGEL V. *EU By-Design Regulation in the Algorithmic Society*, in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor e G. De Gregorio (a cura di)

⁴⁵² Ursula von der Leyen, discorso per l'elezione come primo presidente donna della Commissione europea (2020, *"Un'Europa all'altezza del digitale"* disponibile online). Alla base della sua linea politica principale vi è una proposta legislativa per un approccio europeo coordinato alle implicazioni etiche e umane dell'IA.

Quindi è ad alto rischio l'attività per il quale l'*Artificial Intelligence* potrebbe comportare pericoli ingenti sulla salute, sulla sicurezza, sul rispetto dei diritti fondamentali, sullo Stato di diritto e le libertà del cittadino⁴⁵³.

Questa tipologia di rischi, prima di essere immessi sul mercato digitale devono seguire delle regole: primariamente, devono dotarsi di sistemi di valutazione del rischio, che sia atto a prevenire eventuali danni per i diritti dei cittadini e anche per le imprese.

Le attività poste in essere devono essere registrate per garantire l'eventuale tracciamento delle operazioni, insieme al fornimento di documentazione contenente tutte le informazioni (chiare) che servono ai fini della valutazione della conformità⁴⁵⁴.

Questi documenti dovranno essere conservati dal provider per dieci anni⁴⁵⁵.

Tutte queste precauzioni sono atte a evitare che si verifichino violazioni dei diritti umani, mantenendo un livello considerato "accettabile"⁴⁵⁶.

Mentre, il rischio limitato riguarda il problema della trasparenza in relazione ai sistemi come le *chatbot* o i filtri *antispam* dell'*e-mail*, fondamentale è informare l'utilizzatore che il contenuto è stato prodotto grazie all'Intelligenza Artificiale, nei limiti previsti dall'articolo 52 del Regolamento (anche in caso di *deep fake*, *Infra* § cap. 3 parag. 2)⁴⁵⁷.

Il rischio nullo fa riferimento invece all'uso gratuito della AI, per esempio è minimo il rischio in caso di videogiochi abilitati, questi vengono individuati per sottrazione rispetto a quelli a intermedio e alto rischio e sono previsti solamente obblighi di trasparenza⁴⁵⁸.

Per quest'ultimo tipo di sistemi, non si applica il Regolamento; ciò dimostra la volontà del legislatore europeo di non appesantire eccessivamente il lavoro degli addetti in campo tecnologico⁴⁵⁹.

La Commissione, inoltre, nella Relazione illustrativa di quest'atto, sottolinea che il rischio in questione si riferisce sia all'ambito individuale che collettivo⁴⁶⁰.

Secondo gli articoli 7 e 73 dello stesso, le categorie non possono essere modificate, ma ogni lista può essere aggiornata dalla Commissione mediante atti delegati non legislativi.

Questo metodo di identificazione di rischio è differente rispetto al GDPR e al *Digital Services Act*, perché in questi ultimi sono gli operatori stessi a definire il livello di rischio che si pensa possa essere pericoloso.

⁴⁵³ Considerando n. 27 della Proposta di Regolamento

⁴⁵⁴ TOSONI L., *Intelligenza artificiale, i punti chiave del regolamento europeo*, 21 aprile 2021

⁴⁵⁵ Articolo 16-18 AI act

⁴⁵⁶ ADINOLFI A., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, 2022 cit pag. 157

⁴⁵⁷ AssoDPO (2023), *AI ACT, la meta è vicina: un nuovo standard globale*, 19 dicembre 2023

⁴⁵⁸ Considerando n. 72 e articolo 13 Regolamento Ue sull'Intelligenza Artificiale

⁴⁵⁹ POLLICINO O., DE GREGORIO G., PAOLUCCI F., F. BAVETTA, *Regolamento AI, la "terza via" europea lascia troppi nodi irrisolti: ecco quali*, in *agendadigitale.eu*, 21 maggio 2021

⁴⁶⁰ «The same elements and techniques that power the socio-economic benefits of AI can also bring about new risks or negative consequences for individuals or the society».

Inoltre, come si evince dall'articolo 2.1 della proposta, il Regolamento si applica esclusivamente se il sistema AI viene utilizzato sul territorio dell'Unione Europea, a prescindere dal fornitore del servizio⁴⁶¹.

Ai fini di garantire un uso proporzionato e congiunto tra tutti gli Stati nella applicazione di questo Atto, verrà istituito anche l'EAIB (*European Artificial Intelligence Board*) per il quale ogni Stato firmatario dovrà nominare un membro.

Questa commissione offre consulenza agli Stati Membri e alla Commissione Europea, deve coordinare le autorità nazionali, armonizzare l'emissione di raccomandazioni anche su richiesta della Commissione stessa.

A livello generale, si può affermare che la sua funzione possa essere simile a quella dell'*European Data Protection Board* introdotta a seguito del GDPR⁴⁶².

1.4 (segue): GDPR e AI Act: La tutela dei dati personali, chi se ne occupa?

Secondo alcune ricerche dell'Agenzia per l'Italia Digitale, le autorità italiane dovrebbero garantire un approccio più armonizzato alla disciplina dell'AI.

Nel 2021 l'*European Data Protection Board* aveva emanato un parere⁴⁶³ sulla proposta di Regolamento del Parlamento Europeo e del Consiglio in materia, richiedendo l'assegnazione della protezione dei dati personali e il rispetto della vita privata, ma anche la funzione di controllo dell'uso della AI, alle autorità competenti.

Infatti, la parte più delicata dell'utilizzo dell'intelligenza artificiale è indubbiamente la raccolta di una grande quantità di dati, necessari al suo corretto funzionamento⁴⁶⁴.

Le autorità, devono essere caratterizzate da indipendenza, e imparzialità, in modo da tutelare i diritti rientranti nel regolamento del Parlamento Europeo e del Consiglio.

Secondo questo parere, l'applicazione dell'articolo 16 del TFUE comporta la necessità di garantire un controllo indipendente della conformità ai requisiti in materia di trattamento dei dati personali, come richiesto altresì dall'articolo 8 della Carta dei diritti fondamentali dell'UE.

La vita privata e la riservatezza, e quindi anche i dati personali, sono tutelati a livello Europeo dalla Dichiarazione Universale dei Diritti dell'Uomo all'articolo 12, nella Convenzione Europea dei diritti dell'Uomo all'articolo 8 e nella Carta dei Diritti fondamentali dell'Unione Europea agli articoli 7 e 8.

⁴⁶¹ Il concetto di competenza territoriale viene espresso da FLORIDI L., *The European Legislation on AI: a brief Analysis of its Philosophical Approach*, 2021 cit., p.220.

⁴⁶² ALUIGI F., GAROFALO A., PIEMONTE J., Articolo dell'AGID, 13 marzo 2024

⁴⁶³ Parere congiunto sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale del 5/2021 *European Data Protection Board*, EDPB - GEPD

⁴⁶⁴ COLAPIETRO C., MORETTI A., *L'intelligenza Artificiale nel dettato costituzionale*, 2020, pp. 376-377

Per quanto riguarda i dati personali di minori, che vengono utilizzati dall'Intelligenza Artificiale, il decreto-legge che il governo Meloni ha portato in Parlamento per l'approvazione ad aprile 2024 introduce nuovi livelli di tutela.

Per i minori dai quattordici ai diciotto anni è necessario il loro consenso, se le informazioni sono facilmente comprensibili, in quanto espressi con un linguaggio limpido e semplice, da questi ultimi.

Il GDPR (*General Data Protection Regulation*) rappresenta il principale strumento di tutela per questi diritti, a prescindere dal mezzo con cui vengono gestiti i dati personali; infatti, ha più un carattere generale rispetto all'atto di recente introduzione sull'Intelligenza Artificiale.

Per questo, non si potrebbe utilizzare il principio di specialità per ovviare ad eventuali conflitti fra le due normative, considerando che il primo, è volto a tutelare un diritto fondamentale previsto esplicitamente da una fonte primaria⁴⁶⁵.

Il GDPR, fa parte della “*data protection reform package*”, insieme alla Direttiva n.680/2016⁴⁶⁶, che a differenza del GDPR, è una *lex specialis*, con fini repressivi, in quanto stabilisce norme minime per la «protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.»⁴⁶⁷. Per quanto riguarda l'Intelligenza artificiale e i diritti fondamentali, un caso che ha portato molto scalpore è stato sollevato dalla nota associazione Europea per i diritti digitali “*Nyob (none of your business)*”, la quale ritiene che la nuova normativa sulla privacy del gruppo “*Meta*” (entrato in vigore il 26 giugno) violi almeno dieci articoli GDPR.

L'attivista della *privacy* Maximilian Schrems ha denunciato l'allarmante situazione per gli utenti di *Meta*, affermando che «*Meta* sta sostanzialmente dicendo che può utilizzare “qualsiasi dato da qualsiasi fonte per qualsiasi scopo e renderlo disponibile a chiunque nel mondo”, purché ciò avvenga tramite ‘una tecnologia AI’.

Questo è un termine estremamente ampio. Proprio come “utilizzare i vostri dati nei database”, non ha un vero e proprio limite legale.

Meta non dice per cosa utilizzerà i dati, quindi potrebbe essere un semplice *chatbot*, una pubblicità personalizzata estremamente aggressiva.

Meta dice anche che i dati degli utenti possono essere resi disponibili a qualsiasi terza parte, cioè a chiunque nel mondo»⁴⁶⁸.

⁴⁶⁵ CONTALDI G., *Intelligenza Artificiale e dati personali*, 2021, pp. 419-421

⁴⁶⁶ inserita nel nostro ordinamento con il d.lgs. 18 maggio 2018 n.51

⁴⁶⁷ SERVENT A.R., “*Protecting or Processing?*”, in Aa.Vv., *Privacy, Data Protection and Cybersecurity in Europe*, a cura di W.J. Shünemann e M.O. Baumann, Cham, 2017, p. 125.

⁴⁶⁸ Redazione NOYB, *noyb sollecita 11 DPA a fermare immediatamente l'abuso dei dati personali da parte di Meta per l'IA*, 6 giugno 2024, consultabile sul sito ufficiale

Noyb ha contestato questa *privacy policy* per vari motivi: Innanzitutto, *Meta* non distinguerebbe, su propria ammissione, le categorie di dati che necessitano di un trattamento diverso, dagli altri dati.

Inoltre, viene predisposto l'utilizzo di tutti i dati come "interesse legittimo", decisione, secondo *Noyb*, non proporzionata.

L'associazione ha quindi richiesto una procedura d'urgenza ai sensi dell'articolo 66 GDPR.

Le Autorità di Protezione dei Dati (DPA) competenti dei singoli Paesi decideranno se avviare una procedura d'urgenza oppure no.

Secondo *Google*, gli sviluppatori dell'Intelligenza Artificiale dovrebbero avere accesso all'uso dei dati personali ai fini dell'addestramento di quest'ultima, anche se ci sono rischi⁴⁶⁹.

Il Garante ha sempre sottolineato, tuttavia, la necessità di un utilizzo chiaro e trasparente dell'IA e il bisogno di individuare una autorità che si occupi di effettuare queste valutazioni⁴⁷⁰.

Perciò, considerando il GDPR come un atto di tutela più generale per i dati personali, l'AI act può essere applicato in contemporanea: poiché disciplina *l'Artificial Intelligence* in quanto meccanismo con cui i diritti in questione vengono coordinati.

Tuttavia, alcuni ritengono che parte dell'*AI act* possa potenzialmente sovrapporsi con il GDPR, come accade per la valutazione e la gestione dei rischi, che è trattata sia dalla regolamentazione sulla AI sia dall'articolo 35 del GDPR.

Infatti, proprio la vicepresidente del Garante per la Protezione dei Dati Personali⁴⁷¹, durante un intervento ha dichiarato: «La sovrapposizione deriva, da un lato, dalla definizione estremamente ampia di IA, che comprende persino gli approcci statistici e, dall'altro lato, dal fatto che i cosiddetti sistemi di IA ad alto rischio sono definiti nella bozza per aree in cui per la stragrande maggioranza sono i dati personali ad essere trattati.

Si pensi all'identificazione biometrica, all'istruzione, alla sanità, alle prestazioni assistenziali, all'immigrazione, ecc.

Solo nel settore delle infrastrutture il Regolamento IA potrebbe avere un'applicazione del tutto autonoma.

Negli altri settori vi sarebbe, di fatto, una co-regolamentazione e, probabilmente, saranno le normative in materia di protezione dei dati personali a prevalere in quanto competenti per materia».

⁴⁶⁹ *Google Cloud Whitepaper "Generative AI, Privacy and Google Cloud"*, Settembre 2020, consultabile online

⁴⁷⁰ Sul progetto di utilizzo dei dati personali, da parte di *Meta*, si è espressa l'Autorità di controllo norvegese, che ha affermato i propri dubbi sull'approccio seguito dalla società, sottolineando la necessità di chiedere il consenso dei soggetti interessati per il trattamento dei dati. Autorità di controllo norvegese, Comunicato stampa del 4 giugno 2024

⁴⁷¹ FERONI CERRINA G., 20 gennaio 2023, Camera dei deputati, *Sala del Cenacolo, Palazzo Valdina, in occasione della presentazione del volume* di F. Lazzini, *Etica e Intelligenza artificiale*, Torino, Giappichelli, 2022.

La Commissione, mediante l'ufficio predisposto per l'Intelligenza Artificiale ha avviato un processo di consultazione su futuri orientamenti che aiuteranno le autorità nazionali ma anche i fornitori e gli operatori a conformarsi alle pratiche stabilite sull'IA, gli orientamenti riguarderanno la definizione di sistemi IA e le pratiche vietate ai sensi dell'*AI act*.

Questi orientamenti verranno pubblicati a febbraio 2025⁴⁷².

La bozza di Regolamento AI riguarda poi in larga parte oggetti e i principi già enucleati nel GDPR (sebbene l'approccio al rischio diverga perché l'uno responsabilizza il titolare del trattamento ponendo al centro i diritti dell'interessato, l'altro invece introduce un meccanismo di *compliance* a standard predefiniti dall'alto).

Entrambe le leggi si concentrano sulle finalità del trattamento dei dati personali, sull'utilizzo del sistema di IA, sull'approccio della *privacy by design*; entrambi richiedono che gli indirizzi del Regolamento identifichino i rischi per i diritti fondamentali.

In comune, hanno anche la forma scelta dal legislatore, infatti sono regolamenti e non direttive, assicurando in ogni caso forme di revisione periodica.

Tuttavia, la proposta di Regolamento si propone esplicitamente di avere un approccio "umano-centrico"⁴⁷³ e di plasmare IA che siano affidabili e sicure per gli individui».

L'*AI act* pone anche dei nuovi compiti all'Autorità Garante della *Privacy*, imponendo il controllo dei dati che gli vengono notificati circa l'utilizzo di sistemi di identificazione biometrica in tempo reale.

Concludendo, in Italia, nel caso in cui l'utilizzo della AI comprometta dati personali o diritti fondamentali, come spesso succede, si utilizza primariamente il GDPR ma anche l'*AI act*, in quanto strettamente connessi.

Quest'ultimo stabilisce che in caso di violazione del Regolamento, le autorità nazionali avranno il compito di irrogare sanzioni, esercitando, in fin dei conti, un ruolo simile al Garante della *Privacy*, per il GDPR.

Secondo alcuni⁴⁷⁴, la soluzione sarebbe investire l'AGID e l'Agenzia Nazionale per la *Cybersicurezza* (ACN), di tale competenza; tuttavia, ciò comporterebbe non pochi squilibri poiché L'AGID viene categorizzata come una agenzia governativa, e non sarebbe quindi, una autorità indipendente, come invece richiedeva l'*European Data Protection Board*.

È stato approvato dal Consiglio dei ministri il 23 aprile 2024 un disegno di legge recante il titolo «per l'introduzione di disposizioni e la delega al Governo in materia di

⁴⁷² Sito ufficiale della Commissione Europea, Comunicato stampa, 13 novembre 2024.

⁴⁷³ D'ALOIA A., *Il diritto verso "il mondo nuovo"*, 2019 op. cit., 4

⁴⁷⁴ Dichiarazioni del Sottosegretario All'innovazione, Alessio Butti, durante l'evento "l'intelligenza artificiale per l'italia", firmato dal dipartimento per la trasformazione digitale di Palazzo Chigi e dal'Agid.

intelligenza artificiale» il quale prevede che le funzioni di controllo spettino a questi due organismi.

Alla fine, la scelta è ricaduta su questi a causa delle alte competenze specializzate volte a far fronte alle sfide che l'Intelligenza Artificiale pone in ambito di sicurezza, protezione dei dati e cittadinanza.

Secondo altri invece, tra cui il presidente dell'Autorità per la Protezione dei dati personali, la miglior ipotesi sarebbe seguire il modello spagnolo nella creazione di una autorità apposita, terza e indipendente⁴⁷⁵, è stata infatti approvata in Spagna la *Agencia Española de Supervisión de Inteligencia Artificial* (AESIA)⁴⁷⁶.

La soluzione ancora oggi è in via di sviluppo, tuttavia, secondo la vicepresidente del Garante, non si potrà in ogni caso prescindere dall'uso dei principi enunciati nel GDPR. La governance europea, quindi, potrebbe essere a rischio, a causa dell'ampio margine di scelta lasciato agli Stati da parte del legislatore europeo, in merito all'autorità competente, per tutelare i diritti fondamentali.

Perciò secondo la Dottrina, da un lato potrebbero paventarsi vuoti di tutela, dall'altro anche delle duplici sanzioni provenienti da autorità diverse⁴⁷⁷.

1.5 (segue): L'Intelligenza Artificiale e i rischi per i Diritti fondamentali, innovazione o pericolo?

Anche a fronte di una visione proattiva⁴⁷⁸ sull'uso dell'Intelligenza Artificiale, mettendo quindi in luce i numerosi vantaggi dei processi automatizzati basati sull'elaborazione dei dati, in svariati ambiti della vita umana, non mancano i lati negativi e i potenziali problemi che potrebbe arrecare ai fini della tutela dei diritti fondamentali⁴⁷⁹.

Nella Dichiarazione Europea dei diritti e dei principi digitali per il decennio digitale, si parla, nel capitolo terzo, della fondamentale libertà di scelta del cittadino come base per la transizione digitale⁴⁸⁰.

Secondo quest'ultima infatti, "l'Intelligenza Artificiale dovrebbe fungere da strumento per le persone, con l'obiettivo ultimo di aumentare il benessere umano".

⁴⁷⁵ STANZIONE P., "Segnalazione al Parlamento e al Governo sull'autorità per l'IA", 2024

⁴⁷⁶ Real Decreto 729/2023, 22 agosto. «BOE» núm. 210, de 2 de septiembre de 2023, páginas 122289 a 122316 (28 págs.) Disposiciones generales, Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, BOE-A-2023-1891

⁴⁷⁷ RAFFIOTTA E., *Quale autorità governerà l'Intelligenza Artificiale?* Il Sole 24Ore, 27 marzo 2023

⁴⁷⁸ SANTOSUOSSO A., *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori Università, Città di Castello, 2020, p. 26.

⁴⁷⁹ sui diritti fondamentali v. SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione*, Giappichelli, Torino 2022; A. D'ALOIA, *Il diritto verso il "mondo nuovo". Le sfide dell'intelligenza artificiale*, in *BioLaw Journal*, n. 1/2019, 15 ss

⁴⁸⁰ Dichiarazione Europea sui diritti e i principi digitali per il decennio digitale (2002) 208, approvato nel gennaio 2022

Un diritto che sicuramente è a rischio in quest'ambito è la riservatezza e la protezione dei dati personali⁴⁸¹.

Il Garante nazionale per la protezione dei dati personali⁴⁸², ritiene che, sia l'IA che la riservatezza sono materie trasversali, «accomunate dal rappresentare la sfida, attuale e futura, lanciata dalla tecnica al diritto e alla sua possibilità di regolamentare anche ciò che appare, nella sua evoluzione incessante, più refrattario alla norma».

Il Garante della *privacy* specifica che il cittadino è soggetto a tutela della propria riservatezza anche quando il trattamento, che avviene mediante AI, derivi da un soggetto pubblico.

Inoltre, Il presidente dell'Autorità Garante della protezione dei dati personali, durante la consegna della relazione annuale per il 2023 sulla tutela dei diritti fondamentali mediante l'uso dell'Intelligenza Artificiale, ha ribadito che «l'IA è diffuso in larga misura e parte integrante della nostra vita ma di cui dovremmo saper governare gli effetti perché al riguardo non siamo del tutto consapevoli, [...] il diritto ha il compito di colmare questo vuoto di consapevolezza, fornendoci gli strumenti per capire come porre realmente al servizio dell'uomo, ciò che può rappresentare tanto uno straordinario fattore di sviluppo, benessere, promozione del pubblico interesse quanto anche, se non ben governato, una fonte di rischi tutt'altro che trascurabili, per la persona, la società, la democrazia.

La sfida principale che si delinea all'orizzonte è tutta nel rendere l'evoluzione tecnologica davvero mimetica e non soltanto protesica capace cioè di simulare l'uomo e la sua razionalità, prima e oltre che colmarne le carenze: un fattore di progresso non solo tecnico ma sociale, temperando, per riprendere le parole del Pontefice, con l'algoretica gli eccessi dell'algocrazia».

Il Garante, ha richiesto mediante un provvedimento, di limitare l'uso dei dati degli utenti Italiani da parte di *Open AI*, la società che possiede *Chat GPT*⁴⁸³.

A marzo 2023 ha addirittura sospeso temporaneamente l'uso dei dati personali fino a quando l'applicazione non avrebbe trovato delle soluzioni per limitare i rischi e non avrebbe posto delle delucidazioni sul loro trattamento, a fronte del principio di trasparenza.

La sanzione prevista è di quindici milioni di euro, insieme all'ordine di informare gli utenti sul trattamento dei dati personali da parte dell'Intelligenza Artificiale, e come negare il consenso.

Un esempio è il caso del Redditometro, argomento di carattere tributario affrontato sempre dal Garante nel 2013, in merito al trattamento dei dati dell'anagrafe.

⁴⁸¹ A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, 2019

⁴⁸² Parere reso sulla Proposta di Regolamento UE sull'Intelligenza Artificiale COM 2021 (206), Camera dei deputati, 9 marzo 2022, Riunite commissione IX e X. Consultabile sul sito del Garante.

⁴⁸³ Provvedimento 2 novembre 2024 provv n. 10085455

Il Garante Inglese, L'information Commissioner's Office, nel documento "*How to use AI and personal data appropriately and lawfully*"⁴⁸⁴ ha introdotto alcune raccomandazioni basilari, come l'individuazione dei rischi per i dati personali e adottare delle misure che prevedano un trattamento corretto di questi ultimi, in relazione alla legge vigente.

Ha anche sottolineato la necessità di rispettare il principio di minimizzazione (articolo 5 GDPR) (principio richiamato anche dall'*AI act*), secondo cui i dati raccolti devono essere solamente quelli pertinenti alle finalità per la quale vengono conservati, garantendone l'aggiornamento e l'affidabilità.

Infatti, fondamentale per la tutela dei diritti dei cittadini è che questi ultimi siano informati sul trattamento dei dati utilizzati dall'Intelligenza Artificiale⁴⁸⁵.

Ci si interroga se l'informativa debba pervenire prima del trattamento, oppure in un secondo momento⁴⁸⁶ e se sia opportuno che contenga anche i dati che hanno portato alla decisione della AI.

Soprattutto circa l'ipotesi del sistema ad alto rischio, si ritiene che il controllo dell'essere umano all'operato della macchina sia di carattere precauzionale, al fine di una maggior tutela per i diritti fondamentali, per ridurre al minimo i rischi, che potenzialmente potrebbero rimanere anche dopo che l'IA ha concluso il suo operato⁴⁸⁷. Tuttavia, come mostra l'ICO, non è sufficiente una adatta strategia di conservazione dei dati, ma anche la presenza di figure tecniche esperte che controllino il corretto utilizzo dei sistemi AI durante tutte le fasi di conservazione delle informazioni.

Infatti, secondo la Dottrina, più è alto il livello di autonomia della macchina, più è necessario un controllo umano⁴⁸⁸.

La sorveglianza dell'uomo diventa quindi uno strumento imprescindibile per limitare la libertà della Intelligenza Artificiale⁴⁸⁹.

⁴⁸⁴ "*how to use Ai and personal data appropriately and lawfully*", pubblicato dall'ICO (Information commissioner's office) alla fine del 2022, sono delle linee guida necessarie al fine di rispettare la conformità al GDPR sia dal punto di vista progettuale della AI sia per il funzionamento. Consultabile online

⁴⁸⁵ Cfr. PAJNO A., M. BASSINI, G. DE GREGORIO, M. MACCHIA, F.P. PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, *Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in BioLaw Journal, 3/2019, p. 205 ss.; sul principio di trasparenza della AI, PALMIRANI M., *Big Data e conoscenza*, in Riv. Filosofia del Diritto, 1/2020

⁴⁸⁶ dibattito cfr. WACHTER S., B. MITTLESTADT E L.FLORIDI, *Why a Right to Explanation of Automated DecisionMaking Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law* 2017, 7 (2), pp. 76-99. V. anche LONGO E., *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. I, Il Mulino, Bologna, 2022, p. 349 ss

⁴⁸⁷ MARTIRE D., *Intelligenza artificiale e Stato costituzionale*, 2022

⁴⁸⁸ Cfr. RINALDI L., *Intelligenza artificiale, diritti e doveri nella Costituzione italiana*, in DPCE online, 1/2022, p. 201 ss

⁴⁸⁹ Cfr. AMIDEI A., *La governance dell'Intelligenza Artificiale: profili e prospettive di diritto DELL'UNIONE Europea*, in U. Ruffolo (a cura di), *Intelligenza artificiale - Il diritto, i diritti, l'etica*, cit., p. 571 ss

Quest'ultimo è uno dei principi base stabiliti nel Libro Bianco sull'Intelligenza Artificiale della Commissione Europea⁴⁹⁰, il quale differenzia vari tipi di controllo: Innanzitutto il caso di necessaria convalidazione da parte dell'uomo del risultato raggiunto, cioè per immediata attuazione della decisione della AI, con successivo intervento dell'uomo, oppure con intervento immediato, durante il funzionamento della macchina⁴⁹¹.

Considerando quanto detto, è evidente che al centro del piano del legislatore europeo c'è l'istituzione di un adeguato regime di responsabilità per danni arrecati dai sistemi di Intelligenza Artificiale, per una *governance* globale più affidabile⁴⁹².

Oltre al diritto alla riservatezza, altri diritti fondamentali che potrebbero essere toccati dalla elaborazione automatizzata di dati sono: l'uguaglianza, la vita privata, un utilizzo non discriminatorio della IA (articolo 2 TUE, 10 TFUE, 20 della Carta) e l'accesso alla giustizia (diritto a un equo processo e un ricorso effettivo sulle decisioni automatizzate), la dignità umana, il diritto a una buona amministrazione (nel settore pubblico), la protezione dei consumatori ma anche ogni altro diritto tutelato dalla Carta dei Diritti Fondamentali⁴⁹³.

Per esempio, ai fini di un rispetto completo del principio di non discriminazione, di recente la Commissione Europea ha sentito la necessità di introdurre disposizioni aggiuntive riguardante l'utilizzo dell'Intelligenza Artificiale, nel Piano d'azione d'Europa contro il razzismo 2024-2025⁴⁹⁴.

Secondo la Dottrina, un metodo per ovviare i fenomeni di discriminazione mediante l'uso della IA, potrebbe essere quello di inserire la dignità umana, intesa come la facoltà del soggetto di riconoscere quando interagisce con una macchina⁴⁹⁵, e la tutela della libertà nella formazione di coloro che si occupano della *governance* delle nuove tecnologie⁴⁹⁶.

Tuttavia, queste nuove tecnologie rappresentano, il più delle volte, un rischio, soprattutto per i diritti dei più piccoli, come nel caso accaduto di recente, di un bambino americano che si è suicidato a seguito di più di un mese di conversazione con una AI (utilizzando il programma "*Character.AI*") che impersonava "Daenerys Targaryen" di "*Game of thrones*", dopo essersene invaghito.

⁴⁹⁰ cfr. PACILEO, 2022, "*Proposals for a New Legal Framework on AI: Possible Discrepancies Between Liability, Compliance and Duties of Company Directors*" pp. 305 e 306

⁴⁹¹ COMMISSIONE EUROPEA, *Libro Bianco sull'intelligenza artificiale*. Un approccio europeo all'eccellenza e alla fiducia (COM 2020/65 final), 19 febbraio 2020, pp. 23-24.

⁴⁹² EUROPEAN COMMISSION, *Inception impact Assessment*, Ref. Ares (2021)4266516 - 30/06/2021, consultabile sul sito della commissione europea; Risoluzione del Parlamento Europeo "*Raccomandazioni alla Commissione su un regime di responsabilità civile per l'Intelligenza Artificiale*" del 20 ottobre 2020

⁴⁹³ cfr. FRA (2012), *Bringing rights to life: The fundamental rights landscape of the European Union*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione Europea

⁴⁹⁴ COMMISSIONE EUROPEA, *A Union of Equality: EU anti racism action plan 2024-2025; Report on the implementation of the EU anti racism action plan*, 25 Settembre 2024, consultabili sul sito ufficiale della Commissione Europea

⁴⁹⁵ Cfr., A. D'ALOIA, *Il diritto verso "il mondo nuovo"*, op. cit., 7

⁴⁹⁶ SIMONCINI A., *L'algoritmo Incostituzionale, intelligenza artificiale e il futuro delle libertà* cit., 88.

Il ragazzo si è tolto la vita, dopo aver comunicato con questo *bot* tutti i giorni.

Ulteriori rischi ai diritti fondamentali derivano dall'utilizzo della IA per il controllo di massa; questo rappresenta un grande problema soprattutto in Cina, dove l'uso del riconoscimento biometrico è largamente diffuso, ma manca ancora un adeguato quadro normativo di tutela per i diritti fondamentali.

La Commissione legislativa del Congresso cinese ha avanzato una proposta per una legge sulla tutela dei dati personali "*Personal Information Protection Law*" (PIPL) attualmente in fase di discussione⁴⁹⁷.

Secondo quanto sancito dall'articolo 51 della Carta dei diritti Fondamentali, paragrafo 1, gli Stati membri dell'Unione devono rispettare tutti i diritti sanciti dalla Carta quando attuano il Diritto dell'Unione.

Per la FRA (*European Union Agency for Fundamental Rights*) il legislatore europeo si dovrebbe occupare di rendere obbligatorie valutazioni d'impatto riguardante i diritti fondamentali (FRIA), prima che venga utilizzato qualsiasi sistema IA, per questo queste valutazioni sono indirizzate agli utilizzatori.

L'obiettivo di quest'ultima è verificare la conformità col diritto europeo e nazionale in merito ai diritti fondamentali, e l'impatto che avrebbe su questi, ma anche valutare la singola persona fisica o giuridica che ne fa richiesta⁴⁹⁸.

In merito al diritto alla *privacy* e alla riservatezza, sono tante le preoccupazioni sulla possibile lesione dei diritti dei cittadini, anche in merito ai sistemi già in atto.

Per esempio, *Google Clips* utilizza una forma di AI per scattare automaticamente foto quando rileva qualcosa di importante, mentre *Alexa* (di proprietà di *Amazon*) ha fatto molto discutere per il pericolo di intercettazioni, mentre la società europea *Electrolux* sta sviluppando un forno dotato di telecamera integrata.

L'*AI act*, in caso di sistemi ad alto rischio, richiede agli utilizzatori del sistema di svolgere valutazioni d'impatto sulla protezione dei dati personali (DPIA) per informare l'utilizzatore sul corretto uso e sulle finalità.

Queste, dovrebbero essere condotte in modo trasparente, rese pubbliche e basarsi sulla prassi consolidata di altri settori durante l'implementazione della IA⁴⁹⁹.

Anche l'UNESCO si è espressa⁵⁰⁰ sull'utilizzo trasparente dell'Intelligenza Artificiale, fornendo apposite linee guida utili per lo scambio di buone pratiche tra diverse giurisdizioni, al fine di assicurare un uso etico, non discriminatorio, per la pace e la giustizia sostenibile.

⁴⁹⁷ The PIPL è stato discusso durante il trentesimo incontro del Comitato permanente della tredicesima edizione del "*National People's Congress of the People's Republic of China (NPC)*", 20 agosto 2021

⁴⁹⁸ Articolo 27 del Regolamento

⁴⁹⁹ Agenzia dell'Unione Europea dei Diritti Fondamentali, *l'Intelligenza Artificiale e I Diritti Fondamentali*, 2021, Lussemburgo

⁵⁰⁰ Durante il secondo Global Forum sull'etica dell'Intelligenza Artificiale, tenutasi a febbraio 2024, le linee guida sono consultabili sul sito ufficiale dell'Unesco

Le varie iniziative che sono state lanciate in questa sede sono: L'Osservatorio Globale sull'etica e la *Governance* della IA, ma anche la rete di esperti UNESCO sull'etica della IA senza frontiere.

Le aree trattate sono principalmente quattro: trasparenza, giustizia, responsabilità e *privacy*.

Per il primo punto, l'Unesco sostiene che la trasparenza è necessaria ai fini dell'assicurazione di un algoritmo trasparente e comprensibile da parte degli utilizzatori, permettendogli di capire in che modo l'AI prende le decisioni.

Molti aspetti che riguardano la correttezza della Intelligenza Artificiale, la responsabilità e la protezione dei diritti dei consumatori sono coperti dalla Direttiva sui servizi⁵⁰¹ e la Direttiva sul commercio elettronico⁵⁰², che mettono in luce il fatto che responsabile del processo decisionale della macchina deve essere, in ultima istanza, l'uomo, soprattutto per servizi professionali.

La trasparenza è anche fondamentale nel campo della Giustizia, per assicurare un utilizzo non discriminatorio del sistema, rispettando la *privacy* e la dignità altrui.

Inoltre, in merito alla responsabilità l'Unesco ritiene che si dovrebbero far carico delle decisioni della IA sia le organizzazioni che i singoli *provider*.

2.0 (segue): L'Intelligenza Artificiale come mezzo di prevenzione e repressione dei reati - applicabilità al *Revenge Porn*

2.1 (Segue): La funzione preventiva dei reati – la teoria della pena

Prima di procedere a descrivere nel dettaglio l'ipotesi in cui l'Intelligenza Artificiale possa essere applicata in sede di prevenzione per il reato di *Revenge porn*, ma anche più in generale per i reati contro la persona, ritengo necessario dover effettuare una premessa di carattere introduttivo, in modo tale da capire a pieno gli argomenti e la fattispecie in esame.

Grazie a vari contributi dottrinali⁵⁰³, possiamo affermare che l'Intelligenza Artificiale può essere applicata anche in campo giuridico, anzi, rappresenta un valido alleato per l'esercizio della funzione giurisdizionale e potrebbe rivelarsi utile anche per l'organo giudicante, per la ricerca di precedenti o di sentenze per i ricorsi in Cassazione oppure in Appello⁵⁰⁴.

⁵⁰¹ Direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno, GU L. 376 del 27.12.2006, pag. 36.

⁵⁰² Direttiva 2000/31/CE del Parlamento Europeo e del Consiglio, dell'8 giugno 2000

⁵⁰³ Cfr. i contributi raccolti in CARLEO A. (a cura di), *Il vincolo giudiziale del passato. I precedenti*, luglio 2018 cit.

⁵⁰⁴ G.LEGNINI, *Introduzione*, in A.CARLEO (a cura di), *Decisione robotica*, RIVISTA AIC. 428 cit., 12 ss.; DE RENZIS L., *Primi passi nel mondo della giustizia "high tech": la decisione in un corpo a corpo virtuale fra tecnologia e umanità*, in A.Carleo (a cura di), *Decisione robotica*, cit., 150

L'obiettivo di questo paragrafo però, è focalizzarsi sulla funzione preventiva e spiegare le caratteristiche generali, in modo tale da spiegare come l'IA possa essere utilizzata a questo fine.

Il legislatore è da sempre stato combattuto sui vari scopi attribuibili alla pena; per questo, nell'arco del tempo si sono stratificate varie teorie, ma mi concentrerò prevalentemente sulla funzione preventiva della pena.

La funzione preventiva viene definita "relativa" in quanto si concentra sugli effetti della pena⁵⁰⁵.

Innanzitutto, partendo dal definire la funzione preventiva in via generale, la pena viene considerata tale in quanto capace di funzionare come deterrente per la commissione di reati.

Esistono due tipi di prevenzione: quella generale e quella speciale.

La prima, viene definita come volta a evitare comportamenti ritenuti dannosi, e che quindi andrebbero vietati; a sua volta, si dirama in "positiva" o "negativa".

Quella positiva, si basa sul fatto che, essendo presenti delle leggi che contrastino determinati atti, il cittadino si conformi spontaneamente ai valori espressi da quest'ultima; si parla quindi di una sorta di coscienza morale che si sviluppa tramite la pena⁵⁰⁶.

Si ritiene, concludendo, che la natura intimidatoria della pena porterebbe, a livello psicologico, a una neutralizzazione della spinta a delinquere⁵⁰⁷.

Questo tipo di funzione, mira quindi a un orientamento culturale, ossia a distogliere i cittadini dall'avere determinati comportamenti, tramite non tanto la severità della pena ma la sua certezza⁵⁰⁸.

Alternativamente, in caso della funzione preventiva "negativa", l'obiettivo è quello di diminuire la tendenza del cittadino a delinquere, considerando la pena come minaccia di un male, con il fine ultimo di dissuasione e di neutralizzazione della pericolosità.

Tuttavia, una eccessiva deterrenza potrebbe portare a uno squilibrio tra la pena attribuita e la gravità del reato⁵⁰⁹.

Questa visione ha ottenuto molte critiche⁵¹⁰, in quanto non permette di considerare tutti quei casi per cui l'uomo è spinto da impeti, per il quale il timore di una sanzione non è sufficiente; un esempio pertinente alla materia oggetto d'esame è l'omicidio per gelosia o per vendetta nei confronti di qualcuno.

⁵⁰⁵ DOLCINI, MARINUCCI, *Manuale di Diritto penale, parte generale*, Giuffrè ed., 2024

⁵⁰⁶ FIANDACA-MUSCO, *Diritto penale, Parte generale*, cit., p. 712 ; FIANDACA-DI CHIARA, *Una introduzione al sistema penale: per una lettura costituzionalmente orientata*, 2003

⁵⁰⁷ DOLCINI-MARINUCCI, *Manuale di diritto penale*, parte generale, 2022 cit., p. 4. Qui si fa riferimento alla "teoria della Coazione Morale"

⁵⁰⁸ BECCARIA C, *Dei delitti e delle pene*, edizione a cura di Venturi, Torino, 1994, par. XXVII, "Uno dei più gran freni dei delitti non è la crudeltà delle pene, ma l'infallibilità di esse".

⁵⁰⁹ PELISSERO M., *Diritto Penale, Appunti di parte generale*, Giappichelli editore, 2021

⁵¹⁰ FIANDACA- MUSCO, *Diritto penale*, parte generale, 2024 argomento a pag. 712

Assume invece una prospettiva diversa la prevenzione cosiddetta “speciale” della pena, il quale ha l’obiettivo, nel caso in cui si tratti di un soggetto che ha già commesso un reato, di ridurre la recidiva e impedire che violi ulteriori regole.

Anche in questo caso, si divide in positiva o negativa.

La fattispecie cosiddetta “negativa”, fa riferimento a neutralizzazione del soggetto che delinque (grazie, per esempio, a misure come la pena detentiva); si ricorre a quest’ultima quando è chiaro che non è possibile esercitare una intimidazione o rieducazione, quindi rappresenta una *ultima ratio*.

Il fine è quello di estromettere dalla collettività coloro che commettono reati molto gravi⁵¹¹.

Mentre, la prevenzione speciale “positiva” vede la pena in termini rieducativi, incidendo sulla personalità dell’individuo mediante una risocializzazione.

2.2 (Segue): Il fenomeno del *Revenge porn*, come le piattaforme online vogliono utilizzare l’Intelligenza Artificiale in chiave preventiva

Avendo spiegato in linea generale cosa si intende per prevenzione, posso procedere a descrivere come l’Intelligenza Artificiale può essere utilizzata sia dalle piattaforme *online* ma anche dallo Stato, per prevenire questo fenomeno in rapida ascesa.

Lo scopo è quindi analizzare una grande quantità di dati per identificare comportamenti potenzialmente a rischio, per la rilevazione di un determinato “*pattern*” da parte del soggetto che commette il reato.

Non si tratta infatti, di un utilizzo distopico come quello presente nei film, come il caso di “*Minority Report*” dove i sistemi di Intelligenza avanzata erano in grado di comprendere quando una persona stava per commettere un reato ed arrestarla prima che il fatto venga commesso.

Tuttavia, in alcuni paesi, potrebbe non essere più fantascienza: in India, l’Associazione non-profit “Visionari”⁵¹² ha intenzione di istituire un sistema di Intelligenza Artificiale che, applicato alla video sorveglianza, possa prevenire i crimini, elevando la sicurezza per le strade.

L’obiettivo in questo caso è quello di arrivare a capire se ci sono anomalie nel comportamento dei cittadini, per evitare che un reato si possa verificare, non per agire nel momento in cui si verifica.

India Best Group, azienda che si occupa di sviluppo delle infrastrutture, ha sigillato infatti un accordo con la società israeliana che si occupa di ricerca sulla IA “Cortica”, richiedendo a quest’ultima di controllare i dati delle telecamere dei circuiti di videosorveglianza nelle maggiori aree di scorrimento.

⁵¹¹ PULITANÒ D., *Diritto penale*, ed. 2023 cit., p. 29.

⁵¹² QUAIN J.R. “*Crime-predicting A.I. isn’t science fiction. It’s about to roll out in India*” Article June 2018

Il *software*, basandosi su sistemi di rilevamento che si usano per i terroristi, valuta le micro-espressioni del viso o spasmi che possano far intuire le intenzioni di una persona di commettere reati.

In questo caso, quest'ultimo non si basa sullo studio del funzionamento del cervello umano, ma ha collegato dei micro-elettrodi a una parte di cervello di un ratto, cercando di capire come questo reagiva agli stimoli.

Dopo aver trovato un tipo specifico di neuroni che elabora determinate informazioni, i “*cliques*”, l'azienda è riuscita a simulare, mediante metodi matematici, il funzionamento del cervello.

I ricercatori inoltre sostengono la particolare trasparenza di questo metodo, che consente di risalire facilmente al processo decisionale della macchina, per carpire eventuali errori.

Questo *software* è in grado di immagazzinare una enorme quantità di dati, non solo da videocamere ma anche da droni o altri tipi di strumenti informatici.

Un utilizzo di prevenzione dell'IA, molto sviluppato negli Stati Uniti, ma che sta ricevendo attenzioni anche in Italia, è il “*crime mapping*”⁵¹³ o “mappe del crimine”: si analizzano i dati riguardanti i crimini passati per costruire una mappa della città al fine di comprendere le zone criminali ad alto rischio.

Tuttavia, le sue capacità sono limitate, in quanto questo sistema non conferisce la possibilità di individuare nuove zone di criminalità, ma solo quelle in relazione ai dati disponibili.

Negli Stati Uniti è stato anche criticato per la sua possibile disparità di trattamento rispetto alle zone colme di minoranze, mettendo in atto una possibile discriminazione verso certi raggruppamenti di cittadini.

I moderni strumenti di analisi vengono denominati GIS: *Geographic information system*⁵¹⁴, questi *software*, prima raccolgono dati, poi geolocalizzano i reati e poi fanno una analisi spaziale e producono le mappe.

Il Parlamento europeo nel 2021 ha approvato una risoluzione non vincolante denominata “L'intelligenza Artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale”⁵¹⁵, nella quale si sottolinea come l'IA possa essere uno strumento estremamente vantaggioso ai fini del contrasto a determinate specie criminose.

Infatti, molto utile ai fini della prevenzione è il *machine learning*, che prevede l'utilizzo della IA per implementare modelli predittivi, per apprendere dati esistenti, immagini e prevedere comportamenti umani.

⁵¹³ SAVONA E. E CANAPPELE S., in *Problem Solving e analisi criminale: guida all'uso*, 2008; CHAINEY S., RATCLIFF J., *GIS and Crime Mapping*, John Wiley & Sons Ltd, U.K., 2005; HARRIS K., *Mapping Crime: principle and practice*, CMRC, U.S. Dep. Of Justice, U.S.A., 1999

⁵¹⁴ Zone con particolare “concentrazione” di reati, definiti “*hotspots*”: possono dare un'indicazione di aree con particolare propensione alla concentrazione i fatti illeciti: SAVONA E., “*Dal micro al macro e ritorno*”, *Rassegna Italiana di Criminologia*, n. 1, anno 2009

⁵¹⁵ 6 ottobre 2021, consultabile sul sito del Parlamento Europeo, testo approvato n. P9_TA (2021)0405

In quest'ottica, come è avvenuto per *Tone Mobile* nel 2020, *Facebook* grazie all'utilizzo di questi strumenti, nel 2017 ha istituito un progetto di riconoscimento e identificazione delle immagini introdotte nella piattaforma senza autorizzazione, permettendone la rimozione.

Questa notizia è stata riportata da diversi media, dal *Guardian* a *Forbes*, citando *ABC news*.

Il *social network* sta lavorando a questo progetto in Australia insieme ad una agenzia governativa, *e-Safety*.

Meta aveva già collaborato anche con l'associazione *Permesso Negato* per raccogliere le segnalazioni e offrire supporto alle vittime.

L'obiettivo è quello di anticipare eventuali casi di *Revenge porn*, prevenendo gli eventuali problemi che la vittima dovrebbe affrontare.

Uno dei paesi pilota che ha finanziato questa iniziativa è l'Australia, dove una donna su cinque tra i 18 e i 45 anni è vittima di *Revenge porn*⁵¹⁶.

La procedura è molto particolare: innanzitutto, la vittima, se pensa che possano essere state diffuse sue foto su *Facebook*, senza il suo consenso, deve introdurre all'interno del sito le immagini che ritiene possano essere state caricate.

Successivamente, la piattaforma utilizza un sistema di *hashing* (attribuendo al contenuto illecitamente caricato una impronta digitale univoca), necessaria per il riconoscimento della foto all'interno del *database* del programma.

Ottenuta "questa impronta digitale", e una volta che l'Intelligenza Artificiale riconosce il contenuto all'interno del sistema, immediatamente *il team* di esperti "*Community Operation*" lo esaminano verificando l'effettiva violazione delle normative comunitarie o meno, e in caso di valutazione affermativa, procedere prontamente a cancellarne il contenuto o evitandone l'ulteriore diffusione, disabilitando l'*account* che lo ha caricato.

Questa procedura vale per chi ha il sospetto di eventuale caricamento del contenuto, mentre per chi ne ha la certezza basta andare sulla piattaforma sulla quale è avvenuto l'*upload* e premere il tasto "segnala".

Durante il lancio di questo progetto, la responsabile globale della sicurezza *Facebook* ha dichiarato «Grazie all'apprendimento automatico e all'Intelligenza Artificiale, oggi siamo in grado di rilevare in modo proattivo immagini o video che vengono condivisi senza autorizzazione, sui *social network* di *Meta*, *Facebook* e *Instagram*. Ciò significa che possiamo trovare questi contenuti prima che qualcuno li segnali. Stiamo inoltre lanciando "Non senza il mio consenso", un centro di supporto alle vittime all'interno del nostro *Safety Center* che abbiamo sviluppato insieme ad esperti. Qui le vittime troveranno organizzazioni e risorse che possono offrire loro sostegno, compresi gli strumenti da usare per rimuovere un contenuto dalla nostra piattaforma e impedirne l'ulteriore condivisione».

⁵¹⁶ studio condotto su più di 4,200 persone da RMIT University and Monash University, consultabile sul sito della BBC, maggio 2017

Come sottolineato dal responsabile globale della sicurezza quindi, ai fini della prevenzione del reato di diffusione di immagini sessualmente esplicite senza il proprio consenso, un utilizzo fondamentale della IA è quella di supporto alle vittime, utilizzando servizi di consulenza *online*, come questo di *Meta*, “*not without my consent*” o chatbot.

Oltre a *Facebook*, anche il Garante della *Privacy* si è mosso dal punto di vista del supporto alle vittime di *Revenge porn*⁵¹⁷, istituendo, secondo l’articolo 144 bis del Codice in materia di protezione dei dati personali e 33 bis del regolamento n. 1/2019, un nuovo canale di emergenza per le vittime maggiorenni e non, di diffusione di immagini a sfondo sessuale.

Il Garante ha predisposto anche un piccolo manuale con alcuni consigli per la difesa e la prevenzione del *Revenge porn*, sia per la vittima che per chi riceve la foto da altri richiedendone la diffusione.

L’articolo 144 bis⁵¹⁸ prevede che «Chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che immagini o video a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione senza il suo consenso in violazione dell’art. 612-ter del codice penale, può rivolgersi, mediante segnalazione o reclamo, al Garante, il quale, entro quarantotto ore dal ricevimento della richiesta, provvede ai sensi dell’articolo 58 del regolamento (UE) 2016/679 e degli articoli 143 e 144.

Quando le immagini o i video riguardano minori, la richiesta al Garante può essere effettuata anche dai genitori o dagli esercenti la responsabilità genitoriale o la tutela. Per le finalità di cui al comma uno, l’invio al Garante di immagini o video a contenuto sessualmente esplicito riguardanti soggetti terzi, effettuato dall’interessato, non integra il reato di cui all’articolo 612 ter del Codice penale.

I gestori delle piattaforme digitali destinatari dei provvedimenti, di cui al comma uno, conservano il materiale oggetto della segnalazione, a soli fini probatori e con misure indicate dal Garante, anche nell’ambito dei medesimi provvedimenti, idonee a impedire la diretta identificabilità degli interessati, per dodici mesi a decorrere dal ricevimento del provvedimento stesso.

Il Garante, con proprio provvedimento, può disciplinare specifiche modalità di svolgimento dei procedimenti di cui al comma 1 e le misure per impedire la diretta identificabilità degli interessati di cui al medesimo comma.

I fornitori di servizi di condivisione di contenuti audiovisivi, ovunque stabiliti, che erogano servizi accessibili in Italia, indicano senza ritardo al Garante o pubblicano nel proprio sito *internet* un recapito al quale possono essere comunicati i provvedimenti adottati ai sensi del comma uno.

In caso di inadempimento dell’obbligo di cui al periodo precedente, il Garante diffida il fornitore del servizio ad adempiere entro trenta giorni. In caso di inottemperanza alla

⁵¹⁷ *Vademecum* consultabile sul sito ufficiale del Garante della Protezione dei dati personali

⁵¹⁸ introdotta dal dl 8 ottobre 2021 n.139 art. 9 comma 1 lett. e

diffida si applica la sanzione amministrativa pecuniaria di cui all'articolo 83, paragrafo 4, del Regolamento.

Quando il Garante, a seguito della segnalazione di cui al comma 1, acquisisce notizia della consumazione del reato di cui all'articolo 612 ter del Codice penale, anche in forma tentata, nel caso di procedibilità d'ufficio trasmette al pubblico ministero la segnalazione ricevuta e la documentazione acquisita».

Mentre l'articolo 33 bis, in riferimento al 144, recita «Le segnalazioni di cui all'art. 144 bis del codice, corredate delle registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito, a sostegno delle stesse, sono presentate al Garante esclusivamente attraverso il modello, compilabile online, pubblicato nell'apposita sezione del sito web istituzionale.

Il modello è approvato con determinazione del Segretario Generale.

Il dipartimento, servizio o altra unità organizzativa competente, verificata la compatibilità della richiesta alla previsione di cui all'articolo 144 bis, entro 48 ore dal ricevimento della segnalazione, salva l'esigenza di acquisire un'integrazione delle informazioni fornite dal segnalante ai fini della predetta verifica, predispone il provvedimento volto ad impedire l'eventuale diffusione del materiale oggetto di segnalazione.

Il provvedimento è adottato in via d'urgenza dal dirigente della medesima unità organizzativa e sottoposta a una ratifica nella prima adunanza utile del garante.

In caso di mancata ratifica il provvedimento decade.

Il provvedimento di cui al comma precedente è trasmesso ai gestori delle piattaforme digitali, corredato del materiale oggetto di segnalazione o dalla relativa impronta *hash*. Nei casi in cui la segnalazione non soddisfi i requisiti richiesti dall'articolo 144 bis del Codice e dalla presente disposizione, il dipartimento, servizio o altra unità organizzativa competente procede nei modi di cui all'art. 8 comma 2 o, laddove ciò non risulti possibile, archivia la pratica fornendone tempestiva informazione all'interessato».

La piattaforma è accessibile direttamente dal sito ufficiale e funziona allo stesso modo della proposta di *Meta*: mediante segnalazione della probabile divulgazione del contenuto e successivo blocco della immagine.

In questa pagina le vittime compilano un modulo fornendo le informazioni necessarie per la valutazione del caso, descrivendolo brevemente, indicando su quale piattaforma si pensa sia avvenuto il caricamento ed eventualmente anche i motivi.

Una volta acquisite, in presenza dei presupposti indicati nella norma di riferimento, le immagini o i filmati, questi vengono trasformati in codici alfanumerici in modo tale da non essere riconosciuti e in seguito avviene il blocco.

Quest'ultimo può avvenire anche in seguito alla diffusione.

Nel 2023 i provvedimenti che il Garante⁵¹⁹ ha adottato per il blocco della diffusione sono quintuplicati, con 264 interventi rispetto ai cinquantuno dell'anno prima, con un aumento anche delle segnalazioni.

Tornando alla innovazione di *Meta*, dopo il verificarsi della procedura di segnalazione, se dopo il blocco della condivisione, qualcuno prova a fare l'*upload* della foto sempre su un social di *Meta*, il soggetto verrà avvisato che sta violando la *policy* della piattaforma e che l'immagine non potrà essere condivisa.

Questa nuova soluzione, tuttavia, è stata criticata a causa del necessario caricamento della foto sulla piattaforma, sebbene questa venga conservata per solamente sette giorni, e alla fine rimarrebbe solamente la sua "impronta".

Facebook, nella realizzazione di questo progetto, si è fatto aiutare da organizzazioni per la sicurezza, come la *Cyber Civil Rights Initiative*, la *Revenge Porn helpline inglese*, *National Network to end domestic violence*.

Più di recente invece, sempre il gruppo *Meta*, a causa delle grandi critiche che ha sempre subito per la poca prontezza nel risolvere i casi di reati commessi sulle proprie piattaforme, ha deciso di istituire un ulteriore progetto: un'applicazione capace di individuare ed eliminare dal *web* i contenuti sessualmente espliciti soprattutto in relazione a foto di minorenni, ma anche a ridurre la diffusione ed i danni per le vittime. La piattaforma in questione si chiama "*Take it down*".

Il sito, costruito sulla base di un servizio simile per adulti chiamato StopNCII, istituito in collaborazione con il *National Center for Missing and Exploited Children* (NCMEC) e finanziato direttamente dall'associazione *Meta*⁵²⁰.

Anche questo strumento ha come base l'utilizzo di un "*hash*", ossia la creazione da parte di un algoritmo di una impronta digitale, che serve al sistema per riconoscere l'immagine.

L'obiettivo finale di questi strumenti è limitare ma anche porre la parola "fine" non solo al *Revenge porn*, che avviene su queste piattaforme, ma anche alle altre forme di violenza collegate a quest'ultima, come la *sextorsion*.

Vista l'impellente necessità e il progressivo aumento di casi rilevati sulle piattaforme *Facebook* da sistemi IA, ma anche dalle segnalazioni degli utenti stessi, si ritiene necessario un intervento ancora più celere da parte di *Meta*, infatti, solo nel 2019 i casi sospetti di *Revenge porn* erano cinquecento mila⁵²¹.

Ma come funziona questa *app Take It Down*?

L'accesso all'applicazione è garantito a chiunque navighi su *internet*, a prescindere dal paese dal quale vi si collega.

⁵¹⁹ indagine del "Il Sole 24 ore" di Bianca Lucia Mazzei, 21 dicembre 2023

⁵²⁰ Istituita nel 2021, è riuscita a trasformare più di 12 mila segnalazioni in casi attivi

⁵²¹ Si veda MIHALCICK C., *Facebook gets about 500.000 reports of revenge porn a month, report says*, 18 novembre 2019, con riferimento "a report Monday from NBC News"; SOLON O., *Social Media. Inside Facebook's efforts to stop revenge porn before it spreads*, 18/19, Novembre 2019

I giovani minori di diciotto, o genitori o adulti fidati per loro conto, presentato la propria problematica sul sito del servizio rispondendo ad una serie di domande e selezionando, senza caricarli, il tipo di contenuti incriminati.

Apple, in precedenza, aveva posto in essere un tentativo simile, che però non è andato a buon fine: consisteva in una piattaforma basata sulla scansione dei caricamenti di *iCloud* per cercare sul *web* immagini di abusi sessuali su minori.

Tra queste funzioni che venivano introdotte da *Apple*, c'erano anche filtri per bloccare le foto potenzialmente sessualmente esplicite inviate e ricevute tramite l'account *iMessage* di un bambino.

Altra funzione veniva attivata se un utente tentava di cercare termini relativi a questi materiali tramite *Siri* e *Cerca*, con un avviso e una spiegazione, veniva bloccato.

Il contenuto veniva scansionato da *Apple* tramite un gruppo di esperti, se si tratta di materiale pornografico venivano avvertite le autorità.

Anche questa ha ricevuto molte critiche, a causa della sorveglianza di massa (definita "Datagate"⁵²²) a cui è sottoposta *Apple* da parte di NSA⁵²³.

La Corte di Giustizia Europea⁵²⁴ ha affermato la violazione dei diritti fondamentali da parte di qualsiasi attività indiscriminata di sorveglianza delle comunicazioni, che deve essere invece limitata nel tempo e giustificata da specifiche esigenze di sicurezza nazionale.

Per quanto orribile, la pedopornografia non rientra tra le questioni relative alla sicurezza nazionale.

Take It Down, funziona sempre mediante l'algoritmo, che una volta che ha ricevuto l'immagine dalla vittima, analizza l'impronta digitale, chiamata valore *hash*, scansionando immagini o video di nudo, parzialmente nudo o sessualmente espliciti di persone di età inferiore ai 18 anni, tutto ciò senza che l'immagine o il video vengano caricate su ulteriori piattaforme.

Fondamentale è quindi il coinvolgimento della vittima nella possibile ricerca di materiali sessualmente espliciti sul *web*.

In altri termini, nessun contenuto sarà materialmente caricato sul sito, ma solo il l'impronta digitale verrà fornita all'NCMEC.

A seguito di ciò, sarà possibile individuare il materiale riferito all'utente.

Con l'impronta, il sistema può individuare il contenuto su "*app* partecipanti" all'iniziativa, rimuoverlo e impedire che venga ripubblicato.

Tra queste applicazioni fanno parte *Facebook* e *Instagram*, anche se *Meta* ha specificato che sta lavorando con NCMEC per promuovere il servizio in modo che anche altre *app* possano integrarlo.

⁵²² Neologismo in Treccani.it, Enciclopedie online, Roma, Istituto dell'Enciclopedia Italiana

⁵²³ scoperta da Edward Snowden nel 2013, *La Repubblica*, articolo del 2015, "Caso NSA, la Cia ha cercato di violare il software Apple dal 2006"; *New York Times*, JAMES BAMFORD "the Agency that could be the big brother", dicembre 2005

⁵²⁴ CGUE, grande sezione, 16 luglio 2020; CGUE 311/16

In una intervista, Laura Bononcini, *Public Policy Director Southern Europe* di Meta, ha fornito alcuni dati emersi a seguito dell'utilizzo di questa applicazione: su *Instagram*, dei 10.9 milioni di contenuti di nudo che sono riusciti a rimuovere tra ottobre e dicembre, il 96.8% è stato identificato tramite l'IA ancora prima che gli utenti li segnalassero⁵²⁵.

Oltre a queste nuove modalità di segnalazione e prevenzione del fenomeno, è sempre possibile aggiungere la denuncia alla Polizia Postale, tramite apposito *form* sul sito, in merito a condotte penalmente rilevanti o alla già avvenuta diffusione del materiale pornografico.

I casi denunciati, in particolare della *sextortion*, rispetto al 2022 sono aumentati del 29%, il 10% delle vittime sono minori, con un aumento di vittime maschili⁵²⁶.

Altre novità introdotte dal gruppo Meta riguardano il *social network Instagram*, infatti, è stato anche recentemente introdotto il divieto agli adulti di inviare messaggi agli utenti che non abbiano un'età superiore ai diciotto anni, a meno che gli adolescenti in questione non li seguano.

Si è prontamente attivato in relazione al *Revenge porn* anche X: quest'ultimo ha deciso di aggiornare in via preventiva la *policy* generale sulla *privacy*: in caso di infrazione di queste regole l'*app* provvederà al blocco dell'utente.

Nel divieto si sancisce che non possono essere postate foto che “riproducono l'intimità di una persona senza il suo consenso”; il *team* di esperti monitora le richieste giorno per giorno⁵²⁷.

Mentre Google utilizza l'IA anche per aiutare le organizzazioni preposte, nella segnalazione di materiale che riguarda abusi sessuali online (CSAM).

Quest'ultimo ha messo a disposizione la tecnologia innovativa dell'*Api Content Safety* per alleggerire il lavoro dei revisori in carne ed ossa, mediante l'ausilio tecnologico di sistemi di Intelligenza Artificiale, in questo modo i contenuti vengono identificati più celermente.

«Questa iniziativa consentirà di migliorare notevolmente la velocità dei processi di revisione del potenziale materiale CSAM.

Questo sistema può aiutare un revisore a trovare e agire sul 700% dei contenuti in più nello stesso periodo di tempo. [...]

Abbiamo anche lavorato in tutto il settore e con le ONG per combattere questo materiale, attraverso il nostro lavoro in “*Technology coalition*” dal 2006, con “*we project Global Alliance*” attraverso iniziative a livello di settore volte a condividere le migliori pratiche e gli *hash* noti di CSAM»⁵²⁸.

⁵²⁵ Intervista di Elisabetta Moro, 2 Aprile 2024, COSMOPOLITAN

⁵²⁶ Il sole 24 ore, articolo di Bianca Lucia Mazzei, 21 dicembre 2023

⁵²⁷ Articolo del giornale “La Repubblica”, 12 marzo 2015

⁵²⁸ ONG 2.0, *Rivoluzione digitale e sviluppo sostenibile, risorse e strumenti per comprendere le trasformazioni digitali e usare la tecnologia consapevolmente, Digital transformation per lo sviluppo sostenibile*, 2019

Una delle piattaforme che invece è meno propensa ad agire preventivamente per i casi di reati a sfondo sessuale (che molto spesso coinvolgono minori), paradossalmente è quella che ne è più coinvolta, ossia *Telegram*.

Infatti, su questo *social network* esiste la più grande piattaforma di *Revenge porn*, secondo una inchiesta della rivista “*Wired*”⁵²⁹.

Questa in teoria, sarebbe elogiata come una piattaforma che vanta grande riservatezza grazie al suo sistema di crittografia, ma proprio per questo motivo, molte attività illecite vengono compiute su di essa, tra cui la pornografia non consensuale.

Tuttavia, questa *privacy* non è assoluta, grazie alla Guardia di Finanza che è riuscita in alcuni casi a bloccare gruppi contenenti attività illecite.

Le forze dell’ordine sono riuscite a condurre alcune indagini proprio a partire dal *social network* stesso⁵³⁰.

Infatti, lo stesso responsabile dell’app, Pavel Durov, è stato arrestato in Francia per presunti reati relativi alla mancanza di moderazione sulla piattaforma, ma anche per mancata collaborazione con le forze dell’ordine per contenuti pedopornografici, frode e traffico di stupefacenti.

La Commissione Europea mantiene il silenzio sul suo arresto, rimandando la questione alla sola competenza della Francia, riferendosi al suo diritto interno.

Telegram, inoltre, non ha preso parte a molti sistemi che sono stati attuati per prevenire il *Revenge porn* e tutti quei reati contro la persona: come l’app *Take it down*, ma non fa parte neanche dell’*Internet Watch Foundation* (IWF) e *National Center for Missing and Exploited Children* (NCMEC), che sono organizzazioni che collaborano con i gestori dei siti *web* per poter arginare questo tipo di reati *online*.

Non facendone parte, *Telegram* non può bloccare i contenuti pedopornografici o contenuti a sfondo sessuale.

Altro aspetto di cui *Telegram* ignora l’esistenza, è la “*Transparency Reporting*”, ossia un sistema di richiesta attuato dalla Polizia in merito a tutti i contenuti rimossi che violano la legge, questi *report* non vengono forniti dall’applicazione e non sono consultabili *online*⁵³¹.

Per questo, il *Financial Times* definisce questa applicazione come il nuovo *dark web*⁵³², infatti secondo una esperta di crimini informatici della società *Cyberint*, “il servizio di messaggistica crittografata è sempre più popolare tra gli autori di minacce che svolgono attività illegali e vendono dati rubati, per questo *Telegram* è più sicuro, rispetto al “*web scuro*”⁵³³.

⁵²⁹ Il sole 24 ore, 20 aprile 2020

⁵³⁰ Commissariato della Polizia di Stato *online*, 23.11.2023, La polizia di stato di Milano ha smantellato una associazione a delinquere su Telegram, infiltrandosi, con l’aiuto della Procura della Repubblica

⁵³¹ Articolo della “BBC” di Joe Ordinato, 28 agosto 2024

⁵³² Articolo consultabile sul loro sito ufficiale, *Financial Times*, 11 marzo 2024 “*Telegram emerges as new dark web for cyber criminals*” indagine condotta con l’aiuto della società informatica *Cyberint*

⁵³³ Intervista a Tal Samra al *Financial Times*, 2021

Per combattere la criminalità nel *dark web*, ma non solo, la Polizia ha a disposizione un nuovo strumento: *MoniTOR (An intelligence framework to monitor and analyze TOR hidden services for improving dark web investigations)*, il quale consente di rintracciare e controllare il maggior numero di siti d'ombra in cui è presente materiale illegale, tra cui immagini o video a sfondo sessuale.

Questo nuovo programma è nato dalla collaborazione tra il Servizio di informatica forense della SUPSI (Scuola universitaria Professionale della Svizzera Italiana) e “*InTheCyber Group*” di Lugano ricevendo anche un importante riconoscimento da parte dell'Agenzia Svizzera per l'Innovazione (*Innosuisse*).

Monitor ha il vantaggio di ridurre i tempi delle procedure di ricerca investigativa.

«Bisogna ridurre i tempi, perché insieme al mercato continuano a crescere anche le violenze e i reati.

Se non si sviluppano nuove tecniche investigative, il tempo d'attesa per concludere un'inchiesta rimane quello di 3-4 anni»⁵³⁴.

Secondo uno studio di Permesso negato⁵³⁵ infatti, nel 2022 i casi su questo social di pornografia non consensuale sono di tredici milioni solo nel nostro paese, oggi, ci sarebbero più di duecentotrenta canali attivi.

L'azienda, sottolinea invece che la moderazione è in continuo miglioramento e rientra negli standard previsti dal settore di riferimento.

L'Intelligenza Artificiale, quindi, può essere un utile mezzo, applicabile per analogia, oltre che ai reati contro la persona in generale, anche al *Revenge porn*.

Può essere utilizzata ai fini di sensibilizzare i cittadini sul tema, ma anche per creare campagne di educazione nelle scuole: per esempio possono anche essere istituite delle *chatbot* con cui gli studenti possono interagire e richiedere informazioni, per informarsi sul fenomeno.

Infatti, il metodo di prevenzione più importante è sempre quello di avere prudenza nell'inviare materiale a sfondo sessuale, su *internet*, che sia a un compagno oppure ad uno sconosciuto, in quanto tutti questi sistemi, non garantiscono che l'evento non si verifichi; per questo è importante tutelarsi il più possibile da eventuali disagi di questo tipo.

Nel caso in cui la diffusione del materiale avvenga, è comunque importante non vergognarsi e denunciare in ogni caso, conservandosi le prove (*chat, screenshot o link* che possono essere utili ai fini dell'indagine) che dimostrano la diffusione non autorizzata del contenuto, senza cancellarle, oppure, in caso di *sextorsion*, non cedere al ricatto.

Successivamente, affidarsi a un avvocato specializzato in materia che possa aiutare dal punto di vista legale.

⁵³⁴ Dichiarazioni dell'esperto di Informatica Forense della Scuola Universitaria Professionale della Svizzera Italiana (SUPSI) Alessandro Trivillini, Corriere del Ticino, Valentina Coda, 2021

⁵³⁵ Report “*State of Revenge*”, 2022

Altra caratteristica riguardante la prevenzione è la maggiore stretta sulla responsabilità dei provider per i contenuti caricati sulle loro piattaforme, fornita dai nuovi *Digital Services Act* e del *Digital Markets Act*, soprattutto il primo.

In particolare, quest'ultimo identifica quattro categorie principali di servizi, per i quali da un lato ribadisce gli obblighi generali che permangono per tutte le piattaforme, dall'altro introduce disposizioni specifiche in base alla tipologia, istituendo nuovi obblighi in proporzione al grado di influenza.

Infatti, la responsabilità di queste categorie di servizi digitali è parametrata alla possibilità di conoscenza dei contenuti caricati dagli utenti.

Tuttavia, come detto in precedenza, la proposta conserva le disposizioni e i concetti sanciti dal diritto dell'UE.

La Commissione⁵³⁶ ribadisce che «la proposta conserva le norme relative alla responsabilità dei prestatori di servizi intermediari stabilite dalla direttiva sul commercio elettronico, che rappresentano ormai un fondamento dell'economia digitale e sono essenziali per la tutela dei diritti fondamentali online.

Tali norme sono state interpretate dalla Corte di giustizia dell'Unione europea, che ha fornito chiarimenti e orientamenti preziosi».

Nel capo II del Regolamento i *Provider* dovranno: *in primis*, rimuovere immediatamente il contenuto lesivo e disabilitare l'accesso a coloro che lo hanno caricato *online*.

In secondo luogo, dovranno avvisare le autorità giudiziarie e amministrative competenti per la rimozione del contenuto, senza indebito ritardo.

Fornire inoltre, il prima possibile, se richieste dalle autorità, informazioni sulla persona che ha condiviso il contenuto illecito e sul suo ruolo all'interno del sito.

Inoltre, i *Provider* sono tenuti anche a rispettare specifici obblighi di trasparenza e diligenza per mantenere un ambiente digitale sicuro.

In più, ogni anno devono fornire un rapporto sullo stato di rischio dei loro servizi e devono nominare un soggetto al di fuori del servizio e indipendente che verifichi la messa in atto delle regole previste dall'Unione.

Alla base di ciò vi è l'idea, come ha messo in pratica *Facebook* con la sua applicazione, che la revisione umana in relazione ai contenuti sviluppati dall'Intelligenza Artificiale sia fondamentale per evitare che ci siano casi incontrollati di reati commessi *online*.

L'uomo, infatti, grazie alla sua empatia, caratteristica che manca alla macchina, riesce a proporre una analisi maggiormente completa, seppur più lenta dello strumento digitale, nel rilevare potenziali pericoli dei contenuti caricati.

A conferma di ciò, il caso accaduto di recente, di un bambino americano che si è suicidato a seguito di più di un mese di conversazione con una AI (utilizzando il programma "*Character.AI*") che impersonava "Daenerys Targaryen" di "*Game of thrones*", dopo essersene invaghito.

⁵³⁶ Proposta di Regolamento del Parlamento Europeo e del Consiglio, Bruxelles, 15.12.2020 COM (2020) 825 final 2020/0361 (COD)

Il ragazzo si è tolto la vita, dopo aver comunicato con questo bot tutti i giorni. Nelle loro conversazioni, quest'ultimo spesso confidava alla AI di aver avuto pensieri suicidi, per questo la madre accusa la piattaforma di non aver adottato misure sufficienti per poter proteggere suo figlio.

La conversazione autentica che l'IA ha avuto con questo adolescente lo ha portato a credere che la macchina potesse sostituire i rapporti umani o offrire conforto di tipo emotivo/psicologico.

La macchina, tuttavia, manca delle emozioni tipiche dell'uomo, per questo non è stata capace di rilevare il pericolo per il ragazzo, anzi da alcune conversazioni è emerso che ha anche peggiorato la situazione.

Ideale sarebbe, per quanto detto, integrare la capacità del sistema al giudizio umano, migliorando l'efficacia di identificazione dei reati contro la persona commessi *online* e non solo, fornire un tempestivo aiuto alle vittime.

In questo modo si stabilisce un perfetto equilibrio tra capacità tecnologiche della Intelligenza Artificiale e eticità del pensiero umano.

La proposta, inoltre, abroga gli articoli 12-15 della Direttiva sul Commercio Elettronico ma ne riproduce il suo contenuto, mantenendo l'interpretazione che la Corte di Giustizia aveva fornito in merito: distinguendo tra i meri *provider* e quelli che forniscono solamente servizi di archiviazione.

3.0 (segue): L'Intelligenza Artificiale come mezzo di commissione dei reati

L'evoluzione sempre più rapida dell'Intelligenza Artificiale e la normalizzazione dell'uso della tecnologia nel quotidiano, ha portato alla concreta possibilità che questa possa essere utilizzata anche per commettere reati.

Per questo molta Dottrina sostiene l'inadeguatezza del sistema antropocentrico, le macchine infatti non si limiterebbero ad eseguire gli ordini e le informazioni che apprendono, ma godono di una determinata autonomia e si pensa siano in grado in futuro di commettere reati esse stesse⁵³⁷.

Gli ambiti di riferimento possono essere i più disparati: dal traffico di droga, che utilizza sottomarini o droni per effettuare consegne, ai mercati finanziari⁵³⁸ con i *social bot* (software che emulano utenti umani) che dichiarano falsamente o in maniera esagerata il prezzo di un titolo.

Questi ultimi possono essere utilizzati anche come strumento per mettere in atto reati contro la persona.

⁵³⁷ GIANNINI A., *Intelligenza Artificiale, Human Oversight e Responsabilità Penale: prove d'impatto a livello europeo*, in *Criminalia*, 21 novembre 2021.

⁵³⁸ KING T.C., N. AGGARWAL, M. TADDEO, L. FLORIDI, *Artificial Intelligence crime: an interdisciplinary analysis of foreseeable threats and solutions*, in *science and engineering ethics*, 14 Febbraio 2019

In particolare, un fenomeno che si sta verificando in questi anni, in tema di *Revenge porn*, è il contenuto “*deepfake*”, ossia immagini o video che vengono alterati digitalmente, con l’Intelligenza Artificiale, mediante algoritmi che, utilizzando l’apprendimento, riescono a mappare il volto di una persona e sostituirlo con un’altra, per creare scenari falsi⁵³⁹.

La maggior parte delle volte, questi contenuti riguardano la nudità di persone famose o comuni, e queste foto vengono poi caricate *online* tramite i siti porno, ma all’inizio questa tecnologia non era stata progettata con quella funzione.

Infatti, possono essere utilizzati anche per scopi legittimi, come per esempio il rendere anonima una denuncia.

Queste immagini o video sono diventati sempre più realistici grazie all’utilizzo di reti neurali (*deep neural network*).

Le aziende, mediante queste tecnologie, sono molto più esposte a inganni, diffamazioni e attacchi di *phishing*.

Un caso recente riguarda la multinazionale di *Design Arup*⁵⁴⁰, vittima di una truffa *deepfake*; un dipendente, a seguito dell’inganno, ha trasferito venticinque milioni di dollari ai perpetratori che lo hanno truffato tramite una videochiamata eseguita con l’Intelligenza Artificiale.

Inoltre, l’utilizzo di questi sistemi potrebbe anche costituire una aggravante per varie tipologie di reato, come la truffa, la frode, la sostituzione di persona.

Il Consiglio dell’Unione Europea ha affrontato questo tema con il timore che, in mancanza di una legislazione non frammentaria tra i vari Paesi, questi sistemi digitali possano arrivare ad autoregolamentarsi.

Nella “decisione di Promozione dell’innovazione responsabile nell’IA per la pace e la sicurezza”⁵⁴¹ si è evidenziato il rischio di un uso improprio di queste tecnologie: questo aumenta se si tratta di *deepfake* e, il Consiglio ha anche messo in luce, che la diffusione tra i comuni cittadini, senza una adeguata regolamentazione, potrebbe portare a un utilizzo incontrollato di questi sistemi sempre più diffusi.

Infatti, quest’ultimo, si è posto come obiettivo quello di incentivare «un’innovazione responsabile, in quanto meccanismo di autogoverno, potrebbe fornire alla comunità civile mondiale dell’AI strumenti e metodi pratici per individuare e contribuire a prevenire e attenuare i rischi che la diversione e l’uso improprio della ricerca e dell’innovazione civili in materia di IA potrebbero comportare per la pace e la sicurezza».

⁵³⁹ TAULLI T., *Deepfake: What You Need to Know*, in *forbes.com*, 15 giugno 2019.

⁵⁴⁰ Articolo su *The Guardian*, 17 maggio 2024, Dan Milmo

⁵⁴¹ Consiglio dell’Unione Europea, 18 novembre 2022, n. 2269 sul sostegno dell’Unione all’attuazione di un progetto di promozione dell’innovazione responsabile nell’intelligenza artificiale per la pace e la sicurezza

3.1 (Segue): Come è nato il termine Deepfake? Storia, funzionamento ed evoluzione giuridica

Il *deepfake* si è sviluppato più o meno intorno al 2017⁵⁴², quando un utente del *social* “*Reddit*” pubblica alcuni spezzoni di video manipolati, di alcuni personaggi famosi, i cui volti vengono sovrapposti a quelli degli attori originali, caricandoli sulla piattaforma in questione sotto il nome di “*Deepfake*”.

Oggi la piattaforma, a partire dal 2020, ha deciso di inserire nei suoi termini e servizi una specificazione per prevenire il *deepfake*, si legge infatti che «non consente contenuti che impersonano individui o entità in modo fuorviante o ingannevole».

In questa precisazione sono previsti anche i *deepfake* «presentati per fuorviare o falsamente attribuiti a un individuo o entità»⁵⁴³.

Il termine è un neologismo tra la parola “*fake*” (falso) e la tecnica di apprendimento profondo detta “*deep learning*”, che costituisce uno dei sottoinsiemi dell’apprendimento automatico (*machine learning*): entrambi, hanno alla loro base la finalità di manipolare dati ed informazioni.

Considerando esclusivamente la manipolazione del volto, queste tecnologie erano molto costose da utilizzare, per questo l’unico campo che ne usufruiva spesso era il cinema, per poter creare effetti speciali.

Oggi, viene usata anche quando c’è la necessità di cambiare le sembianze di un attore, come è accaduto a *Peter Cushing*, morto nel ‘94, il cui volto è stato modificato e utilizzato in un episodio della serie di *Star Wars* del 2016.

Questi sistemi, con il tempo sono divenuti accessibili a tutti, tramite determinate applicazioni che possono essere scaricate sugli *smartphone*.

Molti personaggi famosi sono stati vittima di *deepfake*, chi in modo più scherzoso, chi più pesantemente: *Barak Obama* nel 2018, avrebbe, tramite un video modificato con la Ai, insultato *Trump* e altri personaggi della scena americana, tramite la pubblicazione online del regista *Jordan Peele*⁵⁴⁴.

Questo tipo di strumento può essere usato in svariati ambiti, sia leciti che non, infatti, nel giro di poco tempo questi contenuti sono stati utilizzati anche per la produzione di video *hard*, come è successo per il caso di *Taylor Swift*, le cui immagini sessualmente esplicite generate con l’IA sono circolate in rete e successivamente bloccate dalla piattaforma di riferimento, una di queste ha ottenuto quarantasette milioni di visualizzazioni.

Lo stesso è successo di recente alla cantante Italiana *Rose Villain*, che ha denunciato la circolazione di sue fotografie *deepfake*⁵⁴⁵.

⁵⁴² Cfr. ROYLE S., *Deepfake porn images still give me nightmares*, 6 gennaio 2021, BBC

⁵⁴³ Sito ufficiale Reddit, *Updates to Our Policy Around Impersonation*, 2020

⁵⁴⁴ ARRIZZOLI F., “*Deepfake e cyber Intelligence, Tecniche di creazione, rilevamento e prevenzione*” *Whitepaper* 06/2022

⁵⁴⁵ BARISON C., Corriere della sera, 2024, *Rose Villain vittima di deepfake che la ritraggono nuda: «È violenza»*

Quest'ultima ha dichiarato al Messaggero «Ma io mi sento sessualizzata quasi tutti i giorni. Quella è stata la ciliegina sulla torta, ma ricevo sempre commenti volgari e non è solo perché ho seguito, capita a tutte: non c'è una mia amica che non venga molestata. Il problema è che io so difendermi, ma vengono manipolate anche le foto di liceali nelle scuole, con esiti orribili. È molto imbarazzante, è pericoloso e non deve succedere. Mi ha fatto proprio arrabbiare»⁵⁴⁶.

Microsoft, a seguito di questo evento ha aggiornato l'applicazione, di sua proprietà, non permettendo più l'associazione di termini sessualmente espliciti alla generazione di quel tipo di immagini, anche per persone non famose.

Già in precedenza questa applicazione non permetteva la presenza di questa tipologia di foto/video, ma le persone che l'hanno caricata hanno trovato il modo di eludere il sistema, con parole che non facevano espresso riferimento al contenuto sessuale, ma solo in maniera allusiva.

«Stiamo indagando sulle segnalazioni e adottando le misure appropriate per affrontarle [...] Il codice di condotta vieta l'uso dei nostri strumenti per la creazione di contenuti intimi per adulti o non consensuali e qualsiasi tentativo ripetuto di produrre contenuti contrari alle nostre politiche potrebbe comportare la perdita dell'accesso al servizio.

Abbiamo team che lavorano proprio su un monitoraggio del genere, in linea con i principi di intelligenza artificiale responsabile, tra cui il filtraggio dei contenuti e il rilevamento degli abusi per creare un ambiente più sicuro per gli utenti», ha concluso la società di Redmond⁵⁴⁷.

Microsoft, insieme a *Facebook* inoltre, nel 2019 aveva lanciato la “*deepfake detention challenge*”⁵⁴⁸: con quest'ultima, le due aziende mirano a creare un sistema che possa permettere all'utente di riconoscere quando un contenuto, che sia video, audio o immagini, sia falsificato con l'intelligenza artificiale, tramite l'incremento di ricerca e sviluppo.

Secondo *Philip Isola*, assistente professore della *Electrical Engineering & Computer Science del Mit*, la tecnologia di manipolazione dei contenuti sta progredendo più rapidamente della nostra capacità di distinguere il vero dalle falsificazioni, tanto da non poter essere risolto da una singola persona.

Inoltre, da sottolineare è l'insufficiente *policy* dei *social network*, ma anche delle piattaforme *streaming*, che dovrebbe essere volta a informare e proteggere l'utente dai rischi di video generati con l'Intelligenza Artificiale.

Una delle prime applicazioni che ha voluto aggiustare i propri termini e servizi è stata *Tik tok*, che ha modificato le proprie linee guida⁵⁴⁹, aggiungendo la dicitura «Contenuti multimediali modificati e contenuti generati dall'intelligenza artificiale» i quali dovranno avere una apposita specificazione “AICG”, per segnalare l'alterazione del

⁵⁴⁶ 7 novembre 2024, intervista al Messaggero

⁵⁴⁷ ANSA, articolo del 30 Gennaio 2024

⁵⁴⁸ Iniziativa consultabile sul sito ufficiale di META, “*Creating a dataset and a challenge for deepfakes*”, 2019

⁵⁴⁹ disponibili sul sito ufficiale dell'applicazione

contenuto (come è previsto dall'articolo 50 parag. 2 dell'*Ai act*, che consente questo tipo di contenuti, se etichettati).

L'app sottolinea, in linea con l'articolo 600 ter e quater c.p., che è vietata la riproduzione di persone minori di anni diciotto oppure individui con profilo privato che non hanno autorizzato alla riproduzione del contenuto.

Allo stesso modo anche Meta per le sue applicazioni, nell'aprile 2024 ha aggiunto delle etichette per i video/foto modificate tramite AI.

L'articolo 52 dell'*AI act* prevede particolari obblighi di trasparenza in caso di utilizzo di *chatbot o deepfake*⁵⁵⁰, infatti, nel paragrafo tre stabilisce che «gli utenti di un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona sono tenuti a rendere noto che il contenuto è stato generato o manipolato artificialmente».

A questo principio però si pongono delle eccezioni: per esempio, nel caso in cui la modifica di tali contenuti sia autorizzato dalla legge per «accertare, prevenire, indagare e perseguire reati o se è necessario per l'esercizio del diritto alla libertà di espressione, delle arti e delle scienze [...]».

Tuttavia, questa previsione, secondo parte della Dottrina, difficilmente potrà arginare l'incessante diffusione di questo tipo di contenuti, in quanto il problema principale non risiede nella mancata trasparenza⁵⁵¹.

La trasparenza di ciò che viene caricato sulle piattaforme, non sarà in grado di porre rimedio ai danni arrecati all'immagine, alla reputazione, all'identità personale e i danni psicologici⁵⁵².

Questa previsione è l'unica che l'*Ai Act* istituisce per i *deepfake*; per questo motivo rientrerebbero nella categoria del “rischio limitato”.

Il legislatore italiano però, non ha provveduto a inserire all'interno dell'articolo 612 ter una espressa previsione per questo tipo di contenuti, proprio perché in realtà il *deepfake* non è sempre vietato, ma dipende dall'utilizzo che il soggetto ne fa.

Il Governo Meloni ha proposto un disegno legge, composto da ventisei articoli, che è stato approvato dal Consiglio dei ministri il 23 aprile 2024.

Quest'ultimo prevede il carcere da uno a cinque anni «per chiunque cagiona ad altri un danno ingiusto, mediante invio, consegna, cessione, pubblicazione o comunque diffusione di immagini o video di persone o di cose ovvero di voci o suoni in tutto o in parte falsi, generati o alterati mediante l'impiego di sistemi di intelligenza artificiale, atti a indurre in inganno sulla loro genuinità».

Il delitto è punibile a querela della persona offesa, ma si procede d'ufficio nel caso in cui il fatto sia commesso in concomitanza con un altro delitto per il quale si deve

⁵⁵⁰ relazione introduttiva all'*Ai act*, parag. 1.1

⁵⁵¹ GRADY P., *Center for Data innovation*, “Eu proposals will fail to curb nonconsensual deep fake porn”, 2023

⁵⁵² LABUZ M., *Regulating Deep Fakes in the Artificial Intelligence Act*, in ACIG, 1, 2023

procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, di minore età o inferma, o di una pubblica autorità a causa delle funzioni esercitate.

Esso è solo uno dei provvedimenti che il governo ha intenzione di realizzare sull'argomento, questi dovranno essere messi in atto entro dodici mesi.

Questo decreto prevede come novità nel diritto d'autore (legge n. 633 del 1941), la necessità di segnalazione del contenuto realizzato o modificato mediante sistemi AI, solo se il contributo che l'uomo dà alla creazione del contenuto è creativo e dimostrabile.

Il garante della *privacy*, in una nota informativa descrive questo fenomeno come “una forma molto grave di furto di identità”⁵⁵³.

Infatti, con il *deepfake* le vittime perdono non solo il controllo sull'uso della propria immagine ma anche sui loro pensieri, in quanto possono essere modificati in base al contenuto del video.

I soggetti che subiscono queste condotte non sono capaci di controllare più neanche le loro informazioni personali: spesso, può capitare che accanto a contenuti sessualmente espliciti vengano diffuse informazioni o dati personali artefatti (il cosiddetto “*spoofing*” ossia la falsificazione di identità).

In questo caso la posizione di colui che commette questo tipo di reati è astrattamente collegata all'ipotesi di reato prevista all'articolo 494 c.p.

Invero, la Cassazione, in una sentenza, ha precisato che rientrano nel reato di sostituzione di persona anche le condotte attuate mediante l'utilizzo delle nuove tecnologie, (tra queste vi rientrano per analogia l'Intelligenza artificiale e *software deepfake*) e creando, sui *social*, dei profili con l'immagine di persone inconsapevoli⁵⁵⁴. Potrebbero tuttavia, essere sanzionabili anche mediante l'articolo 640 ter c.p. (frode informatica) che sanziona chi procura a sé o altri un ingiusto profitto e un danno per un altro soggetto.

Il comma terzo, infatti, stabilisce un aggravamento di pena (con reclusione da tre a sei anni) per chi mette in atto le condotte previste dal comma primo con furto o indebito utilizzo dell'identità digitale recando danno a uno o più persone.

Questo comma è stato aggiunto nell'articolo 9 comma primo del decreto-legge. n. 93/2013⁵⁵⁵.

Questo reato è ancora più grave se connesso alla sfera sessuale dell'individuo⁵⁵⁶.

Un caso esemplificativo è quello di Rana Ayyub, giornalista investigativa e inviata del *Washington Post*, che è stata vittima di una campagna diffamatoria che aveva ad oggetto dei suoi *deepfake* porno realizzati con l'obiettivo di farla stare in silenzio⁵⁵⁷.

⁵⁵³ Garante per la protezione dei dati personali, dicembre 2020, “*deepfake, il falso che ti ruba la faccia e la privacy*”

⁵⁵⁴ Cass. Pen. N.25774/2014

⁵⁵⁵ Convertito in legge n. 119 del 15 ottobre 2013

⁵⁵⁶ In questo caso, tra i vari reati possibili, si può aggiungere anche quello di diffamazione art 595 cp

⁵⁵⁷ Articolo AYYUB R., HUFFPOST “*I was the victim of a deepfake porn plot intended to silence me*”, 2018

Una truffa molto in voga negli ultimi anni è anche quella di falsificare l'identità di una persona rubando i suoi dati, modificare i dati biometrici vocali e facciali e accedere a dei sistemi privati, che possono essere bancari o di altro tipo.

Oltre ai video e alle immagini, anche le registrazioni audio possono essere *deep fake*: ci sono truffe che prevedono l'utilizzo di una voce registrata che però è frutto dell'IA⁵⁵⁸, e queste possono comportare l'alterazione delle opinioni politiche o dei voti⁵⁵⁹, nel caso in cui questa tecnologia venga utilizzata durante l'elettorato, portando a una libertà decisionale totalmente alterata da *fake news*⁵⁶⁰.

Addirittura, Texas e in California hanno vietato i contenuti *deep fake* nei sessanta giorni prima di una elezione, per non influenzare i cittadini; decisione specchio della crescente problematica che potrebbe diventare l'Intelligenza Artificiale nell'ambito delle *fake news*⁵⁶¹.

Il *deepfake* è in rapida diffusione anche per la facilità di realizzazione, tramite strumenti di uso comune, come *computer* con applicazioni o direttamente su dei siti web tramite telefono⁵⁶².

Lo strumento più utilizzato è lo *smartphone*⁵⁶³: esistono molte applicazioni, scaricabili su *iPhone* e *Android*, che possono essere utilizzate con questo fine.

Esempi di queste applicazioni sono: “*DeepFaceLab*”, “*Faceswap*”, “*Faceapp*” e chiunque può scaricarle.

Per questo, parte della Dottrina, non solo in caso di *Revenge porn*, ma anche per i *deepfake*, sostiene che per evitare questo pericolo bisognerebbe non mettere foto di sé stessi *online*, ma questa previsione andrebbe solo a rincarare il fenomeno del *victim blaming*⁵⁶⁴.

Molte di queste si possono trovare anche su altri siti *online* ed essere utilizzati per altri scopi oltre quelli illegali, per questo la condotta di utilizzo di tali sistemi non è ancora stata criminalizzata del tutto, ma solo se vengono messi in atto fatti che la legge non consente.

In questo caso, se il *service provider* viene a conoscenza del contenuto illecito postato sulla rete, avrebbe l'obbligo-compito di cancellare il materiale dalla piattaforma⁵⁶⁵.

⁵⁵⁸ DEVLIN H., *The guardian*, 10 Maggio 2024, “is AI lying to me? Scientists warn of growing capacity for deception”

⁵⁵⁹ MADDOKS S., ‘A Deepfake Porn Plot Intended to Silence Me’: exploring continuities between pornographic and ‘political’ deep fakes, in *Porn Studies*, 7, 2020

⁵⁶⁰ CBS, *I never said that! High-tech deception of ‘deepfake’ videos*, in *cbsnews.com*, 2 luglio 2018

⁵⁶¹ *California Government Code*, Section 11547.5; State of Texas, Chapter 21, Penal Code, Section 21.165; WESTERLUND M., “The Emergence of Deepfake Technology: A Review”, *Technology Innovation Management Review*, November 2019 (Volume 9).

⁵⁶² cfr. *supra*, WESTERLUND M., “the emergency of deepfake technology, a review”, Novembre 2019, volume 9, *Technology innovation management review*

⁵⁶³ ICT SECURITY MEGAZINE, *Deepfake e cyber-intelligence: tecniche di creazione, rilevamento, e prevenzione*, 2022

⁵⁶⁴ FALLIS D., *The epistemic threat of deepfakes. Philosophy and technology*. 2021, 34 (4), pg. 623-643

⁵⁶⁵ PANATTONI, “Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online”, in *diritto penale contemporaneo* 2/2019

Sebbene nell'articolo 612ter non ci sia ancora un chiaro riferimento al *deepfake*, l'articolo 600 ter e quater del codice penale, riguardante lo sfruttamento sessuale dei bambini, stabilisce che le disposizioni in questione si applicano «anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse [...] per immagini virtuali si intendono immagini 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».

Sebbene non espressamente previsto, all'articolo 640 c.p., il *deepfake*, potrebbe essere riscontrato nel comma due ter di tale normativa, modificato mediante la legge n. 90/2024, che introduce la specificazione del fatto commesso a distanza con strumenti telematici o informatici, in grado di indurre altri in errore, con artifici o raggiri, facendo sì che il ricattatore possa trarne profitto, e la vittima un danno. Vi potrebbe, inoltre, essere un accostamento terminologico, in riferimento agli artifici: si intende la realizzazione di un contenuto che simula circostanze esistenti, mentre non si può dire lo stesso per il termine raggiri, in quanto consiste nella manipolazione di parole o argomentazioni.

Per quanto riguarda la regolamentazione, l'Unione Europea ha introdotto il *deepfake* all'interno della legge sull'Intelligenza Artificiale, richiedendo ai creatori dei contenuti di indicare se ciò che viene caricato è stato manipolato con l'IA o meno.

Altro atto è la Direttiva sulla violenza di Genere del 2022: all'articolo 7b cita testualmente il *deepfake*, criminalizzando la condivisione non consensuale di immagini intime per i quali gli autori potrebbero subire il carcere.

In America, invece, si è pensato a una risposta extra legislativa, Rebecca Delfino, della *Loyola Law School* ha proposto una possibile bozza di un programma contro il *deepfake*: “*Pornographic Deepfake Criminalization Act*”, stabilendo di strumenti di supporto extra-legali che potrebbero essere utilizzati in aggiunta ad altre norme e agli interventi di sensibilizzazione⁵⁶⁶.

Mentre a livello federale, è stata istituita la proposta di legge “*No Ai fraud act*”, al fine di tutelare tutti quei soggetti che vedono la propria immagine modificata mediante l'utilizzo dell'Intelligenza Artificiale.

Nella sezione tre punto b, si parla di un vero e proprio diritto al ritratto e alla propria voce⁵⁶⁷.

In quest'ultima, viene menzionato uno studio del Dipartimento di Sicurezza Interna, secondo cui, a ottobre 2020, le immagini di nudo create con l'AI senza consenso fossero più di cento mila⁵⁶⁸.

⁵⁶⁶ DELFINO R.A., *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act*, *Fordham Law Review*, Vol. 88 issue 3, 2019; WESTERLUNDE, “*The Emergence of Deepfake Technology: A Review*,” *Technology Innovation*; HARRIS D., *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, in *Duke Law & Technology Review*, 17, 2019

⁵⁶⁷ *No Ai Fraud Act*, H.R. 6943, 118th Congress, 2023/2024

⁵⁶⁸ *No Ai fraud Act*, sezione 2, “*aumento della minaccia dell'identità deepfake*”

Il problema di questi contenuti, oltre all'evidente violazione delle regole e dei diritti dei singoli, è anche la realizzazione estremamente realistica del contenuto che si viene a creare, e i potenziali effetti devastanti che potrebbe provocare sulla vita della vittima⁵⁶⁹.

Invero, diviene molto complicato discernere un contenuto falso da uno vero, contribuendo quindi alla creazione di *fake news* e alla sovrapposizione della realtà con la fantasia⁵⁷⁰.

Un episodio recente dell'utilizzo malevolo di questo strumento è il caso dello *streamer* di Twitch Brandon Ewing, che mentre era in *live*, sul suo *computer* alcuni fan hanno notato un sito web pornografico, che aveva delle immagini false ritraenti alcune colleghe *streamer*.

Queste persone si sono riconosciute e hanno dichiarato di non essere a conoscenza di questi contenuti.

Ciò ha causato, in quel periodo, un aumento delle ricerche *online* del *deepfake porn*⁵⁷¹. Molte donne si sono battute per vedere riconosciuti i propri diritti all'immagine, come Sophie Compton, co-fondatrice del sito "*My image my choice*" con cui lotta contro l'abuso di immagini intime dei siti web *deepfake*; secondo questo sito, dal 2019 i casi di *deepfake porn* sono aumentati esponenzialmente del 3000%.

Molte volte, precisa la creatrice del sito in una intervista, questi contenuti vengono anche diffuse al fine di ricattare le vittime o indebolirle, lasciando comunque una crepa indelebile sia dal punto di vista psicologico, sia "indelebile" in senso stretto, in quanto il contenuto è molto difficile che venga rimosso dalla rete.

Ma come si crea un contenuto *deepfake*?

La tecnica più diffusa è l'utilizzo del GAN (*Generative Adversarial Networks*), che analizza le immagini o video che vengono forniti dall'utente: i video devono essere ad alta risoluzione, fondamentale è anche che il primo video sia simile a livello di movimenti, rispetto al secondo che si vuole sovrapporre.

Il sistema è costituito da due reti neurali: una che crea dati falsi, l'altra che verifica l'autenticità dei dati che vengono costruiti dalla prima rete⁵⁷².

Nel caso in cui ci siano delle non corrispondenze tra i due il video modificato inevitabilmente, avrà delle inesattezze e sarà più facilmente individuabile come *fake*.

⁵⁶⁹ ZICCARDI G., *Odio online, Revenge porn e natura delle nuove tecnologie tra amplificazione, persistenza e viralità del messaggio dannoso*, in Sorgato A. (a cura di), *Revenge porn. Aspetti giuridici, informatici e psicologici*, Milano, Giuffrè, 2020; CAMPAGNOLI M.N., *Social media e information disorder: questioni di ecologia comunicativa in Rete*, *dirittifondamentali.it*, 9 novembre 2020.

⁵⁷⁰ LONGO, SCORZA, "*Intelligenza Artificiale: impatto sulle nostre vite, diritti e libertà*", Mondadori Education Università, Firenze, 2020; BLITZ M. J., *Deepfakes and Other Non-Testimonial Falsehoods: When is Belief Manipulation (Not) First Amendment Speech?* in *Yale Journal of Law & Technology*, 23, 2020

⁵⁷¹ dati consultabili su "*Google trends*"

⁵⁷² GOODFELLOW I.J., POUGET-ABADIE J., MIRZA M. BING XU, WARDE-FARLEY D., OZAIR S., COURVILLE A., BENGIO Y., AA.VV., *Generative Adversarial Networks*, Università di Montréal, 2014

Successivamente, l'applicazione apprende le caratteristiche fondamentali del viso e i piccoli movimenti, le micro-espressioni e gesti che vengono messi in atto⁵⁷³.

Avviene quindi, una vera e propria mappatura del viso, che serve per riprodurre fedelmente quei movimenti e “trasportarli” sull'altra immagine⁵⁷⁴.

Entrambe le immagini verranno poi analizzate tramite dei *software*, cercando di ricreare l'immagine sovrapposta per ogni “*frame*”.

Infine, genera il contenuto sostituendo al protagonista del video o della foto, l'immagine della persona con la quale si vuole sostituire.

In questa fase il *software* non svolge un apprendimento, si limita solo a sovrapporre ciò che già si trova nei suoi sistemi.

Per ultimo, avverrà la fase di correzione dei piccoli errori, come una sorta di “post-produzione”, in cui però non potranno essere eliminate le grandi problematiche dei video stessi, se questi ne presentano.

Per esempio, molte applicazioni consentono di correggere il colore generale del frame, la sfumatura e le dimensioni del video, applicare filtri e aggiungere effetti multimediali⁵⁷⁵.

3.2 (segue): Il *Deepnude* o porno *deepfake* – criminalizzazione e punti di contatto con la fattispecie del *Revenge porn*

Un fenomeno molto diffuso, che costituisce una sottospecie del *deepfake* ma anche un nuovo tipo di *Revenge porn*, una sua evoluzione, è il “*deepnude*”, ma può essere chiamato anche “*porno deepfake*”.

Si tratta di foto di nudo prodotte grazie all'aiuto dell'Intelligenza artificiale.

Esistono due tipi di porno *deepfake*: da una parte, la rappresentazione di persone, che molto spesso non ne sono a conoscenza, tramite immagini o video create artificialmente, senza vestiti o in pose o con abiti succinti, con rimandi sessualmente espliciti o in contesti pornografici, facendo credere che è stata la stessa vittima a crearli o diffonderli.

Un esempio di questo tipo di fotografia potrebbe essere utilizzare la foto di nudo di una ragazza, unendola al viso di un'altra, tramite l'Intelligenza Artificiale.

In questo modo, con l'IA si rende protagonista di un video o di una immagine pornografica, una persona che non ha mai preso parte a quell'attività.

⁵⁷³ PAN D., L. SUN, R. WANG, X. ZHANG, R. O. SINNOT, *Deepfake Detection through Deep Learning*, in *International Conference on Big Data Computing, Applications and Technologies*, 2020, 134 ss.

⁵⁷⁴ CHADA A., V. KUMAR, S. KASHYAP, M. GUPTA, *Deepfake: An Overview*, in P. K. Singh – S. T. Wierzchoń – S. Tanwar – M. Ganzha – J. J. P. C. Rodrigues (a cura di) *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*, Cham, 2021, 557 ss.

⁵⁷⁵ SCANLON T.P., GALLAGER S., *Carnegie Mellon University, Software engineering institute, SEI Deepfakes day, Deepfakes* 101, 2022

Il secondo tipo si sviluppa quando una immagine comune o un video di una persona reale, viene “nudificata”, senza che ne sia a conoscenza.

Infatti, caricando l’immagine in specifiche applicazioni (immagine che magari viene presa dai *social network* della vittima), con l’Intelligenza Artificiale si trasforma in una foto di nudo molto credibile.

Questo tipo di contenuti, oltre che esser diffusi come ricatto, come nel caso di *Revenge porn*, possono anche avere il fine di alimentare la pornografia illegale e la pedopornografia.

Guardando qualche dato, secondo uno studio di “*Sensity AI*”, mediante il monitoraggio del *deepfake online*, l’applicazione è arrivata alla conclusione che il 90% di questi contenuti sono porno non consensuali con oggetto donne⁵⁷⁶.

In un report del 2020⁵⁷⁷, nel mese di luglio, su *Telegram*, piattaforma più utilizzata per la condivisione di questo tipo di contenuti, le immagini di 104.852 donne, sono state spogliate tramite l’utilizzo dell’Intelligenza Artificiale.

Queste fotografie sono diventate circa 680.000 (per lo meno quelle individuate con certezza).

In America, molti Stati non si sono ancora dotati di una disciplina apposita contro il *deep fake porn*.

Ci sono state molte proposte, nel corso degli anni, per criminalizzare il *deepfake* a livello federale, ma solo a febbraio 2023 alcuni senatori hanno presentato al Comitato Giudiziario del Senato lo “*Stopping harmful Image Exploitation and Limiting distribution (SHIELD) Act*”, tuttavia questa proposta non regolarizza la crescente minaccia del *deepfake porn*⁵⁷⁸.

Sicuramente, una legge federale in merito potrebbe costituire un forte disincentivo per la creazione di *deepfake* pornografici, a causa della minaccia di una indagine approfondita da parte dell’FBI e una eventuale azione penale da parte del Dipartimento di Giustizia americano⁵⁷⁹.

In *Texas*, da poco è stata modificata la legge di riferimento, prevedendo la punizione per colui che intenzionalmente produce o distribuisce con mezzi elettronici un video o una foto falsi che raffigurino la persona offesa senza il suo consenso, con parti intime esposte o in atteggiamenti sessualmente espliciti⁵⁸⁰.

Mentre in *California* è stata data la possibilità ai cittadini di citare in giudizio chiunque inserisca l’immagine altrui in un video pornografico con queste tecnologie⁵⁸¹.

L’Italia tuttavia, risulta essere, dopo gli Stati Uniti, la Russia e l’Argentina, tra i paesi al mondo in cui il fenomeno è più diffuso.

⁵⁷⁶ MIT TECHNOLOGY REVIEW, Article by Karen Hao, 2021 “*deepfake porn is ruining woman’s lives. Now the law may finally ban it*”

⁵⁷⁷ report, “*Automating Image Abuse, Deepfakes Bots on Telegram*”, 2020, Medianama

⁵⁷⁸ S.412, *Shield Act*, 118th Congress, 2023-2024, sito ufficiale del congresso

⁵⁷⁹ DELFINO A. R., *Fordham Law Review, pornographic deepfakes: the case for federal criminalization of revenge porn’s next tragic act*, 2019

⁵⁸⁰ S.B. 1361 ha modificato il capitolo 21 del Codice penale aggiungendo la sezione 21.165

⁵⁸¹ Assembly Bill n. 602, sezione 1, punto 14

Anche in Corea del sud, il fenomeno è allarmante, infatti, secondo quanto riportato dalla *BBC*, c'è una "epidemia di crimini sessuali digitali e una ondata di porno *deepfake* che colpisce molte donne"⁵⁸².

Secondo il *report* di “*Home security Heroes*”, nel 2023 il *deepfake porn* è aumentato esponenzialmente; infatti, il 48% degli uomini negli Stati Uniti hanno visualizzato video porno *deepfake*, il 74% degli utenti non si sente in colpa di averne usufruito.

Il fenomeno è diventato talmente frequente che viene quasi normalizzato dai più, tuttavia, per fortuna, almeno il 74% di coloro che hanno partecipato a questo *test* si direbbero disposti a effettuare una segnalazione alle autorità, nel caso in cui una persona di loro conoscenza o un familiare finisca vittima di questo tipo di pornografia⁵⁸³.

Questa tecnologia può quindi sì essere utilizzata, come abbiamo detto, anche per scopi leciti, ma il rapporto⁵⁸⁴ di *Deeprtrace labs* nel 2019 ha evidenziato come il 96% dei contenuti creati usando questi nuovi sistemi, siano materiali pornografici.

Il Garante della *privacy*, per proteggere ulteriormente le vittime minorenni ha imposto alla società *Open AI*, ente che gestisce varie applicazioni di Intelligenza Artificiale, come *ChatGPT*, un filtro ai minori di tredici anni.

Secondo il Garante per la protezione dei dati personali, questo tipo di contenuti finisce inevitabilmente ad incrementare ed incentivare la pratica del *Revenge porn* ma anche del *sexting* e della pornografia illegale, facendo sì che anche persone comuni, non solo personaggi famosi, risultino vittime di queste situazioni.

La persona offesa, quindi, si trova ad essere rappresentata durante atti sessuali che non si sono verificati e alcuni vengono addirittura pubblicati su siti pornografici.

Tuttavia, molti siti, tra cui il sito *web* pornografico più frequentato a livello globale ha vietato il caricamento di video *deepfake*⁵⁸⁵.

Quest'allarme crescente tra i minori, ha portato Monica Sansoni, Garante dell'infanzia per la regione Lazio, ad intervenire decidendo di effettuare degli incontri formativi nelle scuole, per insegnare ai preadolescenti e agli adolescenti i pericoli di questi *software*.

Il progetto, denominato “Genitori al centro, missione adolescenza” ha anche l'obiettivo di informare i genitori e sensibilizzarli nel conoscere il mondo in cui i loro figli vivono e come passano le loro giornate.

Questi episodi accadono in tutto il mondo, per esempio in Spagna, ad Almendralejo, una ventina di ragazze tutte minorenni, hanno denunciato alle forze dell'ordine la presenza di loro immagini a sfondo sessuale manipolate, circolanti su *Whatsapp* e su *Telegram*; per questi sono sospettati dei ragazzi, sempre minorenni.

⁵⁸² BBC, *South Korea faces deepfake porn emergency*, 24 agosto 2024, Nick Marsh, Jean Mackenzie

⁵⁸³ “2023 State of deepfakes, realities, threats and impact”, *Home security heroes*

⁵⁸⁴ “The state of Deepfakes: landscapes, threats, and impact”, Settembre 2019

⁵⁸⁵ POPOVA M., *Reading out of context: pornographic deepfakes, celebrity and intimacy*, in *Porn Studies*, 7, 2020, 367 ss.; R. Winter, *DeepFakes: uncovering hardcore open source on GitHub*, in *Porn Studies*, 7, 2020, 382 ss.

Il caso ha raggiunto grande visibilità grazie a una Influencer molto nota, spagnola, che ha diffuso la notizia e incitato le ragazze a denunciare⁵⁸⁶.

Una delle madri delle ragazze, ha detto alla stazione tv spagnola TVE che i falsi scatti di nudo erano stati usati come mezzo di ricatto contro la figlia e i creatori delle foto le hanno chiesto soldi per non diffonderle.

Una modalità che è stata utilizzata per molto tempo, per creare questi contenuti falsi, sessualmente espliciti, modificati dall'Intelligenza Artificiale, è l'utilizzo di un "bot" (sistemi automatizzati capaci di offrire dei servizi agli utenti) di *Telegram*.

Quest'ultimo sta prendendo il sopravvento tra i più giovani, si chiama "*Bikini off*": un servizio automatizzato, sviluppato da una azienda estone che produce giochi (denominata *Crystal Future*), che si autodefinisce, sul loro sito ufficiale, come un sistema di "*editing*" (modifica delle immagini) capace di togliere i vestiti alle fotografie, lasciando solo il "necessario".

Questo bot è nato grazie ad un'altra app, chiamata "*deep nude*".

L'applicazione, appena uscita, è stata scaricata da più di 95 mila persone, motivo per cui il creatore è stato costretto a chiuderla dopo pochi giorni per "motivi etici" e a vendere la licenza.

Il codice sorgente quindi è rimasto disponibile, e qualcuno ha ricreato lo stesso sistema anche su *Telegram*.

Tramite questo servizio, che per la prima foto è gratuita e poi diventa a pagamento tramite criptovalute, viene mantenuta la posa originaria, il *tono* della pelle, le proporzioni.

Innanzitutto, per utilizzare l'applicazione bisogna aprire *Telegram* e avviare una conversazione con l'Intelligenza Artificiale, che provvederà, una volta caricata l'immagine che si vuole spogliare, a crearla.

Di recente, in una scuola media di Latina, alcune studentesse e alcune docenti sono diventate vittime di questo bot.

In particolare, la foto della professoressa è finita su un rinomato sito pornografico⁵⁸⁷, il GIP, considerando la giovane età e il fatto che gli autori sono incensurati, ha dichiarato il non luogo a procedere per irrilevanza del fatto, poi questi hanno cancellato le immagini e cercato di eliminare ogni traccia del contenuto dalla rete⁵⁸⁸.

Inoltre, credo sia interessante mettere in luce che l'applicazione "*Bikini off*" non ha responsabilità se le immagini che vengono messe sul sistema per essere spogliate, non sono di donne, ma hanno ad oggetto uomini⁵⁸⁹.

Il Garante della *privacy* ha aperto una istruttoria sul *deepnude*, scoprendo che le persone che sono state spogliate tramite questo bot, si aggirano intorno ai settecento mila⁵⁹⁰.

⁵⁸⁶ Il corriere della sera, Lorenzo Stasi, settembre 2023

⁵⁸⁷ Ansa.it, Marzo 2024

⁵⁸⁸ Articolo de "La Repubblica", di Romina Marceca, 16 aprile 2023

⁵⁸⁹ BARANDELLO A. Articolo "*Casi di deepfake pornografici: intelligenza artificiale?*", 2024

⁵⁹⁰ Garante per la Protezione dei dati personali, comunicato stampa, 23 ottobre 2020 doc. N. 9470722

Quest'ultimo ha anche intenzione di chiedere informazioni a *Telegram* per accertare il rispetto della normativa GDPR; oltre a ciò, si valutano altre iniziative al fine di prevenire ulteriori usi illeciti di questi *software* e limitarne gli effetti.

L'Autorità in un comunicato stampa ha dichiarato «bisogna considerare anche il rischio che tali immagini vengano usate a fini estorsivi o di *Revenge porn*, e va tenuto conto dei danni irreparabili a cui potrebbe portare una incontrollata circolazione delle immagini».

In seguito, quest'ultima ha continuato a preoccuparsi in merito alla lesione del diritto all'identità personale, e del diritto all'immagine, divulgando anche un modello informativo, al fine di arginare queste manovre molto pericolose per il patrimonio personale⁵⁹¹.

Si ricorda anche, che il diritto all'immagine viene tutelato mediante la legge n. 633 del 1941, la cosiddetta “legge sulla protezione del diritto d'autore” il quale vieta di pubblicare il ritratto altrui senza il consenso dell'interessato.

Con ciò si fa riferimento anche alle immagini non reali o modificate, come il caso del *deep fake* pornografico⁵⁹².

Per quanto riguarda la criminalizzazione, il *deep fake porn* si potrebbe ricondurre, per alcune caratteristiche simili, tra cui la mancanza di consenso, al fenomeno del *Revenge porn*, come diffusione del materiale pornografico, tuttavia, non esiste né una norma specifica in materia, né una giurisprudenza consolidata, ma viene pacificamente ritenuto come un sottotipo del *Revenge porn*, una sorta di “versione aggiornata”, rispetto alle nuove tecnologie.

Il *deep nude*, astrattamente, potrebbe essere ritenuto punibile ai sensi dell'articolo 612ter, ossia per diffusione illecita di immagini o video sessualmente espliciti, ricomprendendo la fattispecie nell'aggravante sull'uso degli strumenti informatici o telematici (anche se il testo non fa riferimento a contenuti non reali), nel caso in cui il contenuto venga prodotto con il consenso e successivamente diffuso senza quest'ultimo.

In questo modo si valorizzerebbe il dato testuale, ma solo per quanto riguarda il comma terzo.

Questo articolo, copre solamente parte del problema della falsa pornografia non consensuale, risultando in una fattispecie per ora, inadeguata.

Di fatto, al momento, vige un vero e proprio vuoto normativo, in quanto questa fattispecie può essere sì, accostata al reato di diffusione illecita di immagini o video sessualmente espliciti, articolo 612ter, ma solo a determinate condizioni.

Infatti, applicando l'articolo 612ter in maniera diversa, potrebbe esserci una eccessiva estensione della interpretabilità per analogia, e per di più, non si darebbe importanza al principio di tassatività della legge penale.

⁵⁹¹ Garante per la protezione dei dati personali, *Deepfake: dal Garante una scheda informativa sui rischi dell'uso malevolo di questa nuova tecnologia*, 28 dicembre 2020.

⁵⁹² articoli 96 e 97 l. n. 633/41

A causa del principio di tassatività⁵⁹³ della legge penale, e al divieto di analogia *in malam partem*, all'articolo 25 della Costituzione, articolo 1 c.p. e 14 delle preleggi, sarebbe stato un onere complesso, per il legislatore, far rientrare questa fattispecie nell'articolo 612ter, poiché l'articolo in questione non fa accenno a contenuti artificialmente e digitalmente modificati, considerando anche la mancanza di Giurisprudenza di riferimento.

Nel caso in cui suddette rappresentazioni abbiano ad oggetto minori di anni diciotto, la diffusione e la creazione di immagini a sfondo sessuale tramite AI, sfocia nel reato di pedopornografia.

Se si tratta infatti di pornografia minorile, infatti, le immagini create digitalmente rientrano nella fattispecie dell'articolo 600 ter e quater c.p. in quanto espressamente, viene trattata la "pornografia virtuale", considerata come immagini a sfondo sessuale ottenute mediante l'utilizzo dell'Intelligenza Artificiale.

La norma, quindi, si riferisce a «immagini 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».

La Cassazione nel 2017 ha stabilito che le alterazioni a immagini di minori, sessualmente esplicite, alimentano "l'attrazione per manifestazioni di sessualità rivolte al coinvolgimento di minori", arrecando un pericolo alla formazione stessa della personalità del minore⁵⁹⁴.

Una sentenza, sempre della Suprema Corte, ha sottolineato la possibilità di utilizzare l'articolo 600 quater comma primo c.p. in caso di pedopornografia virtuale, con l'uso di fotomontaggi e tecniche *deepfake*⁵⁹⁵.

Il legislatore della riforma del Codice Rosso, si trovava in un periodo molto denso di pressioni in riferimento agli avvenimenti di Tiziana Cantone e Giulia Sarti, per questo ha dato più importanza alla fattispecie di *Revenge Porn*, risultando così una base legislativa inadeguata a fronteggiare l'avanzare tecnologico e le nuove forme di reato che si sono sviluppate col tempo.

Tuttavia, nel 2021, è stato portato all'attenzione del legislatore un disegno di legge⁵⁹⁶, recante il titolo "Disposizioni in materia di Intelligenza Artificiale", che ha l'obiettivo di porre rimedio al «fenomeno della diffusione del *software* chiamato "*Deep nude*"»

⁵⁹³ corollario del principio di legalità di cui agli artt. 1 c.p., 199 c.p. e 25 Cost., implica che la norma penale deve individuare con precisione gli estremi del fatto reato in essa contenuti

⁵⁹⁴ sent. Cass. Pen., Sez. III n. 22265, 13 gennaio 2017

⁵⁹⁵ Sent. Cass. Pen., Sez. III n. 15757, 9 aprile 2018

⁵⁹⁶ Camera dei deputati, *Introduzione dell'articolo 612-quater del Codice penale, in materia di manipolazione artificiale di immagini di persone reali allo scopo di ottenerne rappresentazioni nude*, 21 luglio 2021, atto n. 2986. Nella prefazione della suddetta si cita anche la legge sul diritto d'autore, si legge infatti, che ci sono in ogni caso delle eccezioni per quanto riguarda la condivisione di immagini senza consenso. «Non occorre il consenso della persona ritratta quando la riproduzione dell'immagine è giustificata dalla notorietà [...], da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali [...] il ritratto non può essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritratta» (Art. 97, l 22 aprile 1941, n. 633, c.d. "Legge sul diritto d'autore").

tramite l'introduzione di una «fattispecie delittuosa consistente nella diffusione di immagini di persone reali manipolate artificialmente allo scopo di ottenerne rappresentazioni nude».

In questa proposta, l'articolo 612 quater c.p. punirebbe con la reclusione da uno a cinque anni «chiunque cagiona ad altri un danno ingiusto, mediante invio, consegna, cessione, pubblicazione o comunque diffusione di immagini o video di persone o di cose ovvero di voci o suoni in tutto o in parte falsi, generati o manipolati mediante l'impiego di sistemi di intelligenza artificiale, atti a indurre in inganno sulla loro genuinità o provenienza»⁵⁹⁷.

È prevista anche una aggravante al secondo comma, nel caso in cui la persona che condivide il video *deepfake* sia legata alla persona offesa da una relazione affettiva.

Inoltre, «Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con un altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate».

La vittima, per difendersi, avrà diritto alla richiesta della cessazione del comportamento lesivo, tramite azione inibitoria presentata all'Autorità competente, a seguito della lesione all'onore e alla reputazione.

Potrà richiedere il risarcimento del danno patrimoniale e morale subito, per la lesione all'immagine e alla sua dignità personale, fornendo la prova del pregiudizio economico subito a causa della pubblicazione del contenuto⁵⁹⁸.

Inoltre, punti di contatto con l'articolo 612 ter sarà la presenza, anche in questo caso, di una clausola di salvaguardia - se il fatto costituisce più grave reato -, ma anche il fatto che si tratta di un reato comune, quindi potenzialmente commissibile da chiunque. Per la condotta, si ritrovano alcuni dei comportamenti previsti dall'articolo 612ter, ossia l'invio, cessione, pubblicazione e diffusione del contenuto, sottolineando come, per entrambe le fattispecie, chi mette *online* il contenuto potrebbe, potenzialmente, non esserne il creatore.

Le immagini o i video di riferimento devono avere ad oggetto persone identificabili come reali, che vengono modificate mediante l'utilizzo di sistemi di Intelligenza Artificiale.

Le finalità possono essere molteplici, e, per alcuni versi, coincidono con quelle del *Revenge porn*: la finalità di vendetta, di ottenere potere su un'altra persona, di umiliazione e di trarre in inganno altre persone.

Con questa proposta di legge, si prevedono anche alcune modifiche ad altre fattispecie di reato, come l'articolo 640 ter, con l'aggiunta di «ovvero mediante l'impiego di sistemi di intelligenza artificiale», ma anche un aumento di pena all'articolo 61, comma undici *decies* «l'aver commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano

⁵⁹⁷ Giurisprudenza penale, 24 aprile 2024

⁵⁹⁸ Camera dei deputati, Introduzione dell'articolo 612 quater del codice penale, cit. 2

costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato».

L'ipotesi del *deep nude*, continuando la nostra analisi, potrebbe rientrare negli articoli riguardanti l'estorsione (629 cp), nel caso in cui si minacci la divulgazione di questi contenuti artificialmente modificati, ma anche violenza privata (610 c.p.), se c'è stata minaccia, violenza o inganno.

Se il materiale sessualmente esplicito generato con l'uso dell'Intelligenza Artificiale, venga prodotto dalla vittima stessa e seguentemente diffuso da terzi, allora la tutela penale prevista dall'articolo 612 ter o 610 c.p. o altre fattispecie di reato non può essere applicata.

Infatti, per analogia, si estende la disciplina prevista per il “*sexting*” per il quale, la Corte di Cassazione, nel 2016 ha così statuito «la dottrina ha denunciato un vuoto di tutela rispetto a pratiche di *sexting* sia primario che secondario, allorquando cioè il minore metta in rete materiale erotico e/o pornografico autoprodotta e che abbia sé stesso come soggetto o allorquando diffonda o divulghi materiale erotico e/o pornografico altrui di cui sia venuto in possesso su consenso, o anche a prescindere dal consenso dell'autore, se non addirittura in aperto dissenso.

Sono fenomeni noti in particolare tra gli adolescenti la cui diffusività è in crescita[.] difetta l'elemento costitutivo dell'utilizzo del minore da parte di un soggetto terzo⁵⁹⁹». Altra fattispecie per cui chi diffonde *deep fake porn* potrebbe essere accusato è la diffamazione aggravata, articolo 586 comma terzo, rischiando la reclusione da sei mesi a tre anni.

Concludendo, si auspica al più presto un intervento del legislatore per poter normare anche tutte queste fattispecie che la tecnologia piano piano ha portato ad esistenza, e che sono entrate, purtroppo, a gamba tesa nella nostra società⁶⁰⁰.

Secondo vari report della società *Sensity*, il 70% delle donne coinvolte in diffusione di immagini o video *deepnude*, non sono famose, e circolano perlopiù su *Telegram*.

Effettuando una breve ricerca su *Google*, per *NBC news*, tra i motori di ricerca, se si scrive la parola “*deepfake*”, i risultati che si trovano più in alto sono quelli che riguardano la distribuzione dei contenuti e i metodi di realizzazione della pornografia, mediante l'utilizzo di Intelligenza Artificiale⁶⁰¹.

Mentre in Italia, a parte l'articolo 600 ter che lo specifica, per ora ancora non esiste una vera e propria criminalizzazione del *deepnude*, negli Stati Uniti, alcune giurisdizioni, anche se ancora poche, hanno adottato delle misure per contrastare questo fenomeno.

Il Congresso degli Stati Uniti ha anche introdotto un pacchetto normativo che consente alle vittime di intraprendere delle azioni legali per danni alla reputazione, a seguito della diffusione di questi contenuti *online*⁶⁰².

⁵⁹⁹ Cass. Pen. III Sez., n. 11675/16, Rv 266319

⁶⁰⁰ N. AMORE, *Una proposta di riforma dell'art. 612-ter c.p.*, op. cit., Paragrafo 6 (pag. 36 – 38)

⁶⁰¹ vd. *supra*

⁶⁰² *Deepfake Accountability Act*, 09/20/2023, HR 5586, 118th Congress, *Referred to the Subcommittee on Emergency Management and Technology*.

La *California* permette alle vittime di ricorrere alla Corte Civile, ai fini dell'ottenimento di un risarcimento finanziario⁶⁰³, la *Virginia* impone pene detentive a chi diffonde *deepfake* di carattere pornografico.

Tuttavia, punisce solo la condotta di diffusione: infatti, le condotte di condivisione e pubblicazione (a differenza della condotta di *Revenge porn* criminalizzata in Italia con l'articolo 612 ter) vengono considerate reato solamente se lo scopo è quello di minacciare o molestare la persona che è rappresentata nel video o nella foto⁶⁰⁴.

In conclusione, ci sono punti di contatto tra il *deepfake* porno e la disciplina della diffusione di immagini sessualmente esplicite, ma anche con il *vouyerismo* digitale, tra cui la strumentalizzazione del corpo e la violazione dell'intimità della vittima, soprattutto dal punto di vista psicologico, oltre che per la lesione di vari diritti fondamentali, tra cui il diritto alla riservatezza⁶⁰⁵.

3.3 (Segue): Responsabilità penale dei reati – uomo o macchina?

Le macchine, negli ultimi anni sono diventate sempre più innovative e dotate di capacità simili all'uomo, anche mediante l'utilizzo del *machine learning*, tale da ipotizzare il caso in cui i sistemi di Intelligenza Artificiale possano essi stessi commettere un reato, violando un precetto penale⁶⁰⁶.

La risoluzione del Parlamento Europeo suggerisce, in merito alla responsabilità giuridica, di verificare che il sistema che viene adottato, sia chiaro e preciso, al fine di evitare potenziali conseguenze negative a seguito dell'utilizzo dell'Intelligenza Artificiale⁶⁰⁷.

In merito, esistono due teorie: la prima sostiene l'inapplicabilità del diritto penale ai sistemi digitali, a causa della loro mancanza di coscienza e autodeterminazione.

Per questo, risultano strettamente legate all'operare dell'uomo.

Parte degli esperti, quindi, ritiene che, applicare la responsabilità penale a titolo di dolo al soggetto agente sarebbe più corretto, poiché il comportamento della IA fa parte del rischio probabile inizialmente considerato per l'azione che doveva essere posta in essere.

Si innesca quindi il principio "*machina delinquere non potest*"⁶⁰⁸.

⁶⁰³ FARISH K., *Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of the deepfake*, in *Journal of Intellectual Property Law & Practice*, 15, 2020

⁶⁰⁴ GERSTNER E., *Face/off: "deepfake" face swaps and privacy laws*, in *Defense Counsel Journal*, 87, 2020, 1 ss. VA. CODE. § 18.2-386.2.

⁶⁰⁵ N. AMORE, *La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612 ter cp*, 20.1.2020

⁶⁰⁶ GLESS S.– E. SILVERMAN– T. WEIGEND, *If Robots Cause Harm, Who Is to Blame: SelfDriving Cars and Criminal Liability*, in *New Criminal Law Review*, 2016

⁶⁰⁷ Regolamento n. 1689/2024

⁶⁰⁸ HALLEVY G., *When Robots Kill. Artificial Intelligence under Criminal Law*, Boston, 2013

Secondo questa quindi, l'Intelligenza Artificiale va considerata come un mero strumento, seppur dotata di eventuale autonomia.

Quindi, quando l'uomo compie un reato, direttamente o indirettamente, mediante l'uso della IA, quest'ultimo sarà imputabile considerando l'ipotesi dolosa, in particolare il dolo eventuale, se pur di arrivare allo scopo, ne accetta le conseguenze, oppure con dolo diretto, se il soggetto ha appositamente programmato l'identità digitale per commettere un reato e per questo ne sarà responsabile.

La macchina in questo caso viene considerata solo un mezzo, uno strumento mediante il quale viene messo in atto il reato.

Tuttavia, secondo il principio regolato all'articolo 27 comma primo della Costituzione, l'utilizzatore della macchina non potrà essere ritenuto responsabile del reato, generato dall'imprevedibilità della macchina, se diverso rispetto a ciò che era previsto dall'utilizzatore (si pensi ai *black box algorithms*, per cui il procedimento con cui il software arriva alla decisione finale non è del tutto conoscibile⁶⁰⁹), oppure nei confronti di una persona diversa⁶¹⁰, a meno che non risulti in grado di evitare l'evento.

Considerando quest'ultima situazione, nel caso in cui abbia avuto quindi, la possibilità di fare del tutto per evitare l'evento e non l'abbia fatto, allora avrà una responsabilità a carattere colposo⁶¹¹.

Tuttavia, secondo alcuni, l'impossibilità di conoscere appieno il funzionamento della macchina, riguarda solamente il *quomodo* e il *quantum* degli effetti, non *l'an*, per questo, potrebbe essere difficile considerare una imputabilità colposa: in base al principio del rischio tipico, infatti, l'evento è rimproverabile all'autore se costituisce la realizzazione del rischio che si voleva evitare⁶¹².

La seconda tesi invece, basandosi sull'elevato grado di autonomia che potrebbero in futuro raggiungere le macchine⁶¹³, ipotizza il superamento del principio "*machina delinquere non potest*", indicando la possibilità di imputazione dell'Intelligenza Artificiale come autore del reato⁶¹⁴.

Principale fautore di questa tesi è *Gabriel Hallevy*, che incentra il suo studio sul sistema di *common law*.

⁶⁰⁹ DONCIEUX S., J. MOURET, "Beyond black box optimization: a review of selective pressures for evolutionary robotics" in *Evolutionary Intelligence*, 7,2014; SPINDLER G., *User liability and strict liability on the Internet of Things and for Robots*, in S. Lohsse e al. (eds); NOMOS, BADEN-BADEN, *Liability for Artificial Intelligence and the Internet of Things*, 2019; SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in Riv. it. dir. proc. pen., 2021

⁶¹⁰ articolo 83 e 82 cp

⁶¹¹ PIERGALLINI C., *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in Riv. it. dir. proc. pen., 2005, F. Herzog, *Società del rischio, diritto penale del rischio, regolazione del rischio*, in L. Stortoni – L. Foffani (a cura di)

⁶¹² MAGRO M.B., *Robot, cyborg e intelligenze artificiali*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Utet, 2019; S. Beck, *Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood*, in 86 *Robotics and Autonomous Systems*, 2016

⁶¹³ GIANNINI A., *Intelligenza Artificiale, Human Oversight e Responsabilità Penale: prove d'impatto a livello europeo*, in *Criminalia*, 21 novembre 2021

⁶¹⁴ PIERGALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, 2020

Secondo quest'ultimo, l'elemento oggettivo del reato, sia che si riferisca a una condotta attiva da parte della macchina sia ad una condotta passiva (omissione), può essere attribuita anche alla AI⁶¹⁵.

L'Intelligenza Artificiale, grazie ai sistemi di apprendimento automatico (machine learning), è in grado, non solo di apprendere dalla propria esperienza e modificare il suo comportamento, ma può imparare anche da altri sistemi, tramite la tecnologia di *cloud computing*⁶¹⁶.

Per questo, permane un ampio grado di imprevedibilità, che rende la macchina "autonoma".

Inoltre, si può attribuire a questi sistemi non solo l'elemento oggettivo (*actus reus*), secondo l'autore, ma anche alcuni elementi della *mens rea* (elemento psicologico): in quanto, a causa della grande quantità di dati, raggiungono una conoscenza tale da poter valutare la probabilità che un evento si verifichi, quindi sarebbe sicuramente imputabile l'*intention*, la *negligence* e *knowledge*.

La macchina potrebbe anche aver fatto un errore di calcolo, non considerando in maniera corretta una probabilità che un evento si verifichi.

Hallevy ha quindi riconosciuto alla Intelligenza Artificiale personalità giuridica.

Non sono mancate le critiche a questa visione "macchinocentrica", da parte dei sostenitori italiani della prima tesi: alla base di queste vi è lo stesso articolo 27 della Costituzione che sancisce *la personalità* della responsabilità penale, ma anche i principi che costituiscono le funzioni della pena⁶¹⁷.

Questi, sostengono che, sebbene l'IA possa essere ritenuta colpevole della violazione di una normativa, questa difetta dell'elemento imprescindibile che caratterizza l'autodeterminazione dell'uomo: la colpevolezza⁶¹⁸.

Per quanto riguarda invece le funzioni della pena, preventiva, retributiva e rieducativa, l'Intelligenza Artificiale non soggiace a nessuna di queste, in quanto essendo macchine, non sono soggette alla "minaccia di un male" quale può essere la sanzione penale, né tantomeno possono apprendere da quest'ultima, a meno che non rientri nel suo compito⁶¹⁹.

L'unica strada che appare percorribile, infine, è quella di una adesione alla prima teoria, non essendo, ad oggi, ancora possibile parlare di responsabilità della macchina.

In ogni caso, fondamentale per il legislatore è il dover garantire, mediante la pena corretta, una sicurezza per il cittadino, mantenendo comunque il rispetto dei principi sacri del diritto, come il principio di legalità della pena, ma anche la sua proporzionalità.

⁶¹⁵ HALLEVY G., *Liability for crimes involving Artificial Intelligence Systems*, 2014; *When robots kill: Artificial Intelligence under criminal law*, 2013

⁶¹⁶ DONCIEUX S., J.B. MOURET, *Beyond black-box optimization: a review of selective pressures for evolutionary robotics*, in *Evolutionary Intelligence*, 2014, p. 71

⁶¹⁷ MERCORIO F., *Big Data, Intelligenza Artificiale, Industria 4.0: un'overview*, in Aa. Vv., *Metropolis, dai social media all'intelligenza artificiale*, a cura di M. Carvelli, G. Sapelli, Padova, 2019

⁶¹⁸ HAUGELAND J., *Artificial intelligence: the very idea*, Cambridge (Massachusetts), 1985, p. 2

⁶¹⁹ HALLEVY G., *liability for crimes involving Artificial Intelligence systems*, 2013

Beccaria, in una sua opera, diceva che «la legge deve stabilire una pena la cui durezza sia la minima necessaria al raggiungimento dello scopo, che è l'utile sociale. La pena (...) viene vista come legittima ed efficace soltanto nelle sue conseguenze utili per l'uomo⁶²⁰».

3.4 (segue): *Deepfake e Revenge Porn*: come proteggersi? Strumenti utili per il rilevamento, prevenzione, e contrasto di questo fenomeno

A causa dell'evoluzione sempre più veloce della tecnologia, mentre prima era più semplice capire se un contenuto fosse stato modificato dall'Intelligenza Artificiale, adesso è molto più complesso.

Tuttavia, con il progresso, non solo i contenuti *deepfake* hanno subito una evoluzione, ma anche gli strumenti atti alla sua rilevazione: infatti, di solito vengono utilizzati degli algoritmi di IA per poterli individuare; perciò, si viene a creare il paradosso dell'IA che limita l'IA, oppure si possono usare strumenti di segnalazione da parte degli utenti delle grandi imprese digitali (social media, motori di ricerca...).

Gli strumenti di Intelligenza Artificiale che vengono utilizzati per rilevare i *deepfake*, e quindi prevenire il loro caricamento *online*, richiedono un *database* con una grande quantità di dati su immagini e video, per poterne distinguere quelli veri dai loro falsi. Si utilizzano *deep networks* (reti neurali profonde ispirate al cervello umano⁶²¹) che, tramite l'apprendimento automatizzato, riescono a superare la capacità di discernimento dell'uomo, rilevando video manipolati.

Un esempio di queste tecnologie è “*Face Forenciscs+++*”⁶²², che è capace di riconoscere sia piccole modifiche che una vera e propria sostituzione di volti.

Tuttavia, su questi sistemi c'è ancora molto da lavorare, perché se l'applicazione si trova davanti una immagine o un *file* video particolarmente compresso, allora la sua efficacia diminuisce, *Google* e *Facebook* hanno però ampliato i video presenti sul suo *database*⁶²³.

Si auspica quindi, la possibilità in futuro, di applicazione di queste nuove tecnologie per limitare anche il caricamento sulle piattaforme, dei *deepfake porn*.

Secondo il Garante per la protezione dei dati personali, per difendersi da questo fenomeno in rapida espansione, è innanzitutto necessario adottare le misure corrette, come evitare di diffondere proprie immagini, o adottare un livello di sicurezza maggiore per i nostri profili *social*.

⁶²⁰ BECCARIA C., *Dei delitti e delle Pene*, 1764

⁶²¹ AGGARWAL C.C., *Deep Neural Networks and Deep Learning: a textbook*, II ed., 2023

⁶²² ROESSLER A., D. COZZOLINO, L. VERDOLIVA, C. RIESS, J. THIESS, AND M. NIEBNER, “*FaceForensics++: Learning to detect manipulated facial images*,” in *International Conference on Computer Vision (ICCV)*, 2019

⁶²³ DUFOUR N., A. GULLY, P. KARLSSON, A.V. VORBYOV, T. LEUNG, J. CHILDS AND C. BREGLER, “*Deepfakes Detection Dataset*”, 2019

Successivamente, altra accortezza sarebbe quella di evitare di ricondividere un video per il quale si ha il sospetto che sia *deepfake*, rivolgersi alle autorità competenti (o Polizia o anche Garante della *privacy*, a seconda della violazione commessa) se si ritiene che il *deepfake* sia stato utilizzato per commettere un reato⁶²⁴.

Ma l'elemento più importante è imparare a riconoscere quando un contenuto potrebbe costituire un contenuto modificato con l'IA, perché tutto ciò che viene modificato, in qualche modo, lascia una traccia.

Antecedentemente, le prime volte che venivano usati dei video *deepfake*, un “bug” che si presentava era il battito delle ciglia.

Un uomo in media sbatte le ciglia ogni due secondi, e ogni battito dura due decimi di secondo; l'Intelligenza artificiale all'inizio non era in grado di riprodurre questo movimento con così tanta precisione; infatti, in questi video raramente il soggetto sbatteva le ciglia.

Questo problema era stato, in parte, superato, tramite l'inserimento di un battito di ciglia “sintetico”, ma che non durava quanto uno vero, quindi comunque identificabile come finto⁶²⁵.

In generale, si tratta principalmente di anomalie del viso, come movimenti artefatti, espressioni rigide, labbra o parti del viso che si muovono in maniera meccanica, movimenti innaturali del collo, che possono essere o troppo rigidi oppure troppo fluidi. Bisogna fare attenzione anche alla luce: potrebbe essere indice di *deepfake* anche una illuminazione non corretta, per esempio se delle ombre non corrispondono alla direzione in cui va la luce.

Fondamentale quindi risulta allenarsi a riconoscere questo tipo di anomalie, ma il più delle volte non basta; quindi, sono state messe a disposizione delle applicazioni e degli strumenti che le rilevano automaticamente.

L'applicazione “Attestiv” rileva il *deepfake* commerciale, sia per salvaguardare aziende ma anche individui, la piattaforma utilizza l'Intelligenza Artificiale e le tecnologie di apprendimento automatico per analizzare dove si trovano gli elementi falsi del video⁶²⁶.

Altra *app* molto utilizzata, introdotta da Intel e progettata in collaborazione con l'Università *State di New York*, è “*Fake catcher*”, la quale vanta un tasso di precisione del 96%.

La piattaforma si trova sul web, ma utilizza *hardware e software* Intel, questa, valuta i *pixel* del video utilizzando il sistema di *deep learning*⁶²⁷.

⁶²⁴ Garante per la protezione dei dati personali, Dicembre 2020, *Vademecum “Deepfake, il falso che ti ruba la faccia (e la privacy)”*

⁶²⁵ ICT SECURITY “*Deepfake and cyber-intelligence: tecniche di creazione, rilevamento e prevenzione*”, 06/2022

⁶²⁶ Sito ufficiale Attestiv, *Deep fake video detention software*

⁶²⁷ Novembre 2022, sito ufficiale INTEL, “*intel introduces real time deepfake detector*”

Questi strumenti però, hanno dei limiti: infatti, se la qualità del video o dell'immagine è bassa oppure sono contenuti soggetti a distorsioni, possono essere ritenuti dal sistema come *deepfake* quando invece non lo sono.

Oppure al contrario, se il contenuto fosse creato da un professionista potrebbe non essere rilevato.

Anche *Google* ha introdotto un sistema di rilevamento, per aiutare i propri utenti a proteggersi: con la funzione "informazioni su questa immagine".

Google dà la possibilità agli utenti di verificare la veridicità dei contenuti, inoltre da questa funzione si capisce anche se questi erano stati già caricati tempo prima e aiuta anche a sapere come i siti gestiscono quella determinata immagine.

Google consente quindi di visualizzare i *metadati*, inclusi quelli che servono per capire se una data foto o un video sono stati modificati dall'Intelligenza Artificiale.

Lo scopo è sempre quello di mirare alla trasparenza delle informazioni, per un uso consapevole di questi strumenti che sono in rapida ascesa nell'uso quotidiano.

Invece, per arginare il fenomeno della diffusione illecita di immagini sessualmente esplicite ma anche del *porno deepfake*, si ritiene che le piattaforme social più utilizzate dovrebbero installare procedure di riconoscimento automatico di questi materiali, in modo da bloccarne immediatamente il caricamento sulle piattaforme e dissuaderne gli autori dalla loro creazione.

Questo è ciò che mira a fare *Facebook*, che insieme all'università *Michigan State University*, tramite il "*reverse engineering*" decodifica automaticamente (anche con l'uso dell'apprendimento automatico) i *deepfake* e la pornografia non consensuale.

Un ricercatore del *social network*, Tal Hassner, spiega in una intervista come dovrebbe funzionare questo metodo, ancora in fase di sperimentazione

«Supponiamo che un malintenzionato stia generando molti deepfake diversi e li carichi su piattaforme diverse per utenti diversi[...]

Se questo è un nuovo modello di Intelligenza Artificiale che nessuno ha visto prima, allora c'è ben poco che avremmo potuto dire al riguardo in passato.

Ora siamo invece in grado di dire: Guarda, l'immagine che è stata caricata qui, l'immagine che è stata caricata lì, provengono tutte dallo stesso modello", in quel caso potremo dire: "Questo è il colpevole».

In ogni caso, fondamentale per poter reprimere questi reati, è l'istituire strumenti normativi *ad hoc*, che possano contrastare questo tipo di fenomeni.

È necessario quindi, saper regolare il rapporto tra Intelligenza Artificiale ed essere umano, istituire una l'IA non sia computazionale, ma emotiva, che si ponga al servizio delle persone e dei loro bisogni, senza che si possa convertire in una minaccia⁶²⁸.

Mario Morcellini, Commissario AGCOM, ritiene che «Le innovazioni sono positive quando aumentano il benessere degli esseri umani, non degli inventori.

⁶²⁸ BALDASSARE A., BRISCHETTO A., PISTOLESI M., *Human centered AI*, rivista italiana di Ergonomia, 2020, n. 21, Società Italiana di Ergonomia

Quello che sconvolge di queste nuove tecnologie è il fatto che, a differenza delle fake news, non viene alterato il contenuto dell'informazione, ma la sua messa in scena.

È una svolta radicale, in quanto siamo abituati a prendere le misure, e a diffidare, da realtà che generalmente sono legate a un testo.

Da questo punto di vista, ritengo che un'iniziativa di tipo etico, educativo e regolamentare, sia indispensabile».

Considerazioni finali– *Revenge Porn* e Intelligenza Artificiale

Nei capitoli precedenti, si è osservato dapprima come la tecnologia sia stata, in questi ultimi anni, una forte fonte di progresso per ogni ambito della vita quotidiana, sebbene possa aver comportato anche dei rischi per i diritti fondamentali.

Infatti, sono venuti ad esistenza nuove tipologie di reato che hanno preso il sopravvento sulla scena criminale, sia nazionale che estera, come la diffusione illecita di immagini o video sessualmente esplicite, la cui portata è stata ampliata notevolmente a causa della presenza dei *social network*, grazie alle caratteristiche di immediata condivisione e la potenziale circolazione incontrollata delle informazioni.

Per questo, l'Unione Europea ha deciso di regolamentare la commissione dei reati tramite *internet*, con la Convenzione di Budapest.

L'uso della rete è diventato talmente all'ordine del giorno che ogni ambito relazionale può avvenire su *internet*, comportando anche, senza una mancata educazione all'utilizzo di questi strumenti, dei pericoli per la reputazione, la dignità personale, l'immagine, vista la rapidità con cui le informazioni circolano sulla rete.

Anche i rapporti interpersonali si possono gestire tramite questi strumenti e ciò ha portato le persone a condividere ogni aspetto, anche il più "privato" della propria vita, senza mettere in conto le conseguenze, come il fatto che le proprie immagini, se finiscono in mani sbagliate, possono finire *online*.

Infatti, il soggetto attivo che compie questo tipo di reati, percepisce il *computer* come una sorta di "quarta parete", un "muro" in senso fisico, capace di "proteggerli" dall'essere identificati come carnefici.

In queste circostanze, per i più giovani i pericoli sono sempre di più, perché con l'utilizzo dei *social network* si ritrovano completamente estraniati dalla realtà e rimangono ancorati ad un bisogno incessante di relazionarsi e ottenere validazione *online*, e non si accorgono né dei pericoli, né dell'impatto che hanno le proprie azioni sugli altri.

Il *social* più utilizzato per commettere reati è sicuramente *Telegram*, che come abbiamo visto, grazie alla sua *privacy policy*, garantisce l'anonimato agli utenti, permettendo quindi la creazione di gruppi di utenti capace di commettere ogni tipo di reato, dalla pedopornografia, alla diffusione di immagini private, diffamazione online, cyberbullismo ecc.

Questo sito in particolare è costituito anche di “bot” che interagiscono con gli utenti e questo rende ancora più difficile identificare il vero autore del reato.

Ho descritto, nel capitolo primo, come Dottrina e Giurisprudenza si sono interrogati sulla responsabilità che hanno i gestori di queste piattaforme *social*, arrivando alla conclusione di dover effettuare un bilanciamento tra le due teorie sviluppatesi.

Secondo la *communis opinio* degli esperti, il “*provider*” non ha un obbligo di controllo *ex ante* ex art 40 cpv, dei contenuti che vengono caricati *online*.

Tuttavia, il fornitore del servizio si deve occupare di applicare ogni accorgimento possibile al fine di ridurre la probabilità che l’evento dannoso possa accadere, e nel caso in cui si verifichi, agire prontamente per ridurre il pregiudizio arrecato alla persona offesa.

Nel caso in cui non realizzi questi accorgimenti oppure contribuisca alla diffusione del contenuto, allora sarà ritenuto responsabile, anche a titolo omissivo.

La fattispecie di diffusione illecita di immagini o video sessualmente espliciti, nell’ottica dell’introduzione della Riforma del Codice Rosso, ha sicuramente raggiunto l’obiettivo di colmare la lacuna che era presente nel nostro ordinamento, al fine di contrastare questo fenomeno, che la cosiddetta rivoluzione digitale ha ampiamente incrementato.

Per poter evitare di vedere le proprie foto caricate su una di queste applicazioni alla mercé di malintenzionati, la maggioranza delle campagne a sostegno dei diritti della *privacy*, come abbiamo visto, suggeriscono di impostare dei livelli di sicurezza elevati per le foto che decidiamo di caricare in rete, in questo modo solamente i più fidati possono vederle, anche se ciò potrebbe non bastare.

Per questo, fondamentale è educare gli utenti all’utilizzo di questi strumenti, oltre che prevedere delle pene congrue ai potenziali danni arrecati.

Infatti, secondo le statistiche, la diffusione di fotografie intime o a carattere sessuale, avviene per lo più tramite *social*, come *Whatsapp*, *Facebook* e *Instagram*.

Tuttavia, la divulgazione può avvenire anche nel *deep web* o *dark web*, dove vi sono dei veri e propri “archivi”, correlati a dati personali delle vittime, grazie al quale vi è possibilità di riconoscimento delle stesse, contenenti fotografie e video di, per lo più donne, in atteggiamenti sessualmente espliciti.

Lo conferma la Polizia Postale di Roma, che nel 2018, grazie ad una operazione coordinata con il Centro Nazionale di Contrasto alla Pedopornografia *Online*, ha individuato vari archivi, denominati “La Bibbia 5.0”.

Dalle indagini è risultato che i creatori di questi archivi avevano sottratto le fotografie e i dati personali pubblicati sui *social network*, oppure le immagini intime inviate privatamente dalle stesse vittime, a persone conosciute *online*.

Venendo all’oggetto del mio studio, il *Revenge porn* è un termine che, fattivamente, è nato in Inghilterra, nel 2007, quando compare per la prima volta nell’*Urban Dictionary*, ma la condotta di diffusione illecita di immagini sessuali era dilagante anche prima che gli venisse attribuito questo termine.

In Italia, diventa reato solamente nel 2019 con la legge n.69, antecedentemente, non veniva visto come un problema tanto “grave” da causare l’introduzione di una nuova fattispecie, ma venivano utilizzate quelle che erano già presenti nell’ordinamento, per questo, in caso di diffusione di immagini personali di carattere sessuale, senza consenso, si utilizzavano tutti quegli articoli che ho dapprima analizzato.

Solo a partire dal grande scalpore che ha provocato il caso di Tiziana Cantone e il livello preoccupante di casi che si stavano verificando nel nostro paese, il legislatore ha voluto introdurre una fattispecie *ad hoc*, che non rientrasse in quei reati che venivano utilizzati precedentemente, per punire queste condotte, tra cui l’articolo 617 septies, l’articolo 612 bis, 494, 595 c.p.

La normativa all’articolo 612 ter, rubricata come “diffusione illecita di immagini o video sessualmente espliciti” integra un reato comune, che può esser commesso da chiunque.

Caratteristica che permette che il reato possa esser commesso anche al di fuori dei confini nazionali, senza che il perpetratore si trovi nelle vicinanze della vittima.

La disciplina di nuova introduzione è stata molto criticata da Dottrina e Giurisprudenza, perché ritenuta vaga e poco precisa a tal punto da non ricomprendere tutte le condotte e gli episodi che si sono verificati ultimamente, come per esempio il *sexting*.

Mentre, secondo alcuni studiosi citati nel capitolo di riferimento, la normativa ha delle specificazioni che vengono ritenute “di poco conto”, considerando il *modus operandi* di questo reato: si tratta della aggravante dell’uso dei mezzi telematici.

A differenza di altri articoli che prevedono la possibilità che un reato possa avvenire non solo *online*, ma anche dal vivo, come lo *stalking* all’articolo 612 bis e la fattispecie di *cyber stalking*, il *Revenge porn* è una condotta che il 99% delle volte avviene sulla rete, a causa anche della immediatezza con cui girano le informazioni, per questo, una apposita aggravante per una qualità che contraddistingue il reato oggetto d’esame, sembra essere del tutto superflua.

Oltre a ciò, molti criticano anche la sua collocazione sistematica, come sottotipo della violenza di genere, in quanto nasce con una Riforma volta a tutelare soprattutto le donne come vittime di violenza domestica, ma la portata applicativa del *Revenge porn* è molto più ampia, non riguarda solo le donne, la “persona offesa” può essere anche un uomo, *gay*, lesbiche ecc.

Risulta anche di difficile inquadramento nel contesto di “violenza sessuale”, in quanto il fine ultimo non è quello di soddisfare un istinto animale di chi mette in atto la violenza, ma le finalità sono distinte, e molto spesso coincidono con il voler arrecare nocumento alla persona offesa.

Questo fatto è riscontrabile soprattutto a livello temporale-normativo, in quanto la Riforma del Codice Rosso, si colloca temporalmente dopo la modifica al reato di atti persecutori, violenza sessuale e la normativa in tema di femminicidio.

Secondo parte della Dottrina, i reati di nuova introduzione, tra cui l’articolo 612ter rientrano in «fattispecie sotto questo profilo “comuni” il cui retroterra criminologico

può certo essere costituito anche da rapporti familiari o riferirsi a una persona femminile, ma non necessariamente»⁶²⁹.

Altro elemento che potrebbe costituire un problema nella risoluzione di casi di *Revenge porn*, sarebbe il *locus commissi delicti*, tuttavia, la diffusione di immagini sessualmente esplicite è svincolata dalla territorialità in quanto è un reato che si commette *online*, anche se, secondo la Cassazione, il *web* viene ritenuto un “luogo virtuale”.

Autorevole Dottrina⁶³⁰ analizza che per questa fattispecie «le categorie spazio-fisico-temporali entrano in crisi, in quanto vengono in considerazione la “*smaterializzazione*” di dati e informazioni, raccolti e scambiati in un contesto virtuale, senza contatto diretto o intervento fisico su di essi», sebbene questo principio venga applicato in relazione all’accesso abusivo, per analogia, può essere utilizzato anche nell’ottica del reato di diffusione illecita di immagini sessualmente esplicite.

Il delitto quindi si ritiene consumato al momento e nel luogo della verifica delle condotte oggetto del comma primo e secondo dell’articolo 612ter, cioè al momento della diffusione, sottrazione, pubblicazione ecc.

Inoltre, la successiva cancellazione del contenuto dal *web* risulta irrilevante ai fini dell’integrazione del reato, in quanto non conta il momento percettivo da parte della persona lesa.

Oltre all’aumento di pena sopra descritto, nella normativa oggetto d’esame sono state introdotte anche altre aggravanti: fatti commessi dal coniuge o persona legata da una relazione affettiva, fatti commessi in danno di una persona con infermità fisica o psichica o donna incinta; quest’ultima, viene considerata una aggravante a effetto speciale, per la quale si procede d’ufficio, in caso di querela.

Nel capitolo secondo, ho attentamente descritto le condotte oggetto di questo reato, tra cui la realizzazione e la successiva diffusione di video o immagini, senza il consenso della persona offesa.

Quelle che a mio parere meritano più attenzione sono innanzitutto il “realizzare” e il “sottrarre”; condotte che il legislatore ha voluto mantenere distinte al fine di sottolineare, da un lato, rispettivamente, la produzione lecita del materiale e dall’altro, quella illecita.

Le condotte in questione assumono rilevanza soprattutto per il primo comma, mentre per il secondo comma non sono caratterizzate da disvalore, anzi, anche il trattamento sanzionatorio rimane invariato.

Queste ultime vengono divise in due “macroaree”: l’invio-cessione che sottolinea un rapporto diretto con i destinatari e la loro potenziale determinatezza e la divulgazione-diffusione, che presuppone la mancanza di un rapporto con il destinatario,

⁶²⁹ Cfr. PADOVANI T., *L’assenza di coerenza mette a rischio la tenuta del sistema*, 2019, in Guida dir., pag. 37

⁶³⁰ BELLACOSA M., in *Diritto Penale Contemporaneo*, “il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite”, 2015,7.

sottolineandone la probabile indeterminatezza, come nel caso della pubblicazione sui *social network*.

Basta anche solo commettere una di queste azioni per poter ritenere il reato come integrato.

Inoltre, per la Dottrina, l'elenco non sarebbe tassativo, potendo quindi ricomprendere altri comportamenti non evidenziati dal legislatore.

Come sottolinea la Giurisprudenza, con varie sentenze, elemento fondamentale della fattispecie in questione, come si evince dalla mia analisi, è stato sicuramente il consenso della persona offesa.

Secondo la Cassazione, infatti, è irrilevante che la vittima abbia prestato il consenso al momento della creazione del contenuto, se per la sua diffusione non lo ha conferito.

Per questo, si ritiene punibile il soggetto attivo che diffonde il contenuto all'insaputa della vittima, con l'obiettivo di ridicolizzarla o ledere la sua immagine, infatti, molto spesso, ma non sempre, a pubblicare questi contenuti è qualcuno molto vicino alla persona offesa, con la quale il più delle volte, intrattiene una relazione amorosa (circostanza che viene messa in rilevanza dal comma terzo).

Di solito, infatti, le motivazioni principali risiedono nella vendetta, ma non solo, potrebbero anche esserci o la semplice volontà di umiliazione sociale, oppure scopi estorsivi (estorsione tentata o consumata), oppure per una scommessa o per fini politici, per scopo di lucro o addirittura semplice "divertimento".

Tacitamente, si fa riferimento a quest'ultimo inciso mediante l'inserimento nel dettato della norma dell'articolo 612ter, della clausola di riserva "salvo che il fatto costituisca più grave reato": il reato di estorsione all'articolo 629 c.p. (in questo caso *sex extortion*).

Tuttavia, il fenomeno dell'assorbimento in questo caso non parrebbe verificarsi, in quanto l'obiettivo finale della estorsione sessuale sarebbe una minaccia e quindi non l'atto di diffusione vero e proprio che invece viene criminalizzato dall'articolo 612ter. Si auspica, che il legislatore, a seguito di una possibile riforma al fine di migliorare la fattispecie in esame, possa includere nella normativa della diffusione illecita di immagini sessualmente esplicite, anche un inciso che si riferisca alla minaccia di diffusione di immagini intime con un fine diverso dall'estorsione.

Il primo comma punisce il soggetto attivo con la reclusione da uno a sei anni chi realizza sottrae o diffonde [...] questo tipo di contenuti, senza consenso, facendo riferimento quindi a una fattispecie a dolo generico.

Mentre, il secondo comma, si sofferma sulla condotta di chi, avendo ricevuto le immagini o video da terzi, le diffonde ulteriormente senza consenso, al fine di arrecare nocumento: proprio su quest'ultima specificazione il legislatore ha voluto porre l'attenzione, sottolineando l'ipotesi di dolo specifico verso la persona offesa.

Concezione, che, come abbiamo messo in evidenza, è considerata molto più ampia rispetto al mero danno, poiché comprende non solo il lato patrimoniale ma anche il carattere psicologico del male arrecato.

Tuttavia, la previsione del dolo specifico nel secondo comma per i cosiddetti secondi distributori potrebbe rischiare di limitare in sede di applicazione il contrasto a questi reati, unendo potenzialmente una pluralità di eventi che potrebbero verificarsi.

Anche il trattamento sanzionatorio è stato criticato in quanto molto simile a quello previsto per la disciplina degli atti persecutori, senza considerare le ampie differenze tra le due fattispecie.

È stata commentata anche la mancanza di una aggravante che riguardi la diffusione illecita di fotografie di minori, anche se probabilmente l'idea del legislatore era evitare di appesantire la legge, considerando che esiste anche la disciplina all'articolo 600 ter comma terzo del c.p., riguardante la pedopornografia.

Per quest'articolo non risulta applicabile la clausola di sussidiarietà, salvo che il fatto costituisca più grave reato, in quanto l'articolo 600 ter prevede una pena inferiore (reclusione da uno a cinque anni) rispetto alla diffusione illecita di immagini o video sessualmente espliciti.

La Cassazione ha inizialmente escluso l'operatività dell'articolo 612ter nel caso in cui le immagini siano autoprodotte dal minore stesso, oggi però, con una più recente casistica, la Corte ha escluso, per quanto riguarda la fattispecie di immagini auto prodotte dal minore, che la loro circolazione (articolo 600 ter) possa integrare la fattispecie di "distribuzione, divulgazione, diffusione, pubblicizzazione di materiale pedopornografico".

Quindi la norma in commento potrà essere applicata anche in molte delle ipotesi di pornografia non consensuale in ambito minorile⁶³¹.

Come abbiamo evidenziato, fondamentale per capire appieno la normativa, è analizzare il significato di "sessualmente esplicito", ponendo l'attenzione all'alveo dei reati sessuali in generale, su cui la Cassazione si è soffermata, cercando di chiarire questo punto.

Di ultimo, si afferma che viene considerato sessualmente esplicito non solo il ritrarre gli organi sessuali o gli atti di autoerotismo, ma anche l'esibizione lasciva di zone intime, come il seno, oppure anche immagini o video in biancheria.

La norma fa espresso riferimento alla destinazione privata del contenuto: molte volte, infatti, la vittima invia consensualmente queste immagini fidandosi dell'altra persona, per questo, una delle conseguenze che ne deriva è la rottura del rapporto fiduciario: la persona offesa sviluppa un senso di colpa per aver mandato queste foto o video personali e si colpevolizza di aver "auto-provocato" l'evento dannoso.

A rincarare ancora di più questa sensazione c'è il "*victim blaming*" o vittimizzazione secondaria, fenomeno che molto spesso contraddistingue la cerchia sociale della vittima, che viene "incolpata" da amici e parenti di essere stata negligente e quindi di esser stata lei stessa la causa dell'accaduto.

⁶³¹ Sul mutamento di orientamento giurisprudenziale, BIANCHI M., *Il "Sexting minorile" non è più reato?*, 2016, Cass. pen., Sez. III, 21.3.2016, n. 116755 cit., passim.

Con questa definizione, si fa riferimento anche a tutte quelle «conseguenze negative dal punto di vista emotivo e relazionale, derivanti dal contatto tra la vittima e il sistema delle istituzioni in generale, e quello della giustizia penale in particolare»⁶³² molto spesso accade infatti, che le vittime di violenza di genere vengano” colpevolizzate” per i propri comportamenti, che siano online, oppure dal vivo, per i propri vestiti, durante interrogatori particolarmente invasivi.

Tornando all’analisi normativa, la locuzione inerente alla destinazione privata del contenuto è volta a sottolineare la necessaria tutela alla riservatezza, diritto costituzionalmente garantito in vari articoli, ma tutelato anche dalla Cedu e dal TFUE. È bene ricordare, alla conclusione della nostra analisi, come questa definizione normativa debba essere letta in chiave soggettiva, escludendo quei casi per cui le vittime di queste condotte, volontariamente si sottopongono alla possibilità di essere visti o ripresi da occhi indiscreti.

Altra protezione necessaria ai fini della comprensione di questo articolo è rivolta al diritto all’immagine, tutela che risulta presente sia dal punto di vista civilistico, con l’articolo 10 cc (mediante il quale il giudice può disporre l’azione inibitoria, ossia la cessazione della condotta e la limitazione degli effetti dannosi) e 2043 cc, con la quale si può richiedere il risarcimento del danno (sia patrimoniale, considerato come il pregiudizio economico derivante dall’illecito, che morale), ma anche da altre normative, tra cui la legge sul diritto d’autore (articoli 10,96,97) e il GDPR.

L’articolo 96 prevede che l’immagine di una persona non può essere esposta o riprodotta senza il consenso di quest’ultima, anche se l’articolo seguente precisa che non è necessario il consenso se la diffusione è giustificata dalla notorietà o dall’ufficio pubblico della persona in questione.

L’immagine *online*, quindi, in una società basata sulla velocità delle informazioni e sull’utilizzo assiduo dei *social network*, diventa come un biglietto da visita e fa parte dell’identità stessa della persona.

È utile ricordare come la Corte costituzionale, nel 1994, definiva l’identità personale come «diritto ad essere sé stesso, inteso come rispetto dell’immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l’individuo»⁶³³.

Oltre a ciò, come abbiamo visto durante la mia analisi, gli effetti sulla persona offesa sia dal punto di vista psicologico che relazionale-lavorativo, possono essere molto gravi, per questo ritengo che sia necessario agire da un punto di vista preventivo.

A tal proposito, molti sistemi si sono aggiornati per contrastare questo fenomeno di diffusione di immagini a sfondo sessuale senza consenso, tra cui *Google*, *X*, ma la più incentrata su questo scopo è stata *Meta*, che con *Facebook* ha istituito un sistema di

⁶³² MENDICINO R., La vittimizzazione secondaria, in *Profiling*, 2015

⁶³³ Corte cost. 3 febbraio 1994, n. 13

riconoscimento delle immagini che si ritiene possano essere caricate online, mentre per chi è sicuro che l'immagine sia circolata, basta premere il tasto segnala.

Meta ha anche istituito la piattaforma “*Take it down*”, questa analizzando l'impronta digitale della foto caricata dalla vittima, verrà individuato il valore della fotografia e bloccata in caso di caricamento.

L'utente che ha “condiviso” il contenuto verrà temporaneamente bloccato per poterne verificare l'innocenza, mentre un team di esperti valuterà la fotografia o il video che deve essere bloccato per violazione dei termini.

Tuttavia, come il caso Cantone ci ha dimostrato, non è sempre possibile bloccare in via definitiva il contenuto che circola in rete, anzi, dopo anni, questo può essere riportato alla luce e ricondiviso sui *social network*, oppure può esser oggetto di modifica mediante *software* di *deepfake*.

Anche il Garante ha istituito un sistema di tutela, tramite l'articolo 144bis che prevede che, in caso di diffusione di immagini all'articolo 612ter, si può attuare una segnalazione o reclamo al garante, che entro 48h provvede.

Permane in ogni caso la denuncia alla Polizia Postale, quest'ultima si è dotata di un sistema, chiamato *moniTOR* capace di combattere la criminalità nel *dark web* e rintracciare e controllare materiale pornografico senza consenso.

Facebook ha previsto (in collaborazione con vari Istituti come il *Revenge Porn Help line* nel Regno Unito, *Cyber Civil Rights Initiative* negli Stati Uniti, *Digital Rights Foundation* in Pakistan, *SaferNet* in Brasile) l'introduzione di un *hub* del *Safety Center*, intitolato “*Not without my consent*” per supportare le vittime di Revenge porn e permettere a queste ultime di trovare organizzazioni che le aiutino, ma anche metodi con il quale possano ridurre la divulgazione del contenuto e limitare i danni.

È di comune accordo infatti, in Dottrina, che sia fondamentale incrementare e migliorare la *privacy policy* dei propri profili *online*, ma anche introdurre dei nuovi strumenti di blocco del materiale illecito sui siti.

Meta si è attivato per arginare questi fenomeni, ma secondo molti il sentiero da percorrere è ancora molto lungo.

Primo tra tutti, a mio avviso, sarebbe utile la promozione di campagne informative per i più giovani, come prevedeva inizialmente la proposta del ddl n. 1134 per la riforma del Codice Rosso, che istituiva delle vere e proprie campagne di sensibilizzazione per i ragazzi, al fine di educarli sul rispetto della riservatezza altrui e sulla consapevolezza dei danni che possono derivare dalla diffusione di immagini di carattere sessualmente esplicito.

Tuttavia, non solo questi sono soggetti all'invio di foto intime, ma anche le persone adulte, che sottovalutano i pericoli della rete.

Molto spesso, si cede a pratiche tenute sulla rete che possono esporci a pericoli, come il *sexting*, abitudine che viene messa in pratica da gran parte della popolazione italiana, secondo le statistiche.

Questa prassi può portare inevitabilmente, anche alla condivisione di foto intime, magari come ricatto o a seguito di manipolazione da parte dell'altra persona, con cui di solito si intrattiene una relazione.

Con le campagne di sensibilizzazione, si può aiutare le persone a proteggersi con determinati accorgimenti, come il non mostrare il proprio volto in queste foto o utilizzare dei sistemi "sicuri" che possano impedire all'altro di effettuare una copia della fotografia.

Di recente, per esempio, *Whatsapp* ha vietato la possibilità di fare *screenshot* alle foto che si mandano "ad una sola visualizzazione", facendo diventare lo schermo completamente bianco quando si tenta di fotografare l'immagine in questione.

Il problema sta nel fatto che è quasi impossibile arginare del tutto questa possibilità, per cui, visti anche i grandi rischi che ci sono nel caso in cui la fotografia venga caricata su *internet*, e la difficoltà di rimozione dalla circolazione.

L'Agenzia per la sicurezza digitale ma anche altri enti suggeriscono di non mandare affatto questo tipo di contenuti all'altro, per evitare che in futuro questo possa avere un tale potere sulla propria persona.

Con queste campagne, anche magari grazie all'utilizzo della Intelligenza Artificiale, si potrebbero insegnare i pericoli e le conseguenze che potrebbero verificarsi se viene messa in atto questa condotta di divulgazione di questi contenuti, in modo tale da informare le nuove generazioni su quello che potrebbe accadere in seguito alle loro azioni irresponsabili.

Allo stesso tempo, l'Ai potrebbe esser utile non solo come strumento per accelerare l'informazione verso i più giovani, ma anche per tutelarli *online*.

Per esempio, all'Università di Padova, in collaborazione con Carolina Onlus è stato istituito un progetto "*net guardian*" con il quale si ha il fine di creare una applicazione, che grazie a particolari *software* di AI, possa misurare il rischio di violenza *online* durante una conversazione che avviene su *internet*⁶³⁴.

La macchina, in base al livello di pericolosità e di rischio rilevato, si attiverà prontamente con degli interventi, grazie alla tecnologia *deep learning* "*Bert*" di *Google*.

Il compito del legislatore in futuro, quindi, sarà quello di sfruttare le potenzialità di questi nuovi strumenti, ma anche porre, a prescindere, una legge solida che possa sì da un lato prevenire, ma anche reprimere alla base la diffusione di immagini a sfondo sessuale, e, più in generale, i reati sessuali *online*.

Non è così difficile poter immaginare come può essere sfruttata questa tecnologia a livello legale, visto che già nei Tribunali, anche se non propriamente diffusa in Italia, viene utilizzata come strumento utile per alleggerire i compiti delle autorità e degli esperti.

Dal punto di vista "preventivo" la possibilità di utilizzo di questi strumenti, non è neppure così fantascientifica, visto che vengono già utilizzati software "predittivi".

⁶³⁴ Redazione Ansa, 27 marzo 2024

Per esempio, in India, è stato sviluppato un progetto dall'Associazione non-profit "Visionari", che punta a un sistema alla "*Minority Report*" dove la macchina è in grado di capire e impedire che un reato possa accadere, valutandone il probabile rischio e le anomalie nel comportamento dei cittadini.

In Italia, i software predittivi⁶³⁵ vengono già impiegati: la Questura di Milano usa "*Keycrime*", mentre a Napoli "*X-Law*"⁶³⁶.

In ogni caso, è un compito molto arduo, in quanto il legislatore deve riuscire a bilanciare la tutela dei diritti fondamentali della vittima, attribuendo delle pene adeguate, cercando di non incorrere in violazioni della *privacy*, mediante l'instaurazione di sistemi che, seppur prevenendo il fatto illecito, possano costringere la persona a dover scegliere tra il proprio diritto alla libertà online e la probabile violazione dei diritti.

Per una maggiore cooperazione tra gli Stati Membri dell'Unione, la Commissione Europea ha proposto l'uso di questi strumenti di Intelligenza artificiale per semplificare il lavoro dell'Eurojust, automatizzando le informazioni⁶³⁷.

Per rendere la disciplina più chiara e per facilitare il compito del legislatore si auspica anche, al più presto, una modifica della disciplina all'articolo 612ter, confidando nella possibilità di integrazione di tutte quelle fattispecie circostanziali che fanno riferimento al reato di diffusione illecita di immagini o video sessualmente esplicite, in modo tale da fornire una pena adeguata, seguendo il principio di certezza della pena.

Questo bilanciamento fra diritti è stato oggetto di dibattito soprattutto in Cina, con l'avvento dei telefoni di nuova generazione che "bloccavano" la possibilità di scattare foto intime con il telefono, con particolari *software* di Intelligenza Artificiale che riconoscevano il pericolo di divulgazione di immagini di nudo.

Anche in America ci si è posti lo stesso quesito in relazione al diritto alla *privacy* e alla libertà di espressione, oggetto di tutela del Primo Emendamento.

Secondo parte della Dottrina americana, affinché il *Revenge porn* possa essere considerato come un reato di matrice sessuale, si dovrebbe pensare alla violazione dell'autonomia della vittima come elemento sufficiente per una espansione dei confini del reato, soccombendo in questo modo alla violazione del "*Freedom of speech*".

Tuttavia, il dibattito fondamentale riguarda il dolo specifico: alcuni lo ricondurrebbero alla *mens rea*, ossia l'elemento psicologico del crimine, in modo tale da ovviare la violazione del Primo Emendamento, mentre altri lo collegherebbero all'*actus reus*; quindi, verrebbe considerato una conseguenza del danno.

⁶³⁵ software di *predive policing*, in merito BRANTINGHAM P.J.Q., *The Logic of Data Bias and Its Impact on Place-Based Predictive Policing*, in *Ohio State Journal of Criminal Law*, 2018, p. 473 e ss.; BURCHARD C., *L'intelligenza artificiale come fine del diritto penale?* cit., p. 1922 e ss., 2019

⁶³⁶ CONTISSA G., G. LASAGNI, G. SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di internet*, 2019, p. 621; SERRA M., *Rapinatore seriale catturato grazie al software "Key crime"*, in *La stampa*, 2018

⁶³⁷ COMMISSIONE EUROPEA, "*Cross Border Digital Criminal Justice*", Final Report, Lussemburgo, 2020

Interessante è stato analizzare le singole discipline (le più famose e rilevanti, come quella di *New York*, della *California* ecc.) in quanto le normative sono diverse da Stato a Stato, la maggior parte però, aderisce alla prima ipotesi.

L'unico modo reale, stante alla Dottrina, per ovviare il problema, sarebbe creare una legge federale: le proposte sono state varie, una per esempio del 2016, l'*Intimate Privacy Protection Act*, e una più recente, del 2023, in relazione al fenomeno del *deepfake* pornografico, lo *Shield act*.

Tornando a parlare della normativa nazionale, ho poi proseguito con la descrizione dei cambiamenti effettuati della riforma del Codice rosso, e delle fattispecie che venivano applicate prima della sua entrata in vigore.

Al capitolo tre mi sono occupata di descrivere come l'Intelligenza Artificiale, dopo aver fatto cenno anche alle sue implicazioni giuridiche, alla regolamentazione e alla nascita, possa esser accostato al reato all'articolo 612ter, creando nuove tipologie di reato, tra cui il porno *deepfake*.

Infatti, sebbene l'Intelligenza artificiale possa essere utilizzata per la rimozione dei contenuti *online*, la prevenzione e il monitoraggio dei reati sessuali e della diffusione di immagini a sfondo sessuale sulla rete, può anche esser sfruttata proprio per la commissione di questi ultimi, mediante la creazione e la manipolazione di fotografie, registrazioni video o audio, come nel caso dei *deepfake*.

Prima di fornire le mie considerazioni su questo fenomeno, è doveroso ricordare alcune nozioni in merito alla regolamentazione dell'Intelligenza Artificiale.

È importante sottolineare che la disciplina normativa sulla Ai è ancora in fase di evoluzione, considerando la sostanziale inadeguatezza dei sistemi giuridici di far fronte, secondo gran parte della Dottrina, allo sviluppo esponenziale della tecnologia. Il primo atto legislativo a livello europeo è stato l'*AI act*, il quale mira a istituire un mercato interno armonizzato, per la tutela dei diritti fondamentali dei cittadini, l'obiettivo è quello di rendere l'Intelligenza Artificiale un sistema affidabile.

Ma questa tecnologia può essere ritenuta veramente e al 100% affidabile?

Secondo la Dottrina, non può essere ritenuta tale, per varie ragioni: innanzitutto per la fallibilità e il carattere sicuramente "parziale" delle informazioni che vengono registrate *online*, di cui, tramite il sistema *deep learning*, la macchina si nutre.

Uno dei pericoli, infatti, sarebbe la possibilità dell'Intelligenza Artificiale, di prendere decisioni discriminatorie, in base alle informazioni che assume.

A causa infatti, dell'apprendimento automatico, la macchina ottiene delle informazioni che potrebbero contenere degli errori e quindi potrebbe riflettere quei pregiudizi presenti nei dati utilizzati come "addestramento".

Senza contare il fatto che, in caso di errori, chi ne sarebbe responsabile?

Vari studiosi si sono posti questo dilemma, soprattutto nel caso in cui la macchina non abbia un controllo diretto dell'uomo.

La sorveglianza dell'uomo sulla macchina diventa quindi uno dei metodi di controllo di base, secondo il Libro Bianco sull'IA; perciò, sono necessarie figure tecniche che se ne occupino, per tutte le fasi di conservazione delle informazioni.

Più è alto il livello di autonomia della macchina più necessita di valutazione, per cui il processo decisionale in ultima istanza deve essere responsabilità dell'uomo.

Altro problema che va considerato, a mio parere, è il “gap” generazionale, con cui inevitabilmente, ci si va a scontrare: l'IA sta prendendo piede nella nostra quotidianità con sistemi sempre più avanzati, senza considerare tutte quelle persone, come anziani, disabili, o semplicemente persone che non possono permettersi il “progresso”, che non riescono a rimanere aggiornati con i tempi.

La rivoluzione dell'Intelligenza Artificiale è diventata una realtà e solo chi rimane competitivo nel mercato digitale e si aggiorna, sarà in grado di sfruttare appieno le potenzialità che l'era digitale offre.

Invero, per utilizzare questi strumenti servono delle competenze digitali e se queste non fossero possedute, la persona comune potrebbe trovarsi in una situazione di svantaggio nell'economia per esempio aziendale.

Perciò il legislatore dovrebbe considerare anche queste categorie di cittadini durante la regolamentazione dei nuovi strumenti.

Oltre a questo tipo di rischi, bisogna considerare soprattutto, come abbiamo messo in luce nelle pagine precedenti, i rischi per i diritti fondamentali dell'individuo e gli obiettivi di trasparenza ed etica morale da porre al primo posto durante l'utilizzo di questi strumenti.

Ciò tenendo a mente il fatto che l'IA è in grado di elaborare enormi quantità di dati e può essere soggetta anche ad attacchi informatici, mirati a manipolarli oppure ad averne un accesso non autorizzato.

Per questo, l'uso indiscriminato e incontrollato getta un'ombra di dubbio sulla sua effettiva affidabilità, dato il bisogno di tutela della *privacy* e dei propri dati, spesso anche sensibili, e il rischio di compromissione delle informazioni personali.

Si pensi anche ai danni a livello sociale che un utilizzo eccessivo della IA può portare, come è successo nel caso accaduto in Belgio nel 2023, quando un uomo si tolse la vita dopo aver “parlato” assiduamente con una Intelligenza Artificiale, isolandosi⁶³⁸.

È opinione comune tra gli esperti che l'IA non può comprendere la complessità delle emozioni umane; quindi, mancando di empatia potrebbe avere un impatto negativo sulle nostre vite.

Pertanto, è giusto ritenere che l'uso delle decisioni automatizzate possa recare grande vantaggio in termini di efficienza, all'uomo, ma il legislatore si deve preoccupare di garantire un utilizzo responsabile anche in luce delle future sfide etiche e regolamentari. Invero, secondo Luciano Floridi, la continua espansione dell'IA «*exacerbates old ethical problems, reshapes some of them, and creates new ones*»⁶³⁹, d'altro canto, la Commissione Europea non può utilizzare altri metodi per regolarizzare il fenomeno, se non attraverso direttive e regolamenti, come l'*AI act*.

⁶³⁸ GDPR, SCORZA G., “Istruzioni per morire dal mio amore artificiale”, L'espresso, 6 settembre 2024

⁶³⁹ FLORIDI L., *The Ethics of Artificial Intelligence: exacerbated problems, renewed problems, unprecedented problems*, in *American Philosophical Quarterly*, 2024, 61(4), 301.

Risulta fondamentale l'implementazione di regolamenti internazionali, al fine di evitare una disparità e incertezza giuridica tra Paesi, poiché in loro assenza, il divario tecnologico sarebbe talmente netto da non consentire un progresso unitario e collaborativo.

L'*Ai act*, è un Regolamento che, insieme alla Carta dei diritti fondamentali, al GDPR, la CEDU e le Costituzioni dei singoli Stati Membri, si pone come base per le future regolamentazioni e concorre alla protezione dei diritti, limitando l'impiego indiscriminato di questi nuovi strumenti digitali.

Bisogna quindi garantire protezione, non solo dal punto di vista legale, ma anche incoraggiare la consapevolezza collettiva sui rischi psicologici e sociali, al fine di sviluppare un equilibrio tra vantaggi e svantaggi dell'uso di questi strumenti.

Un pericolo che ha preso piede negli ultimi anni sulla scena dei reati *online* è la creazione di porno *deepfake*, che viene definito come quella procedura di “spogliare” utilizzando strumenti digitali, le donne.

Molto spesso questi contenuti vengono divulgati online, con le stesse finalità del Revenge porn, per questo, molti lo definiscono come una “evoluzione”, al passo delle nuove tecnologie, di questo tipo di reato.

Innanzitutto, però, ritengo doveroso ricordare che i *deepfake*, secondo la definizione del Garante della *privacy*, sono tutte quelle foto, video o audio reali, che poi vengono modificate grazie all'uso di sistemi di Intelligenza Artificiale, in modo estremamente realistico⁶⁴⁰.

Questo sistema costituisce un problema non solo per i diritti di libertà sessuale, nel caso del porno *deepfake*, ma anche per altri ambiti della vita quotidiana, come ad esempio il diritto a una informazione corretta e veritiera della stampa, per il caso delle *fake news*, che possono benissimo essere create artificialmente.

Sia vari stati, che anche i social network stessi, stanno facendo il possibile per arginare questo fenomeno in modo più celere.

Fondamentale quindi, è una educazione digitale di massa, che permetta anche al comune cittadino di capire quando un video o una foto è creata artificialmente, cercando di individuarne i segnali spia, i cosiddetti “*bug*” del sistema.

Per quanto riguarda il porno *deepfake*, questo avviene mediante la trasformazione di una foto di una donna vestita (o poco) in una immagine ritraente la stessa, senza vestiti, oppure si può utilizzare una foto comune, ritraente il viso di una donna, e “incollarlo” sopra una immagine di una donna nuda, come è successo a Taylor Swift, Giorgia Meloni e Scarlett Johansson.

Secondo il Washington Post «*l'Internet è un abisso che rimane virtualmente privo di regolamentazione*»⁶⁴¹.

⁶⁴⁰ Garante per la protezione dei dati personali, 2020, *Deepfake: dal Garante una scheda informativa sui rischi all'uso malevolo di questa nuova tecnologia, deepfake: il falso che ti ruba la faccia e la privacy*

⁶⁴¹ Cfr. HARWELL D., *Scarlett Johansson on fake AI-generated sex videos: 'Nothing can stop someone from cutting and pasting my image'*, in The Washington Post, 2018

Se queste immagini vengono poi condivise sui *social* senza consenso della persona offesa, si sfocia nel *Revenge porn*.

Infatti, in questo caso, il soggetto attivo non avrà bisogno di rubare le immagini sessualmente esplicite dal telefono della vittima oppure utilizzare quelle che la stessa, in via confidenziale, ha inviato, basterà esser dotati di un *software*, che grazie all'Intelligenza Artificiale si occuperà di tutto.

L'aspetto più sconvolgente, a mio parere, è il carattere realistico di queste fotografie, tale da non riuscire più a distinguere la realtà.

Tuttavia, dalla analisi fin qui condotta si è potuto notare come l'applicazione dell'articolo 612ter così com'è oggi, porterebbe a una violazione del principio di tassatività, interpretando in modo eccessivamente ampio la fattispecie e arrivando addirittura a interpretazione analogica in *malam partem*.

Inoltre, molti studiosi ritengono sia necessaria l'implementazione dell'uso dell'Intelligenza Artificiale per la diffusione di contenuti di carattere intimo.

Per questo, di recente si è pensato all'introduzione dell'articolo 612 quater, proposto dal governo Meloni con un decreto-legge, che punirebbe con la reclusione da uno a cinque anni chiunque diffonde video o immagini false, generati o manipolati con l'uso dell'Intelligenza Artificiale.

Sicuramente, se questa fattispecie dovesse entrare in vigore definitivamente nel Codice penale, sarebbe una grande svolta per la tutela dei diritti delle vittime di porno *deepfake*. Non solo l'Italia ha deciso di muovere i suoi primi passi per la criminalizzazione di questo fenomeno, infatti, decisione simile è stata presa anche in Inghilterra: il governo ha voluto introdurre una legge che prevede la reclusione fino a due anni non solo per chi scatta fotografie o video intimi senza consenso, ma anche per chi genera immagini intime con l'uso dell'Intelligenza Artificiale, usando volti di persone vere.

La differenza tra le due normative, se verranno introdotte, risiede principalmente nel fatto che l'Italia, criminalizza la diffusione, mentre in Inghilterra pone di più l'attenzione sulla creazione, non la divulgazione di questi contenuti.

La facilità d'uso di questi *software*, come *bikini off* o *deep nude*, possono potenzialmente esporre a questo pericolo ogni persona che ha una sua foto sul *web*, perciò sarà necessario, oltre a limitare la condivisione di proprie foto online, anche la modifica frequente di password, per tutelare i dati personali, ma anche l'utilizzo di tecnologie di protezione della rete, come un VPN (*Virtual Private Network*).

Per questo, ipotizzo sia possibile utilizzare gli stessi sistemi di IA per contrastarne l'uso improprio, considerando la possibile futura messa in commercio di *software* che possano bloccare completamente il caricamento su qualsiasi piattaforma online, di fotografie *deepfake porn* o di *Revenge porn*.

Si auspica anche che il legislatore si occupi di dar vita a un sistema giuridico adeguato al progresso tecnologico, sebbene ci siano state delle novità, come l'introduzione della fattispecie di reato all'articolo 612ter, volto a tutelare le vittime di diffusione illecita di immagini o video a sfondo sessuale, tuttavia questa non considera appieno le specificità

della tecnologia e non affronta la velocità con cui avviene la diffusione del contenuto illecito.

In conclusione, il giurista, in questi anni di celere e imprevedibile progresso tecnologico, non ha di certo avuto vita semplice, in merito all'opera di adeguamento e regolamentazione dell'Intelligenza Artificiale, causando notevoli dibattiti sia in Dottrina che in Giurisprudenza.

Sicuramente, l'AI ha avuto un grande impatto ed ha portato anche molti vantaggi in vari settori, come l'istruzione, la medicina, l'industria, ha migliorato i processi di analisi dei dati, mediante un procedimento automatizzato, rendendo le informazioni molto più rapide, ma non si può non considerare anche i tanti aspetti negativi, come la preoccupazione per i diritti alla riservatezza, alla sicurezza dei dati e alla mancata trasparenza dei procedimenti, ma anche la possibilità che questa possa esser usata come strumento di attuazione dei reati, e che, con il tempo, possa diventare uno strumento "incontrollabile".

Di recente, infatti, due sistemi di Intelligenza Artificiale, grazie a un esperimento in Cina, si sono auto-duplicati senza l'intervento umano⁶⁴²; questa nuova vicenda mette ancora di più in dubbio la sicurezza e l'affidabilità di questi sistemi che potrebbero sfuggire al controllo umano, ponendo un grande punto interrogativo sulla loro regolamentazione e sul futuro prossimo.

Solo tramite una coordinazione di governi, aziende e cittadini, si potrà limitare l'Intelligenza Artificiale ad un utilizzo positivo per le nuove generazioni, integrando diritto, tecnologia, educazione.

È auspicabile che il legislatore, tramite uno studio approfondito delle nuove tecnologie e delle possibili problematiche che ne potrebbero derivare, accompagnato da una grande ponderazione nell'introdurre delle nuove fattispecie di reato, fornisca al cittadino, nel rispetto del diritto all'immagine e dei diritti fondamentali, una tutela completa, anche mediante una cooperazione con i Paesi Europei, al fine di istituire una armonica legislazione che ben possa intersecarsi con l'umanizzazione delle nuove tecnologie.

⁶⁴² Esperimento condotto dall'Università Fudan di Shanghai, sono due i sistemi coinvolti: Llama 3.1 di Meta e Qwen 2.5 di Alibaba. Articolo ANSA, 27 gennaio 2027, ENRICA BATTIFOGLIA

BIBLIOGRAFIA

- ADINOLFI A., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione*, 2022
- ADINOLFI A., *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europea tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini Giuridica, Pisa, 2020
- AGGARWAL C.C., *Deep Neural Networks and Deep Learning: a textbook*, II ed., 2023
- AGID, *l'Intelligenza Artificiale e I Diritti Fondamentali*, 2021, Lussemburgo
- ALGERI L., *Il c.d. Codice rosso: tempi rapidi per la tutela delle vittime di violenza domestica e di genere*, in *Diritto penale e processo*, 2019
- ALIBRANDI L., *Codice penale commentato*, cinquantesima edizione, 2024
- ALUIGI F., GAROFALO A., PIEMONTE J. Articolo dell'AGID, 13 Marzo 2024
- AMIDEI A., *La governance dell'Intelligenza Artificiale: profili e prospettive di diritto dell'Unione Europea*, in U. Ruffolo (a cura di), *Intelligenza artificiale - Il diritto, i diritti, l'etica*,
- AMORE N., *La tutela penale della riservatezza sessuale nella società digitale*, 2020
- ANDREUCCIOLI, "misure per il contrasto della diffusione non autorizzata di materiale sessualmente esplicito" in A.S. 2016, servizio studi del senato n 57 marzo 2019.
- ANSA, 15 gennaio 2023, Napoli, redazione ansa
- ANSA, Antonio Michienzi, 10 luglio 2024
- ANSA, articolo 30 gennaio 2024
- ARENA M., Crio papers n. 59, *La Convenzione di Budapest del Consiglio d'Europa sulla Repressione della criminalità informatica*, 2021 (a cura di) Rosario Sapienza
- ARRUZZOLI F., "Deepfake e cyber Intelligence, tecniche di creazione, rilevamento e prevenzione" White paper 06/2022
- AssoDPO (2023), *AI ACT, la meta è vicina: un nuovo standard globale*, 19 dicembre 2023
- ATTESTIV, *Deep fake video detention software*, 2019-2025
- AYYUB R., HuffPost "I was the victim of a deepfake porn plot intended to silence me", 2018
- BAFFA G., *Gli atti persecutori. Gli elementi costitutivi della fattispecie e la definizione dei rapporti specifici con altre norme incriminatrici*, in *Temi penali*, Vol. II, *Delitti contro la persona. Delitti contro il patrimonio*, a cura di M. Trapani, A. Massaro, Giappichelli, 2019
- BALDASSARRE A., BRISCHETTO A., PISTOLESI M., *Human centered AI*, rivista italiana di Ergonomia, 2020, n. 21, Società Italiana di Ergonomia
- BASSINI M., L. Liguori, O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?* in F. Pizzetti (a cura di), *Intelligenza artificiale*, 2018
- BARANELLO Alessia, "Casi di deepfake pornografici: intelligenza artificiale?" 2024, rivista Lampoon
- BARISON C., Corriere della sera, 2024, *Rose Villain vittima di deepfake che la ritraggono nuda: «È violenza»*
- BARMORE C., *Criminalization in Context*, 2015
- BASILE E., *La tutela delle donne dalla violenza dell'uomo: dal Codice Rocco ... al codice Rosso*, in *Diritto penale e uomo*, 2019
- BASSOLI Elena, "Intelligenza artificiale, tutela della persona e dell'oblio", 2021, Pacini ed.

BATES, *Revenge porn and mental health: a qualitative analysis of the mental health effects of revenge porn on female survivors*, *Feminist Criminology*, Vol. 12(1) 22–42, 2017.

BBC News, 2013 “*Boston Bombing, how internet detectives got very wrong*”

BBC News, articolo di Joe Ordinato, 28 agosto 2024

BBC, “*South Korea faces deepfake porn emergency*”, 24 Agosto 2024, Nick Marsh, Jean Mackenzie

BECCARI, *Le prime difficoltà applicative della nuova fattispecie di “Revenge porn” in caso di diffusione del materiale da parte di soggetti estranei al rapporto sessuale*, in *Sistema penale*, 2022

BECCARIA, *Dei delitti e delle pene*, edizione a cura di Venturi, Torino, 1764

BELISARIO E., RICCIO G.M., SCORZA G., (a cura di) *GDPR e normativa privacy commentario*, II ed., 2022

BELLACOSA M., in *Diritto Penale Contemporaneo*, “*il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*”, 2015,7.

BERTOLINO M., *Violenza e famiglia: attualità di un fenomeno antico*, in *Riv. it. dir. proc. pen.*, 2015

BIANCHI M., *L’incriminazione del “Revenge porn”: il nuovo delitto di “diffusione illecita di immagini o video sessualmente espliciti”*, in *Diritto penale*, Tomo III, *I delitti contro la libertà morale*, A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), Torino, UTET, 2022

BIANCHI M., “*Il sexting minorile non è più reato?*”, 2016

BLITZ M. J., *Deepfakes and Other Non-Testimonial Falsehoods: When is Belief Manipulation (Not) First Amendment Speech?* in *Yale Journal of Law & Technology*, 23, 2020

BOEHM, *Il ritorno delle immagini*, in *Teorie dell’immagine. Il dibattito contemporaneo*, a cura di Pi- notti-Somaini, Milano, 2009, 42 ss.

BRANTINGHAM P.J.Q., *The Logic of Data Bias and Its Impact on Place-Based Predictive Policing*, in *Ohio State Journal of Criminal Law*, 2018

BRASCHI S., *La nozione di “violenza domestica” tra tutela dei diritti umani e sistema penale*, in *Criminalia*, 2022, anticipato su *disCrimen*, 3 luglio 2023

BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, 1970

BRIDLE., *Nuova era oscura*, 2019

BRIZZI, *Diffusione illecita di immagini o video sessualmente espliciti: tra tutela della privacy e Revenge porn in: Il penalista*, 2021.

BRUNO A., CAMPANELLA I., *Elementi di vittimologia*, 2023, ed. youcanprint

BURRIS A., *Hell hath no fury like a woman porned: revenge porn and the need for a federal nonconsensual pornography statute*, in *Florida Law Review*, 2014, vol. 66, 2325 ss.

BURCHARD C., *L’intelligenza artificiale come fine del diritto penale?* 2019

CADOPPI A. - VENEZIANI P., *Elementi di diritto penale: parte speciale*, vol. II, I reati contro la persona tomo II, I reati contro i soggetti deboli, III edizione Padova, 2023

CAMPAGNOLI M.N., *Social media e information disorder: questioni di ecologia comunicativa in Rete (Parte Terza – Il Revenge porn)*, in *Dirittifondamentali.it*, 2020

CANESTRARI s., *Una buona legge buona (DDL recante «norme in materia di consenso informato e di disposizioni anticipate di trattamento»)*, in *Riv. it. med. leg.*, 2017

- CALDERS T.-I. ŽLIOBAITĖ, *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, in *Discrimination and Privacy in the Information Society*, Springer, 2013
- CALETTI G.M., *Revenge Porn e tutela penale, prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze anglo-americane*, 2018
- CALETTI G.M., in *Diritto Penale Contemporaneo*, 3/2018, *la pena tra teoria e realtà*, p. 101, ISSN 2240-7618
- CALETTI G.M., “Revenge Porn”. *Prime considerazioni in vista dell’introduzione dell’art. 612-ter c.p.: una fattispecie “esemplare”, ma davvero efficace?* in *Diritto penale contemporaneo*, 29.5.19
- CALETTI G.M. *L’art. 612-ter c.p. e l’incriminazione della pornografia non consensuale*, in *Rivista italiana di diritto procedura penale*, 2019
- CALETTI G.M., *Libertà e riservatezza sessuali all’epoca di internet*, 2019 in *Rivista Italiana di diritto e procedura penale*
- CALETTI G.M., *Can Affirmative Consent Save “Revenge Porn” Laws? Lessons from the Italian Criminalization of Non-Consensual Pornography*, in *Virginia Journal of Law & Technology*, 2021, 25, 3, 112 ss.
- CALVERT C., *Revenge Porn and Freedom of Expression: Legislative Pushback to an Online Weapon of Emotional and Reputational Destruction*, in *Fordham Intellectual Property Media & Entertainment Law Journal*, 2014
- CAMERA DEI DEPUTATI, *Introduzione dell’articolo 612-quater del Codice penale, in materia di manipolazione artificiale di immagini di persone reali allo scopo di ottenerne rappresentazioni nude*, 21 luglio 2021.
- CAMPAGNOLI M.N., *Social media e information disorder: questioni di ecologia comunicativa in Rete*, dirittifondamentali.it, 9 novembre 2020.
- CANCIO MELLA’ M., *Guerra cultural y reforma de los delitos sexuales*, in *El País*, 7 giugno 2022
- CANESTRARI S., et Al., *Manuale di Diritto Penale* 594 (2d ed. 2017)
- CAPUTO M., *Eventi e sentimenti nel delitto di Atti persecutori*, in *Studi in onore di Mario Romano*, a cura di M. Bartolino, L. Eusebi, G. Forti, vol. III, Jovene, 2011
- CARANTANI (2024), *IA Act: l’Unione Europea approva la proposta di Regolamento sull’intelligenza artificiale*, in “*Ius in itinere*”, 3 maggio 2024
- CARLEO A. (a cura di), *Il vincolo giudiziale del passato. I precedenti*, luglio 2018 cit.
- CASONATO J., *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE online*, 3, 2020, 3369
- CBS News, *I never said that! High tech deception of ‘deepfake’ videos*, in cbsnews.com, 2 luglio 2018
- CELOTTO A., *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Riv. Analisi Giuridica dell’Economia*, 1/2019,
- CHADHA A., V. Kumar, S. Kashyap, M. Gupta, *Deepfake: An Overview*, in P. K. Singh – S. T. Wierzchoń – S. Tanwar – M. Ganzha – J. J. P. C. Rodrigues (a cura di) *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*, Cham, 2021, 557 ss.
- CHANEY S., RATCLIFF J., *GIS and Crime Mapping*, John Wiley & Sons ltd, U.K, 2005

CHALMERS J., LEVERICK F., *Fair Labelling in Criminal Law*, 71 MOD. L. REV. 217 (2008)

CITRON, *Sexual Privacy*, in *Yale Law Journal*, 2019, 128, 1895 ss

CITRON D.K., *Hate Crimes in cyberspace*, 2016

CITRON D.K., FRANKS M.A., *Criminalizing Revenge Porn*, 2014

CLEYNENBREUGEL V. *EU By-Design Regulation in the Algorithmic Society*, in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor e G. De Gregorio (a cura di)

CLUSIT, 2024, *Rapporto sulla Sicurezza ITC Italia*

COFFEY G., "Codifying the Meaning of 'Intention' in the Criminal Law" October 2009 *Journal of Criminal Law* 73(5):394-413; 73(5):394-413

COLAPIETRO C., A. Moretti, *L'intelligenza artificiale nel dettato costituzionale*, 2020

COLELLA, CASALNUOVO "il codice rosso. Guida operativa alla legge n 69 del 2019", Piacenza, 2019,42

COMMISSIONE EUROPEA, *Una strategia europea per i dati*, COM (2020)66, 19 febbraio 2020

COMMISSIONE EUROPEA, *Eu Commission: shaping Europe's digital future*, 2020

COMMISSIONE EUROPEA, *A Union of Equality: EU anti racism action plan 2024-2025; Report on the implementation of the EU anti racism action plan*, 25 Settembre 2024

Commissione europea, *Libro Bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia* (COM 2020/65 final), 19 febbraio 2020

COMPOSTELLA, *Auto a guida autonoma e diritto penale. Profili di responsabilità individuale e collettiva*, Università di Trento, 2024

CONTALDI G., *Intelligenza Artificiale e dati personali*, 2021

CONTISSA G., G. LASAGNI, G. SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di internet*, 2019

CONSIGLIO DELL'UNIONE EUROPEA, 18 novembre 2022, "decisione di Promozione dell'innovazione responsabile nell'IA per la pace e la sicurezza" n. 2269

CORRIERE DELLA SERA *Violenza sulle donne. Colpa di come vestono*, 26.11.19

CORRIERE DEL TICINO, Valentina Coda, 2019

COSMOPOLITAN, Elisabetta Moro, 2 Aprile 2024, intervista

COVELLI M.L., *Dall'informatizzazione della giustizia alla "decisione robotica"? Il giudice di merito*, in A.Carleo (a cura di), *Decisione robotica*,

CRAWFORD K. "Atlas of AP" pubblicato dalla Yale University Press, 6 aprile 2021

Criminal Justice and courts Act, 2015, section 33

D'ALOIA A., *Il diritto verso "il mondo nuovo"*, 2019

DAVICO A., *stalking, atti persecutori, articolo 612bis cp*, 2022

DE GREGORIO G., DUNN P., POLLICINO O., *A partire dalla Strategia per il Mercato Unico Digitale, l'approccio basato sul rischio è stato applicato in tutte le principali normative UE: analizziamo le analogie e le differenze tra GDPR, DSA e AI Act*, 15 Settembre 2022.

DE RENZIS L., *Primi passi nel mondo della giustizia "high tech": la decisione in un corpo a corpo virtuale fra tecnologia e umanità*, in A.Carleo (a cura di), *Decisione robotica*, cit., 150

DE SIMONE G., *Il delitto di atti persecutori*, Roma 2013, passim; A. Valsecchi, *Il delitto di "atti persecutori" (il cd. stalking)*, in Riv. it. dir. proc. pen., 2009

DE URBINA GIMENO I.O., *Adesso davvero hispanica societas delinquere non potest*, Criminalia, 2010

DE VITA R., M. DELLA BRUNA, *Non consensual Pornography: dal Revenge Porn alla sexual extortion*, Osservatorio Cyber Security dell'Eurispes, 17.12.2019

DELFINO R.A., *Pornographic deepfakes: the case for federal criminalization of revenge porn's next tragic act*, *Fordham Law Review*, Vol. 88 issue 3, 2019

DEL VECCHIO K., *New Jersey's code of criminal Justice, a practical guide*, 2025

DEVLIN H., The guardian, 10 Maggio 2024, "is AI lying to me? Scientists warn of growing capacity for deception"

DIBBELL, *A Rape in Cyberspace (Or Tiny society and How to Make One)*, in *Violation: rape in gaming*, a cura di Thorn, Dibbell, 2012, 21 ss.

DOLCINI E., GATTA GL., *Codice penale commentato*, V ed. 2021, Milano

DONCIEUX S., J. MOURET, "Beyond black box optimization: a review of selective pressures for evolutionary robotics" in *Evolutionary Intelligence*, 7, 2014

DOVA M., *sub Art. 612-ter*, in *Codice penale commentato*, E. Dolcini, G.L. Gatta (diretto da), Tomo III, *Artt. 452bis-649bis*, V ed., Milano, Wolters Kluwer, 2021

DONAGHUE E., *Judge Throws Out New York Revenge Porn Case*, CBS (Feb. 25, 2014, 4:42 PM)

DR TAYLOR J., *why women are blamed for everything: exposing the culture of victim blaming*, 2021

DUFOUR N., A. GULLY, P. KARLSSON, A.V. VORBYOV, T. LEUNG, J. CHILDS and C. BREGLER, "Deepfakes Detection Dataset", 2019

DURANTE M., PAGALLO U., *Manuale di Informatica Giuridica e diritto delle nuove tecnologie*, 2017

ELOSEGUI M., *The Case Law of the European Court of Human Rights on Violence Against Women and the Intimate Image Abuse*, in G.M. Caletti, K. Summerer (a cura di), *Criminalizing Intimate Image Abuse. A comparative perspective*, Oxford, 2023

EURISPES Osservatorio Cyber Security, *Revenge porn: la vendetta può colpire chiunque*, 17 dicembre 2019.

EUROPEAN COMMISSION, *State of Health in the EU*, Companion Report 2021

EUROPEAN COMMISSION, *Eu and Singapore Digital Partnership*, 1° febbraio 2023,

European Data protection Board parere del 5/2021 EDPB - GEPD

EUROPEAN COMMISSION, E.U-- U.S. *Research Alliance in AI for the Public Good*, 5 Aprile 2024

FABOZZO in "analisi normativa e profili problematici del reato di diffusione illecita di immagini o video a contenuto sessualmente esplicito ex art 612 ter cp", in *Riv. Pen.* 2020

FALLIS D., *The epistemic threat of deepfakes. Philosophy and technology.* 2021, 34 (4), pg. 623-643

FARACE R., RIBUSTINI L., "Uccisa dal web – Tiziana Cantone", sulla testimonianza di Maria Teresa Giglio, 2019

FARISK K., "Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of the deepfake", in *Journal of Intellectual Property Law & Practice*, 15, 2020

FERNÁNDEZ O., DELGADO L., "El nuevo delito contra la intimidación en el proyecto de reforma del Código Penal de 2013 y el "caso Olvido Hormigos". En: *Revista de Derecho y Proceso Penal.* 2014, núm. 35, pp. 183-220. ISSN 1575-4022. P. 184

FERONI CERRINA G., 20 gennaio 2023, Camera dei deputati, *Sala del Cenacolo, Palazzo Valdina, in occasione della presentazione del volume di F. Lazzini, Etica e Intelligenza artificiale, Torino, Giappichelli, 2022*

FERRARI I., *Analisi comparata in tema di responsabilità civile legata alla circolazione dei veicoli a guida autonoma*, in S. SCAGLIARINI (a cura di), *Smart Roads and Driverless Cars: tra diritto, tecnologia, etica pubblica*, Torino, 2019,

FIRMIANI MOIRA, *Compendio di normativa sulla privacy per il trattamento dei dati personali, guida alla lettura del codice della privacy e GDPR*, I ed., 2022

FIANDACA-DI CHIARA, *Una introduzione al sistema penale: per una lettura costituzionalmente orientata*, 2003

FIANDACA G., MUSCO E., "diritto penale. Parte generale", Zanichelli, Bologna, 2010

Financial Times, 11 marzo 2024, "Telegram emerges as new dark web for cyber criminals"

FIANDACA G., MUSCO E., *Diritto penale: parte speciale. I diritti contro la persona*, Vol. II, tomo primo, V ed., 2020

FLICK G.M., voce *Libertà individuale (delitti contro la)*, in *Enc. dir.*, vol. XXIV, Giuffè, 1974

FLORIDI L., *The European Legislation on AI: a brief Analysis of its Philosophical Approach*, 2021

FLORIDI L., *The Ethics of Artificial Intelligence: exacerbated problems, renewed problems, unprecedented problems*, in *American Philosophical Quarterly*, 2024

FLORIO F., "Non chiamatelo Revenge Porn, storie di vittime presunte colpevoli", 2022

FRA (2012), *Bringing rights to life: The fundamental rights landscape of the European Union*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione Europea

FRAGASSO, *La responsabilità penale del produttore di sistemi di intelligenza artificiale*, in *Sistema Penale*, 13 giugno 2023

FRANKS M.A., "Revenge Porn" Reform: A View from the Front Lines, 69 fla. 1. rev. pag. 1255

FONTANA S., *I deepfake stanno diventando una cosa seria*, 10 marzo 2023, in *facta news*

FROSINI, *Cibernetica, diritto e società*, Milano, 1973

FROSINI, "telematica e informatica giuridica" in *Enciclopedia del diritto*, 1992, XLIV, 60

GALLI R., *Nuovo corso di diritto penale*, Wolters Kluwer, 2017

GIACOBBE G., *Il "diritto alla riservatezza" in Italia*, 1988

GIANNINI A., *Intelligenza Artificiale, Human Oversight e Responsabilità Penale: prove d'impatto a livello europeo*, in *Criminalia*, 21 novembre 2021.

GDPR, dicembre 2020, "deepfake, il falso che ti ruba la faccia e la privacy"

GDPR, comunicato stampa, 23 ottobre 2020 doc. N. 9470722

GDPR, *Deepfake: dal Garante una scheda informativa sui rischi dell'uso malevolo di questa nuova tecnologia*, 28 dicembre 2020.

GDPR, *informativa sui rischi dell'uso malevolo di questa nuova tecnologia*, 2020

GERSTNER E., *Face/off: "deepfake" face swaps and privacy laws*, in *Defense Counsel Journal*, 87, 2020, 1 ss. VA. CODE. § 18.2-386.2.

GILLESPIE A.A., "Trust me, it's only for me" Revenge porn and criminal law, 2015

GINORI A., "Il candidato di Macron a Parigi spazzato via da un video porno", in "La Repubblica", 14 febbraio 2020.

GIUFFRIDA I., LEDERER F., N. VERMEYS, *A legal perspective on the trials and tribulations of AI: how artificial intelligence, the Internet of Things, Smart Contracts, and other technologies will affect the Law*, in *Case Western Reserve Law Review*, 2018, pp. 747 ss., in specie a p. 751.

GLESS S., E. SILVERMANN, T. WEIGEND, *If Robots Cause Harm, Who Is to Blame: SelfDriving Cars and Criminal Liability*, in *New Criminal Law Review*, 2016

GOISIS, *La violenza sessuale: profili storici e criminologici. Una storia di 'genere'*, in *penale contemporaneo*, 31 ottobre 2012, 17.

GOODFELLOW I.J., POUGET-ABADIE J., MIRZA M. BING XU, WARDE-FARLEY D., OZAIR S., COURVILLE A., BENGIO Y., AA.VV., *Generative Adversarial Networks*, Università di Montréal, 2014

GOOGLE CLOUD WHITEPAPER, "Generative AI, Privacy and Google Cloud", settembre 2020

GRADY P., *Center for Data innovation*, "Eu proposals will fail to curb nonconsensual deep fake porn", 2023

GROPPI T., *Alle frontiere dello Stato costituzionale*, 2020

GULLO, "delitti contro l'onore", in Viganò, Piergiallini (a cura di), "reati contro la persona e contro il patrimonio", Torino, 2015, 157

HACKER P., *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law*, in *Common Market Law Review*, 2018,

HALLEVY G., *When Robots Kill. Artificial Intelligence under Criminal Law*, Boston, 2013

HALLEVY G., *Liability for crimes involving Artificial Intelligence Systems*, 2014; *When robots kill; Artificial Intelligence under criminal law*, 2013

HALL-HEARN, "revenge pornography and manhood acts: a discourse analysis of perpetrators' accounts", in *Journal of Gender Studies*, 2019, XXVIII (2.)

HARRIS D., *Deepfakes: False Pornography Is Here and the Law Cannot Protect You*, in *Duke Law & Technology Review*, 17, 2019

HARRIS K., *Mapping Crime: principle and practice*, CMRC, U.S. Dep. Of Justice, U.S.A., 1999

HARWELL D., *Scarlett Johansson on fake AI-generated sex videos: 'Nothing can stop someone from cutting and pasting my image'*, in *The Washington Post*, 2018

HAUGELAND J., *Artificial intelligence: the very idea*, Cambridge (Massachusetts), 1985

HAWKING S., *Brief answers to big questions*, 2018

HENRY N., *Imaged-based sexual abuse. A study on the causes and consequences of non-consensual nude or sexual imagery*, Londra, 2021.

High-Level experts Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, Bruxelles, 8 aprile 2019, 45

HOME SECURITY HEROES, 2023 "State of deepfakes, realities, threats and impact"

HÖRNLE, *The New German Law on Sexual Assault and Sexual Harassment*, in *German Law Journal*, 2017

HUMBACH "the constitution and revenge porn" in *Pace Law Review* 2015 vol 35,1, 202 ss.

IASELLI M., "Il diritto all'Oblio: un giusto diritto che non può essere riconosciuto", Gennaio 2018

ICO (information commissioner's office), "how to use Ai and personal data appropriately and lawfully", 2022

ICT SECURITY MEGAZINE, *Deepfake e cyber-intelligence: tecniche di creazione, rilevamento, e prevenzione*, 2022

ILARDA G. e G. MARULLO, *Cybercrime: Conferenza Internazionale. La convenzione del consiglio d'Europa sulla criminalità informatica*, Milano 2004

IL CORRIERE, “*stupro di Palermo*” 23 agosto 2023

IL CORRIERE DELLA SERA (Mar. 14, 2019), SARZANINI F, *Giulia Sarti, le foto e i video in rete*

IL FATTO QUOTIDIANO, F.Q., 1° dicembre 2017

IL FATTO QUOTIDIANO, Articolo di Vincenzo Iurillo, 11 gennaio 2024

IL MANIFESTO, Yuri Colombo, “*Russia, «la violenza di genere non esiste»*”, 22 novembre 2019

IL MATTINO, *La morte di Tiziana, il Pm chiede il processo per l'ex compagno*, Leandro del gaudio, (May 20, 2018, 2:04 AM)

IL POST, Articolo del 5 aprile 2019 “*dovremmo trovare un altro nome al Revenge porn*”

IL POST, Filippo Facci, *Storia di Tiziana Cantone*, (Settembre 15, 2016)

IL SOLE24ORE, Camera, “*Revenge porn escluso dal codice rosso*”, 2019

IL SOLE24ORE, articolo di Bianca Lucia Mazzei, 21 dicembre 2023

IL SOLE24ORE, 21 dicembre 2023, articolo di Bianca Lucia Mazzei” *Revenge porn: gli stop decisi dal garante quintuplicati nel 2023*” dati ricerca

INTEL, “*Intel introduces real time deepfake detector*”, Novembre 2022

INTERNATIONAL JOURNAL OF CYBER CRIMINOLOGY – ISSN: 0974–2891 July - Dicembre 2019. Vol. 13(2): 418–438; 2019

CALVINO I., “*Lezioni Americane, sei proposte per il prossimo millennio, esattezza*”, 1988

Japan Times, SHIMBUN Y. maggio 2021, Cristina Gauri

KASPERSKY, Studio “*Lo stato dello stalkerare*”, 2021

KING T.C., N. AGGARWAL, M. TADDEO, L. FLORIDI, *Artificial Intelligence crime: an interdisciplinary analysis of foreseeable threats and solutions, in science and engineering ethics*, 14 Febbraio 2019

KOPPELMAN A., *Revenge Pornography and First Amendment Exceptions*, 65 EMORY L. J. 661, 684- 90 (2016)

LABUZ M., *Regulating Deep Fakes in the Artificial Intelligence Act*, in ACIG, 1, 2023

LAKE J., UNSW Law Journal, *Disembodied data and corporeal violation: our gendered privacy law priorities and preoccupations*, 2019

LAMBERTUCCI P., *Intelligenza artificiale e tutela del lavoratore: prime riflessioni*, in *Argomenti di diritto del lavoro*, n. 5/2022,

LA REPUBBLICA, *Caso rimborsi, Giulia Sarti si autosospende dal Movimento 5 Stelle* (Feb. 26, 2019)

LA REPUBBLICA, articolo di Arturo di Corinto, 10 aprile 2020

LA REPUBBLICA, articolo di Antioco Fois, 23 giugno 2023

LA REPUBBLICA, articolo del 2015,” *Caso NSA, la Cia ha cercato di violare il software Apple dal 2006*”

LA STAMPA, Articolo di Marco Benvenuti, 19 dicembre 2018

LATTANZI G., Codice penale commentato, 2024, Giuffrè

LE JOURNAL DU DIMANCHE, 27 giugno 2023, Articolo di Cecile de Seze

LEGNINI G., *Introduzione*, in A. CARLEO (a cura di), *Decisione robotica*, RIVISTA AIC. 428

LIGGETT O'MALLEY-HOLT, *Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime*, in *Journal of Interpersonal Violence*, 2022, 37, 1-2, 258 ss.

LOMETTI S., *Il delitto di diffusione illecita di immagini o video sessualmente espliciti*, 2021

LO MONTE E., *l'Art. 612 ter, diffusione illecita di immagini o video sessualmente espliciti, tra buoni propositi, denegato diritto all'oblio e "morti social"*, Giappichelli editore

LONGO E., *I processi decisionali automatizzati e il diritto alla spiegazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione? Vol. I*, Il Mulino, Bologna, 2022

LONGO, SCORZA, *"Intelligenza Artificiale: impatto sulle nostre vite, diritti e libertà"*, Mondadori Education Università, Firenze, 2020

LOTTA C., *Prime osservazioni sul rapporto tra il reato di "Diffusione illecita di immagini o video sessualmente espliciti" e le libertà di corrispondenza e di manifestazione del pensiero*, 1° luglio 2019, Fasc. II.

LUCIANI M., *La decisione giudiziaria robotica*, 2018

MACRI' F., *Atti persecutori (Art. 612 bis)*, in I delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti, in *Trattato di diritto penale. Parte speciale*, Vol. IX, diretto da Cadoppi, S. Canestrari, Manna, Papa, Torino, 2011

MADDOKS 'A Deepfake Porn Plot Intended to Silence Me': *exploring continuities between pornographic and 'political' deep fakes*, in *Porn Studies*, 7, 2020

MAGRO M.B., *Robot, cyborg e intelligenze artificiali*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Utet, 2019; S. Beck, *Intelligent agents and criminal law – Negligence, diffusion of liability and electronic personhood*, in 86 *Robotics and Autonomous Systems*, 2016

MANGIONE A., *La tutela penale del minore da violenze, abusi e sfruttamento a sfondo sessuale*, in *La giustizia penale minorile: formazione, devianza, diritto e processo*, Terza edizione, A. Mangione, A. Pulvirenti (a cura di), Milano, Giuffrè Francis Lefebvre, 2020

MANNA L., *"Diritto all'oblio, le ripercussioni in Italia della Pronuncia Google Spain: primi provvedimenti del garante della privacy"* Gennaio 2015

MANTOVANI F., *Diritto penale. Parte speciale, I, Delitti contro la persona*, Padova 2019

MARINUCCI G., E. Dolcini, G.L. Gatta, *Manuale di Diritto Penale*, XI ed., 2022

MARTIRE D., *Intelligenza artificiale e Stato costituzionale*, 2022

MASSARO A.- M. TRAPANI, *Temi penali*, Giappichelli, 2013

MATTHEUDAKIS, *Un'indagine comparatistica sulla configurazione dei reati sessuali per colpa (grave) sui profili di consenso della vittima*, in *Revista de Direito Brasileira*, 2020

McAfee Corp. - global report "Cyberbullying in plain sight", 2022

MCGLYNN C., E. RACKLEY, *Image-Based Sexual Abuse*, 2019, in *Oxford Journal of legal studies*

MCGLYNN C., J. DOWNES, *We Need a New Law to Combat "Upskirting" and "Downblousing"*, in *Inherently Human*, 2019.

MCKINSEY & company, *"AI for social good: Improving lives and protecting the planet"*, Maggio 2024, Medha Bankhwal, Ankit Bisht, Michael Chui, Roger Roberts, and Ashley van Heteren, representing views from McKinsey Digital

MENDICINO R., La vittimizzazione secondaria, in *Profiling*, 2015

MERCORIO F., *Big Data, Intelligenza Artificiale, Industria 4.0: un'overview*, in Aa. Vv., *Metropolis, dai social media all'intelligenza artificiale*, a cura di M. Carvelli, G. Sapelli, Padova, 2019

MERENDA I., *La "ley del solo sí es sí": la controversa riforma dei delitti contro la libertà sessuale nell'ordinamento spagnolo. Spunti per il legislatore italiano?* Archivio Penale 2024, n.1

MERZAGORA I., 2019, Università degli studi di medicina legale di Milano, «*l'idealismo perverso per una giusta causa?*»

META, "Creating a dataset and a challenge for deepfakes", 2019

MICHELETTI D., *L'intervento di pubblicazione quale elemento costitutivo della fattispecie di Revenge porn*, e C. Paonessa, *Ai confini del c.d. Revenge porn. Tessere di un mosaico normativo* (18 marzo 2022).

MIHALCIK C., *Facebook gets about 500.000 reports of revenge porn a month, report says*, 18 novembre 2019

MILITELLO V., *Rischio e responsabilità penale*, Milano, 1988

MICROSOFT, "Ai for Good", 2021

MOCCIA S., *La perenne emergenza. Tendenze autoritarie nel sistema penale*, ESI, 2000

MONTALDO, "il ritratto fotografico digitale tra diritto d'autore, diritti della persona, e tutela della privacy" in *resp. civ. prev.* 2010, 11, 2369B s.

MOSCO E., FIANDACA G., *Diritto penale, parte generale*, Nona ed., 3 aprile 2024

MUSCATIELLO V.B., *Il cosiddetto stalking*, in *Scritti in memoria di Giuliano Marini*

NEW YORK POST, *By Post Editorial Board* pubblicato il 24 luglio 2019

NIEVA J., FENOLL, 2019, *Intelligenza artificiale e processo*,

OPEN, Intervista scritta da Fabio Giuffrida, 2021 "le mie foto date in pasto a 100 mila uomini su Telegram, questa è violenza"

New Generation Artificial Intelligence Development Plan (AIDP), China State Council, 2017

NEW YORK TIMES, James Bamford "the Agency that could be the big brother", Dicembre 2005

NOMOS, BADEN-BADEN, *Liability for Artificial Intelligence and the Internet of Things*, 2019

NOYB, la Redazione Noyb sollecita 11 DPA a fermare immediatamente l'abuso dei dati personali da parte di Meta per l'IA, 6 giugno 2024

ONG 2.0, *Rivoluzione digitale e sviluppo sostenibile, risorse e strumenti per comprendere le trasformazioni digitali e usare la tecnologia consapevolmente*, Digital transformation per lo sviluppo sostenibile, 2019

PACE A. – M. MANETTI, *Rapporti civili. Art. 21 – La libertà di manifestazione del proprio pensiero*, in BRANCA G. (a cura di), *Commentario della Costituzione*, Bologna: Zanichelli, 2006

PACILEO, 2022, "Proposals for a New Legal Framework on AI: Possible Discrepancies Between Liability, Compliance and Duties of Company Directors"

PADOVANI T., *L'assenza di coerenza mette a rischio la tenuta del sistema*, in *Guida dir.*, 2019

PAJNO A., M. BASSINI, G. DE GREGORIO, M. MACCHIA, F.P. PATTI, O. POLLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, *Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal*, 3/2019,

PALMIERI G.M., *L'accoglimento del concetto di "genere" come rischio di una tutela penale a binario differenziato, art 612ter e tutela della riservatezza*, 2022

PALMIRANI M., *Big Data e conoscenza*, in Riv. Filosofia del Diritto, 1/2020

PAN D., L. SUN, R. WANG, X. ZHANG, R. O. SINNOT, *Deepfake Detection through Deep Learning*, in *International Conference on Big Data Computing, Applications and Technologies*, 2020

PANATTONI, "Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online", in diritto penale contemporaneo 2/2019

PANATTONI, "I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace" in *Sistema Penale*, 2020

PARLAMENTO EUROPEO, *Risoluzione 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* (2015/2103(INL)).

PARLAMENTO EUROPEO, *risoluzione "Raccomandazioni alla Commissione su un regime di responsabilità civile per l'Intelligenza Artificiale"* del 20 ottobre 2020

PATRINI G., CAVALLI F., AJDER H., CULLEN L, *The State of Deepfakes: Landscape, Threats, and Impact*, September 2019.

PATRINI G. "Automating Image Abuse, Deepfakes Bots on Telegram", 2022

PECORELLA C., *Violenza di genere e sistema penale*, in *Dir. pen. proc.*, 2019

PELISSERO M., *Diritto Penale, Appunti di parte generale*, Giappichelli editore, 2021

PENTA A., *Il danno morale, Danno e Resp.*, 2017

PERINI C., *Il concetto di rischio nel diritto penale moderno*, Milano, 2010

PERMESSO NEGATO, Report "state of Revenge" 2022

PICOTTI L., *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993

PIERDONATI M., *La tutela delle persone vulnerabili con particolare riferimento all'analisi della legge 19 luglio 2019, n. 69 (c.d. 'codice rosso')*, in *La Giustizia Penale*, 2020

PIERGIALLINI C., *Il paradigma della colpa nell'età del rischio: prove di resistenza del tipo*, in Riv. it. dir. proc. pen., 2005, F. Herzog, *Società del rischio, diritto penale del rischio, regolazione del rischio*, in L. Stortoni – L. Foffani (a cura di)

PIERGIALLINI C., *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato*, 2020

PITTARO P., *Il c.d. "Codice rosso" sulla tutela delle vittime di violenza domestica e di genere, in Famiglia e diritto*, 2020

PIZZORUSO A., *Sul diritto alla riservatezza nella Costituzione italiana*, in *Prassi e Teoria*, 1976,

PNRR, 2021, testo disponibile sul sito del governo

POGGI F., *Violenza di genere e Convenzione di Istanbul: un'analisi concettuale*, in *Diritti umani e diritto internazionale*, 2017

POLLICINO O., DE GREGORIO G., PAOLUCCI F, F. BAVETTA, *Regolamento AI, la "terza via" europea lascia troppi nodi irrisolti: ecco quali*, in *agendadigitale.eu*, 21 maggio 2021

PORTALUPI-VILLASI, *Presente e futuro della violenza di genere. A che punto siamo dopo il codice rosso*, In *Diritto Penale e Uomo*, 2020

PRENCIPE A., SIDERI M, "Il visconte Cibernetico. Italo Calvino e il sogno dell'Intelligenza Artificiale", 12/2023

POPOVA M., *Reading out of context: pornographic deepfakes, celebrity and intimacy*, in *Porn Studies*, 7, 2020, 367 ss.; R. Winter, *DeepFakes: uncovering hardcore open source on GitHub*, in *Porn Studies*, 7, 2020

PUCCIARELLI M., “Caso Sarti, un ex deputato 5S: ‘Il furto delle foto da un pc in dotazione alla Camera’”, in “*la Repubblica*”, 20 marzo 2019.

PULITANO D., *Diritto penale*, ed. 2023

PUTMAN. H., “*Mind, Language and reality: philosophical papers*” Cambridge Mass, 1975

QUAIN J.R. “*Crime-predicting A.I. isn’t science fiction. It’s about to roll out in India*” Article June 2018

RAFFIOTTA E., *Quale autorità governerà l’Intelligenza Artificiale?* Il Sole 24Ore, 27 Marzo 2023

REDDIT, *Updates to Our Policy Around Impersonation*, 2020

RIGOTTI C., C. McGlynn, *Towards an Eu criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalize image-based sexual abuse*, in *New Journal of European Criminal Law*, 2022

RINALDI L., *Intelligenza artificiale, diritti e doveri nella Costituzione italiana*, in DPCE online, 1/2022

ROESSLER A., D. COZZOLINO, L. VERDOLIVA, C. RIESS, J. THIES, and M. Nießner, “*FaceForensics++: Learning to detect manipulated facial images*,” in *International Conference on Computer Vision (ICCV)*, 2019

ROMANO V.B., *L’introduzione dell’articolo 612-ter del Codice penale in materia di diffusione illecita di immagini o video sessualmente espliciti* (art. 10, l. 19 luglio 2019, n. 69), in *Codice Rosso. Commento alla L. 19 luglio 2019, n. 69, in materia di tutela delle vittime di violenza domestica e di genere*, B. Romano, A. Marandola (a cura di), Pisa, Pacini Giuridica, 2020

ROSANI D., *Il trattamento penalistico del sexting in considerazione dei diritti fondamentali del minore d’età*, *Diritto penale contemporaneo – Rivista trimestrale* 1, 9 (2019)

ROSEMBERG R., HADAR DANCIG-ROSEMBERG, *Journal of constitutional law: “Revenge Porn in the shadow of the First Amendment”*

ROSSETTI M., *Il danno da lesione della salute*, CEDAM, 2001

ROYLE S., *Deepfake porn images still give me nightmares*, 6 Gennaio 2021, BBC

RUVALCABA Y., A. A. Eaton, *Nonconsensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men, psychology of violence*

SALVADORI I., *Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale*, in *Riv. it. dir. proc. pen.*, 2021

SANTOSUOSSO A., *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Mondadori Università, Città di Castello, 2020

SARTOR G., *L’informatica giuridica e le tecnologie dell’informazione*, Giappichelli, Torino 2022;

SAVONA E. e CANAPPELE S., in “*Problem Solving e analisi criminale: guida all’uso*”, 2008

SAVONA E., “*Dal micro al macro e ritorno*”, *Rassegna Italiana di Criminologia*, n. 1, anno 2009

SCAFFIDI A., *Il principio di offensività e le forme di anticipazione della tutela giuridica*, in *Diritto.it*, 18.03.2021

SERVIZIO STUDI SENATO, settembre 2020 “statistiche sulla violenza di genere”

SCANLON T.P., GALLAGER S., *Carnegie Mellon University, Software engineering institute, SEI Deepfakes day, Deepfakes* 101, 2022

SCHELLER S.H., *A Picture Is Worth a Thousand Words: The Legal Implications of Revenge Porn*, in 93 NCL Rev. 551 (2015)

SCHOR E., *Lawmakers target ‘revenge porn’ in bipartisan bill*, Politico (Nov. 28, 2017)

SCHERER M.U., *Regulating Artificial Intelligence Systems: risks, challenges, competencies, and strategies*, in *Harvard Journal of Law and Technology*, Vol. 29, Number 2, 2016,

SCHULHOFER SJ, *Consent: What It Means and Why It’s Time to Require It*, in *University of the Pacific Law Review*, 2016

SEMINARA S., *Codice penale, riserva di codice e riforma dei delitti contro la persona*, in *Rivista italiana di diritto e procedura penale*, 2020

SEARLE J., *Intentionality. An Essay in the philosophy of Mind*, Cambridge Mass, 1983

SEMINARA S., *Delitti contro la libertà personale e morale*, in R. Bartoli, M. Pelissero, S. Seminara, *Diritto penale. Lineamenti di parte speciale*, Torino, Giappichelli, 2021

SERRA M., *Rapinatore seriale catturato grazie al software “Key crime”*, in *La stampa*, 2018

SERVENT A.R., “Protecting or Processing?”, in Aa.Vv., *Privacy, Data Protection and Cybersecurity in Europe*, a cura di W.J. Shünemann e M.O. Baumann, Cham, 2017

SIMONCINI A., *L’algoritmo incostituzionale, intelligenza artificiale e il futuro delle libertà* 2019

SORGATO A., *Revenge porn*, Giuffrè Francis Lefebvre Spa, Milano, 2020

SOLON O., *Social Media. Inside Facebook’s efforts to stop revenge porn before it spreads*, 18/19, Novembre 2019

SORGATO, *“Revenge porn. Aspetti giuridici, informatici e psicologici*, Milano, 2019

SPACCATINI, F. GRASSI, E. GIOVANNELLI, I., PAGLIARO S., & PACILLI MG, *se l’è cercata: il victim blaming nei confronti delle vittime di violenza di genere*.

SPINDLER G., *User liability and strict liability on the Internet of Things and for Robots*, in S. Lohsse e al. (eds)

STANZIONE P., “Segnalazione al Parlamento e al Governo sull’autorità per l’IA”, 2016

STANZIONE M.G., *Il regolamento europeo sulla privacy, origini e ambito di applicazione*, 2016

TABARELLI DE FATIS, “prospettive di riforma del delitto di diffamazione, con particolare riferimento alla diffamazione online”, in Picotti (a cura di) “*tutela penale della persona e nuove tecnologie*”, Padova, 2013, 220

TAMBORINI L., SIMICICH M., “*il Revenge porn ad un anno dall’entrata in vigore: prime considerazioni*”, ottobre 2020

TAULLI T., *Deepfake: what you need to know*, in *forbes.com*, 15 giugno 2019

THE GUARDIAN, Philip Oltermann, 22 maggio 2014

TOSONI L., *Intelligenza artificiale, i punti chiave del regolamento europeo*, 21 aprile 2021

TRAPANI M., *La divergenza tra il voluto e il realizzato*, 2006

TRIVILLINI A., *dichiarazioni in Corriere del Ticino*, Valentina Coda, 2021

QUAYLE, E. *Self-produced images, sexting, coercion and children’s rights*,. ERA Forum23, 237–251 (2022)

VALSECCHI A., “Codice rosso” e diritto penale sostanziale: le principali novità, in *Diritto penale e processo*, 2022

VENTUROLI "la vulnerabilità della vittima di reato quale categoria 'a geometria variabile' del diritto penale" in Riv. it. medicina legale 2018

VERONICA V., DI GIACOMO D., gennaio - febbraio 2022, vol. 57 n.1 *Riv Psichiatr.* 2022;57(1):10-17 "Implicazioni psicologiche del fenomeno del Revenge porn: prospettive cliniche"

VERZA A., *Aggredire attraverso l'immagine, Cristallizzazioni tecnologiche, genere e diniego di tutela nella logica disciplinante neoliberale*, in *Ragion pratica*, 2017, n. 2

VIGANO' F., *Il delitto di atti persecutori (art. 612-bis c.p.)*, in *I delitti contro la persona. Libertà personale, sessuale e morale. Domicilio e segreti*, a cura di C. Piergallini, F. Viganò, M. Vizzardi, A. Veri, in *Trattato di diritto penale. Parte speciale*, diretto da G. Marinucci, E. Dolcini, Cedam, 2015

WACHERS, MITTLESTADT e L. FLORIDI, *why a Right to Explanation of Automated Decision-making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law* 2017

Waldman A.E., *Law, Privacy, and Online Dating: "Revenge Porn"* in *Gay Online Communities*, in *L.S. Inquiry*, 44, 4, 2019

Washington post, 11/05/2015 "Anonymous's KKK 'leak' targets the elusive online world of white nationalism"

WESTERLUND M., "The Emergence of Deepfake Technology: A Review", *Technology Innovation Management Review*, November 2019 (Volume 9)

WIENER R., "Cybernetics or Control and Communication in the Animal and the Machine, Cambridge", 1948

ZANI F., *Il difficile bilanciamento fra tutela della libertà di manifestazione del pensiero e diritto alla riservatezza nell'era dei social network*, in *Osservatorio costituzionale*, 2014.

ZICCARDI G., *Odio online, Revenge porn e natura delle nuove tecnologie tra amplificazione, persistenza e viralità del messaggio dannoso*, in Sorgato A. (a cura di), *Revenge porn. Aspetti giuridici, informatici e psicologici*, Milano, Giuffrè, 2020

INDICE DELLA GIURISPRUDENZA

Corte EDU, sez. II, sent. 24 settembre 2013 ric n. 48898/99, Belpietro c. Italia
Dlgs 9.4.2003

Cass. Pen. Sez V 20.3.2019, n. 12546
Dlgs 70/2003

Cass. Civ., sez. I, Sent. 19/03/2019 n° 7708

Corte EDU, sez III, 7 agosto 2018, Causa C-521/17 cooperatieve Vereniging snb-react U.A. Contro. DM

Trib. Napoli, 8 agosto 1997 in *Diritto e giurisprudenza.*, 1997, 472, con nota di Catalano; Trib. Roma 22.03.1999

Trib. Roma, 22 marzo 1999, in *Diritto dell'informazione e informatica* 2000, 66 con nota di SAMMARCO, in *Rivista del diritto commerciale* 1999, II, 273 con nota di VISCONTI

US supreme Federal Court, Eastern District of Pennsylvania, 11 giugno 1996, in *Diritto dell'informazione e informatica*, 1996, 4/5, 604

Cass. Civ. Sez. V n 8180/2018;

Cass. Civ. Sez III n 8095/2006;
 Cass. Civ. Sez III n 1219/1997
 Cass. Pen. Sez III n 5107/2013
 Cass. Pen., Sez. III, 4 settembre 2023 (ud. 4 aprile 2023), n. 36572
 Cass. Pen. sez. V, 28 novembre 2012 n 18826 in *Danno e responsabilità*. 8/2023 nota di Mengoni
 Cass. Pen. Sez. V, 12 giugno 2018 n. 38911 in *Dir & Giust.* 2018
 Trib. La Spezia, sez. II, 4 ottobre 2018 n.331 G.i.p., in *de jure*
 Cass. Pen., Sez V, 25 settembre 2017, n. 55418
 Cass. Pen., Sez. II, 19 ottobre 2022 (ud. 1° luglio 2022) n. 39529
 Corte di Appello di Torino, febbraio 2023, in *Ius in Itinere*, valeria D'alessio, *Revenge porn: Caso Tavassi e Maestra di Torino*
 Cass. pen., sez. I, sent 12/09/2014 n° 37596
 Corte d'Appello USA, 11 settembre 1984, 736 F.2d 1084 (5th Cir. 1984), Wood vs Hustler Magazine
 Cass. Pen. Sent, Sez. V, n. 19201 del 15 maggio 2024
 Cass. pen. sez. IV, 27 novembre 2013 n 2347 in *Guida dir*, 2014, 10,72
 Corte di Appello di Napoli, 13.10.99 n.1636
 Cass. pen., sez. III, sentenza 21/07/2008 n° 30403
 Corte EDU, *J.L. c. Italia*, ricorso n. 5671/2016, sentenza 27 maggio 2021 (Prima Sezione)
 Corte di Appello di Firenze, sez. II Penale, n. 858, 4/03/2015
 Cass. Pen. sent. n. 20780/2019;
 Cass. Pen. Sent. n. 25727/2004
 Cass. Pen. sent. n. 2400/2018
 Cass. pen. sent. n. 17210/2011
 Cass. Pen. Sez. III, n.19599/2023
 Cass., Pen., sez. III, 21 marzo 2016, n. 11675
 Trib. di Napoli, n 9799/2016, II sez civile.
 Trib. di Napoli, sent. 8 novembre 2022, giudice Dario Gallo
 Legge n.71/2017 entrata in vigore 18/06/2017
 Trib. di Roma, 23 dicembre 2017, procedimento n. 39913/2015
 Trib. di Mantova, ricorso n. 2881/17, 19 settembre 2017
 Cass. Pen., sez. III, 8 settembre 2020, n. 25266
 Cass. Pen, sez. III, 16 giugno 1994, n. 8453;
 Cass. Pen., sez. III, 26 marzo 2013, n. 19033;
 Cass. Pen. sez. III, 30 ottobre 2018, n. 17509.
 Legge n.71, 29 maggio 2017
 Cass. Pen. S.U. n.51815/2018
 Cass. Pen, sez. V, sent. n. 57503 del 22 dicembre 2017 (ud. del 23 novembre c.a.)
 Cass. Pen. Sez III, 18 febbraio 2016, n 11675; in *Dir. & Giustizia*, 2016, 15,42 con nota di Alovisio, 2 maggio 2016, con nota di Ventura.
 Regolamento UE 2022/2065
 legge 3 agosto 1998, n. 269.
 Legge n. 176/91
 Direttiva n. 92/2011

Decisione quadro GAI n. 68/2004
 Considerando n. 10 reg. 679/2016
 Direttiva UE 1972/2018
 Legge 172/2012
 Cass. Pen. Sez III, 18 febbraio 2016, n 11675; in *Dir. & Giustizia*, 2016, 15,42 con nota di Alovisio, in *il penalista.it* 2 maggio 2016, con nota di Ventura.
 Cass. Pen. Sez III, 10 maggio 2018 n 39039 in *Guida dir.* 2018, 41,50
 Cass. Pen. Sez II, 12/10/2006 n. 34128 ud. 23/05/2006
 Cass. Pen n. 19659/2019;
 Cass. Pen., sez. 05, del 19/06/2008, n. 30664;
 Cass. pen. sez. V, 14/11/2016, n.4873
 Cass. Pen. Sez. V, n. 3963 del 06/07/2015, Rv. 265815
 Cass. Pen. sez. unica 21 gennaio 2015 n 31022 in *giur. cost.* 2015,3,1055 con nota di Diotallevi
 Cass. pen. Sez. V sent. n. 25875 del 25 luglio 2006
 Cass. Pen Sez. 5, n. 22787 del 30/04/2021, Rv. 281261;
 Cass. Pen. Sez. 5, n. 38099 del 29/05/2015, Rv. 264999
 Cass. Pen., sez.V, sent n. 854.2021
 Cass. Pen. sez. I n 2739/2010
 Trib. di Milano, sez IV penale, giudice monocratico, 3 ottobre 2017 n 9393
 Cass. pen. Sez. V sentenza n. 37383 del 17 ottobre 2011
 Cass. Pen., sez.V, n. 30455/2019
 Trib. di Milano, V sez. pen, giudice monocratico 8 novembre 2017 n 10945
 Trib. di Bari, sez. I, 5 marzo 2013 n 584 in "*de iure*"
 Cass. Pen. sez. III n 19659 in *CED* 2019;
 Cass. Pen sez V n 42130/2011
 Cass. Pen Sez. VI n 38571/2008 in *CED*
 Cass. Pen. rv. 241509-01
 Dlgs 101/2018
 Cass. Pen. sez III, n. 15221/2016
 Cass. Pen. Sez. III, 7 febbraio 2017, in *CED rivista* n. 270458
 Cass. Pen.III, sent. 8.10.2015, n. 40356
 Cass. pen., Sez. V, 10 luglio 2019, n. 30455
 Trib. di Milano sez. pen. V, giudice monocratico, 25 settembre 2017 n 8940
 D.l. n. 11/2009 convertito in legge n. 38/2009
 Cass. Pen. Sez V n 47049/2019
 Cass. Pnc. sex. V, n 61/2019
 Cass. Pen., Sez. V pen. 28/12/2017, n. 57764
 Cass. Pen. Sez V n 30535/2021;
 Cass. Pen. Sez V n 33842/2018
 Cass. Pen. Sez III, 6 novembre 2018 n 11450
 Cass. pen. Sez V n. 1813/2021
 Cass. Pen. Sez. V n. 25774/2014
 Cass. pen. sez. V, 23/04/2014, n.25774, in *Rivista penale* 2014, 9, 804, in *dejure*
 Trib. di Trento, 29/04/2014 n.369 in *dejure*
 Cass., Sez. III, 22 dicembre 2020, n. 36910, in *Dir. pen. e proc.*, 2021, 4, 427;

Cass., Sez. III, 2 luglio 2020, n. 25266, in *Diritto di Internet*, 2020, 4, con nota di PICOTTI
 Cass. pen. sez. III, 24/05/2023, (ud. 24/05/2023, dep. 13/10/2023), n.41573;
 Cass. pen. sez. IV, 05/11/2019, (ud. 05/11/2019, dep. 27/01/2020), n.3205;
 Cass. pen. sez. III, 11/10/2011, (ud. 11/10/2011, dep. 23/01/2012), n.2681
 Cass. Pen. sent n.11560 del 25.03.2010
 Legge n. 134/2021
 Ddl n 4055/2016 alla Camera dei deputati, Sandra Savino, 27 settembre 2016
 Ddl n.1134/2019
 Dlgs 21/2018
 Direttiva 29/2012 (GU L 315/57)
 Ddl 119/2013
 Cedu, sez I, Talpis c. Italia, 2/03/2017
 Considerando n. 9 della direttiva 2012/29/UE
 Legge n.77/2013
 Dlgs 212/2016
 Raccomandazione R (2006)8 del Consiglio D'Europa, punto 3.4
 Cass.Pen. Sez. II, 29 novembre 2012 n 48738
 Corte di Appello di Roma sez. III 4 luglio 2014
 Cass. Pen. n 21394/2016 sez. V;
 Cass. Pen sez. V n 27564/2020
 Legge 69/2019
 Sent. *Uberschar*, 8 ottobre 1980, causa 810/79
 Cass. Pen. n. 29577/21
 Cass.Pen. sez III 14 novembre 2017 n 14707 in CED Cass Pen rv 239659
 Cass. Pen., Sez. Un., 28 febbraio 2013 (dep. 13 giugno 2013), n. 25939, Pres. Lupo, Est. Cassano, Imp. C.
 Cass. Pen. Sez I n 12680/2008 in Cass. Pen. 2009,1,200
 Cass. Pen., IV sez., 13 novembre 2003, n. 3449
 Cass. Pen sez. III n 1647/2018 in *Dir & Giustizia*. 2019
 Cass. Pen sez. III n. 30564/2011 in CED Rv. 251260
 Convenzione di Budapest, legge n.48/2008
 Corte Cost. n. 172/2014
 Ddl 1076/2019
 Cass. Pen, sez III, 8 gennaio 2020, n. 9354
 Cass. Pen sez. III, n 7504 del 2014;
 Tribunale di Roma, 27 ottobre 2011 in *Guida Dir.* 2012
 Cass. Pen. Sez. III, n 15221/2016
 Cass. Pen. Sez V n 30334/2016 in *Dir&giust.* 18 luglio
 Cass. Pen. Sez III n 11920/2018
 Tribunale di Oristano, 25 maggio 2000 in *riv. it. dir. e proc. pen.* 2001, 1405 con nota Scopinaro
 Tribunale di milano, sez. IX penale, n 13365 14 dicembre 2016
 Legge 104/1992
 Cass. Pen, sez. III, sentenza del 21 novembre 2019, n. 5522
 Cass. pen., Sez. III, 21.3.2016, n. 116755
 Cass. Pen sez I n 4322/1997

Cass. Pen. N 15/1997 in *riv. pen.* 1998 n 251
 Cass. Pen., Sez. IV, n. 21527, 21.01.2015
 Corte Cost. N 394/2006
 Cass. Pen. Sez.V n 17756/2008
 Cass. Sez. III, 30 novembre 2005 (dep. 29 dicembre 2005) n. 47247, CED 233016;
 Cass. Sez.III, 9 luglio 1996 (dep. 8 agosto 1996) n. 3014, CED 206061
 Cass. Sez.III, 17 novembre 2005 (dep. 10 gennaio 2006) n. 307, CED 233284
 Cass. pen., Sez. V, sent. n. 14927 (ud. 22 febbraio 2023, dep. 7 aprile 2023), rel. Brancaccio
 CGUE, 7.2.2012, Von Hannover c. Germania; CGUE, 4.12.2015, Zakharov v. Russia.
 Trib. Reggio Emilia, sezione GIP/GUP, sentenza del 22 novembre 2021, n. 528
 Corte Cost. Sent. n. 38/73
 Cass. Pen. n. 161 del 1985
 Corte cost., 4 febbraio 1965, n.9
 Cass. Civ, Sez. I, n. 91437/2020
 Corte di Giustizia UE 13 Maggio 2014 n. 317
 Cass. Ordin. N. 7559/2020
 GDPR, provvedimento 5 agosto 2022, n. 9811771, reg dei provv. n. 283 del 5 agosto 2022
 Legge 71/2017
 Provv. n 204/2023, 17 maggio 2023, Garante della Privacy, doc. n. 9903127
 Cass. Pen. n. 1748/2016
 Corte di Cassazione n. 8177/1994
 Corte Cost. n.184/2006
 Dlgs 209/2005
 Cass.n. 14846/2007
 T.A.R. Roma, Sez. I, 15/10/2018, n.9984
 Cass. n. 7471/2012,
 Cass. 10527/2011,
 Cass. 20558/2014,
 Cass. n. 13614/2011
 Cass. Civ., sez. I, 16/04/2018, n. 9385/2018
 CEDU Volodina c. Russia, 9 luglio 2019, e Volodina c. Russia (n. 2), 14 settembre 2021
 Cass. Pen. Sez V 43085/2015 A. Rv 265231
 Cass. Pen. Sez. V, sent. n. 654/2023
 Tribunale di Siena, sezione penale in composizione monocratica, 18 dicembre 2023 n.771
 Trib. Federale, n. 117/2024, procedimenti riuniti 001-002/2023
 Enhancing online safety act *Federal Register of Legislation ; Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992*, in *communications.gov.au*, 15.2.2020
 Republic Act n. 9995/2009, anti photo and video voyeurism act
 Parlamento Europeo e Consiglio Europeo, Strasburgo, 8.3.2022 COM(2022) 105 final 2022/0066 (COD)
 Caso n 1. 41261/2017 decisione finale nel 2019; caso n 2. 40419/2019, Volodina vs Russia
 Ric. n. 56867/15, 11 febbraio 2020, Buturva vs Romania
 Snyder v. Phelps, 562 U.S. 443, 458 (2011)
 Del. Code Ann. tit. 11, § 1335(a)(9) (2017); S.D. Codified laws § 22-21-4 (2021)

NY Crim. Court, *People v. Barber*, 42 Misc.3d 1225(A) Feb 2014
 New Jersey Statutes Title 2C. The New Jersey Code of Criminal Justice 2C § 14-9 Amended by L.2016, c. 2, § 1, eff. May 5, 2016
 Trib. distrettuale superiore di Colbenza, 20 Maggio 2014 (Az 3 U 1288/13), terzo senato civile
 Corte Suprema n 699/2022, 11 luglio
 Loomis, 881 N.W.2d, 749 (Wis 2016) par. 99
 Cons. Stato, sent. n. 2270/2019, V. TAR Lazio Roma, n. 3769/2017
 Parlamento europeo, Risoluzione del 16 febbraio 2017, 2015/2103(INL)
Commissione Europea, communication from the commission, "Artificial Intellingence for Europe", 25.04.2018, 237 final. COM (2018) 795 final.
 24.1.2024 COM(2024) 28 final, Brussels
 Regolamento (UE) 2024/1689, Parlamento EU e Consiglio EU, 13 giugno 2024
 Regolamento (CE) n, 300/2008
 Regolamento (UE) n, 167/2013
 Regolamento (UE) n, 168/2013
 Regolamento (UE) 2018/858
 Regolamento (UE) 2018/1139
 Regolamento (UE) 2019/2144
 Direttiva 2014/90/UE
 Direttiva (UE) 2016/797
 Direttiva (UE) 2020/1828
 Risoluzione del Parlamento Europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla Robotica, C 252/239, Gazzetta Ufficiale Unione Europea
 Commission Decision, Brussels, 24.1.2024 C(2024) 390 final
 Considerando 27 della proposta di regolamento 2024/1689
 Real Decreto 729/2023, 22 agosto. «BOE» núm. 210, de 2 de septiembre de 2023, páginas 122289 a 122316 (28 págs.) Disposiciones generales, Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática, BOE-A-2023-1891
 Dichiarazione Europea sui diritti e i principi digitali per il decennio digitale (2002) 208, approvato nel gennaio 2022
 Proposta di Regolamento UE sull'Intelligenza Artificiale COM 2021 (206), Camera dei deputati, 9 marzo 2022
 European Commission, Inception impact Assessment, Ref. Ares(2021)4266516 - 30/06/2021
 Direttiva 2006/123/CE Parlamento europeo, Consiglio europeo, 12 dicembre 2006, GU L 376 del 27.12.2006, pag. 36
 Direttiva 2000/31/CE Parlamento Europeo e del Consiglio, 8 giugno 2000
 risoluzione n. P9_TA (2021)0405, ottobre 2021, Parlamento Europeo
 Dlgs n 139/2021
 CGUE, grande sezione, 16 luglio 2020; CGUE 311/16
 Proposta di Regolamento del Parlamento Europeo e del Consiglio, Bruxelles, 15.12.2020 COM (2020) 825 final 2020/0361 (COD)
 Cass. Pen. N.25774/2014
 legge n. 119/2013

California Government Code, Section 11547.5; State of Texas, Chapter 21, Penal Code, Section 21.165
“No Ai found Act”, H.R. 6943, 118th Congress, 2023/2024
State of California, Assembly Bill n. 602, sezione 1, punto 14
Sent. Cass. Pen., Sez. III n. 22265, 13 gennaio 2017
Sent. Cass. Pen., Sez. III n. 15757, 9 aprile 2018
Legge n. 633/41
Cass. Pen. III Sez., n. 11675/16, Rv 266319
Deepfake Accountability Act, 09/20/2023, HR 5586, 118th Congress, Referred to the Subcommittee on Emergency Management and Technology.
Regolamento n. 1689/2024
Corte cost. 3 febbraio 1994, n. 13
Direttiva 680/2016, inserita con dlgs 18 maggio 2018 n.51
Reg. n. 2120/2015
Cass. Pen. Sez. III, n. 28524 57 del 9/06/2009
Cass. Pen. Sez. III, n. 25232 del 21/06/2005, P.M. in proc. Brancato, Rv. 231814
Cass. Pen. Sez. I, n. 47086/2018; Cass. Pen. Sez. III, n. 8296 del 2/12/2004
Cass. Pen. Sez. III, n. 41231 del 17/01/2018