



VIOLENZA VIRTUALE, DANNO REALE: ANALISI GIURIDICA DEI DEEPFAKE SESSUALMENTE ESPLICITI

Negli ultimi anni, la diffusione delle tecnologie di intelligenza artificiale ha reso sempre più facile la creazione di contenuti deepfake, ossia video o immagini manipolati digitalmente tramite tecniche di intelligenza artificiale, con l'intento di far apparire persone in situazioni che non hanno mai vissuto realmente. La creazione e la diffusione di deepfake sessualmente espliciti sollevano gravi preoccupazioni in merito alla tutela dei diritti delle persone coinvolte. Il presente contributo si propone di analizzare il fenomeno dei deepfake sessualmente espliciti sotto il profilo storico e tecnico, al fine di comprendere le implicazioni giuridiche e sociali del loro utilizzo dannoso, per poi esaminare i beni giuridici potenzialmente lesi.

di Italo Guagliano

IUS/17 - DIRITTO PENALE

Estratto dal n. 4/2025 - ISSN 2532-9871

Direttore responsabile

Alessio Giaquinto

Publicato, Mercoledì 16 Aprile 2025



Abstract ENG

In recent years, the proliferation of artificial intelligence technologies has increasingly facilitated the creation of artificial content. Among these, sexually explicit deepfakes raise significant concerns regarding the protection of the rights of the individuals involved. This contribution aims to analyze the phenomenon of sexually explicit deepfakes from both a historical and technical perspective, in order to understand the legal and social implications arising from their use.

Sommario: 1. I deepfake sessualmente espliciti: una nuova minaccia dal mondo digitale; 2. Il background tecnico dei contenuti deepfake; 3. Il bene giuridico leso dalla diffusione di deepfake sessualmente espliciti: premessa; 4. La libertà sessuale nell'era digitale; 5. Il primo contatto del legislatore con i deepfake: l'art. 600-quater.1 c.p.; 6. I danni derivanti dalla diffusione di deepfake sessualmente espliciti: gli embodied harm; 7. La libertà sessuale quale bene giuridico leso dalla diffusione di deepfake sessualmente espliciti; 8. Considerazioni conclusive.

1. I deepfake sessualmente espliciti: una nuova minaccia dal mondo digitale

Siamo sommersi quotidianamente, sia nel mondo reale che in quello virtuale, da un'incessante mole di informazioni, notizie, immagini e video, sia veri che falsi. La legislazione non è stata in grado di tenere il passo con i problemi che derivano dalla difficoltà di distinguere la realtà dalla finzione. Negli ultimi anni, dalle oscure pieghe di internet è emerso un nuovo fenomeno: immagini e video pornografici manipolati che mostrano il volto di una persona applicato in modo credibile su un corpo impegnato in atti sessualmente espliciti; un fenomeno che autori^[1], commentatori^[2] e accademici^[3] chiamano deepfake sessualmente espliciti^[4]. Anche se le immagini sono artificiali, essendo create utilizzando la tecnologia assistita dall'intelligenza artificiale^[5], vengono divulgate come immagini vere delle persone rappresentate. La tecnologia deepfake si è evoluta così rapidamente che ad oggi è possibile rinvenire numerose piattaforme online progettate appositamente per la creazione di questi contenuti.

Tali piattaforme riducono la soglia tecnica richiesta per creare tali immagini e video, il che renderà probabilmente sempre più frequente la diffusione di contenuti sessualmente espliciti creati artificialmente con il volto di personaggi pubblici e privati ignari. Ad oggi, chiunque sia apparso in un'immagine digitale può essere protagonista di contenuti sessualmente espliciti contro la propria volontà e, attualmente la legislazione non fornisce alcun rimedio chiaro o diretto per fermare questa pratica.

Con l'avanzare della tecnologia deepfake e la sua crescente facilità di realizzazione, le insufficienze della legge nel proteggere le potenziali vittime sono diventate evidenti. Al fine di comprendere la gravità del fenomeno e la necessità di una risposta chiara da parte del legislatore, consideriamo il seguente scenario ipotetico: Tizio e Caia sono in una relazione a lungo termine. Tizio è appassionato di fotografia digitale e ovunque lui e Caia vadano - passeggiando per le strade di Milano, visitando il porto di Genova o facendo un picnic nel giardino della loro casa - Tizio scatta foto di Caia con il suo smartphone. Caia acconsente alla realizzazione di queste immagini ma non ha mai permesso a Tizio di scattare fotografie che la ritraggano nuda o in contesti sessualmente espliciti.

Al termine della loro relazione, Tizio carica tutte le sue immagini digitali di Caia su un'app sul suo smartphone che gli consente di sovrapporre il volto di Caia sul video del corpo di un'attrice pornografica impegnata in atti sessuali espliciti. Tizio carica quindi il video deepfake, insieme alle informazioni di contatto di Caia, su vari siti di social media online. La storia di Caia riflette il nuovo ed emergente fenomeno dei deepfake aventi ad oggetto contenuti sessualmente espliciti, la cui comprensione deve essere posta alla base di qualsiasi soluzione giuridica. Il presente lavoro si pone l'obiettivo di definire e spiegare il fenomeno dei contenuti deepfake, analizzando i rischi legati alla diffusione di tale tecnologia, approfondendo in particolare il problema legato alla diffusione di contenuti deepfake sessualmente espliciti e le possibili soluzioni giuridiche adottabili. A tal fine, la disamina non può che partire dalla conoscenza del fenomeno, in termini storici e tecnici. La tecnologia alla base della creazione di contenuti deepfake è definibile come l'insieme delle tecniche utilizzate al fine di realizzare video e immagini che sembrano reali ma che, in realtà, sono stati ottenuti attraverso l'utilizzo di sistemi basati sull'intelligenza artificiale: essa implica la sostituzione del volto di una persona con il volto di un'altra – c.d. faceswapping – in maniera tale da simulare la presenza della persona rappresentata in contesti fittizi^[6]. L'output ottenibile attraverso tali tecniche è un video o un'immagine che intende rappresentare realisticamente^[7] un soggetto scelto.

La tecnologia deepfake utilizza la tecnica di intelligenza artificiale nota come deep learning^[8] per identificare e scambiare volti in foto e video: essa analizza una grande quantità di immagini o registrazioni con il volto di qualcuno, addestra un algoritmo di A.I. per manipolarle e quindi utilizza quell'algoritmo per mappare il volto su un'altra persona in un altro video. Sebbene questa tecnica possa avere usi legittimi, ad esempio nel campo dell'intrattenimento satirico o nel settore artistico, un utilizzo distorto della stessa può potenzialmente arrecare gravi danni alle persone rappresentate: come detto in apertura, si pensi al caso di un contenuto deepfake attraverso il quale venga rappresentata la presenza di una persona in un video sessualmente esplicito, alla cui creazione consegua la diffusione sulle piattaforma di social media online.

La diffusione di video così prodotti può comportare rilevanti danni alla reputazione, alla

dignità e alla libertà sessuale^[9] della persona ritratta: i deepfake sessualmente espliciti aggiungono un nuovo livello di complessità a ciò che potrebbe essere utilizzato per danneggiare le persone online. Il livello di rischio è particolarmente alto, anche alla luce della facilità con la quale questo genere di contenuti si è diffuso ed è diventato, oggi, di semplice accesso anche in assenza di specifiche competenze.

I contenuti deepfake, infatti, sono emersi su Internet per la prima volta nel 2017, quando un utente anonimo del social network Reddit^[10] caricò per la prima volta alcuni contenuti video creati artificialmente raffiguranti alcuni attori impegnati in attività sessualmente esplicite. A seguito della pubblicazione dei predetti contenuti, un altro utente del social network citato creò FakeApp, un'applicazione disponibile per tutti gli smartphone, in grado di permettere a tutti gli utenti di creare contenuti deepfake in assenza di competenze tecniche^[11]. Prima dell'avvento di FakeApp, la produzione di contenuti video artificialmente realizzati rappresentava un'operazione costosa e accessibile solo agli utenti esperti. La creazione di FakeApp ha reso la realizzazione di contenuti deepfake possibile per chiunque^[12].

Tale applicazione, infatti, funziona attraverso il caricamento di immagini digitali ritraenti una persona all'interno di un algoritmo di machine learning, addestrato al fine di imprimere le caratteristiche del viso della persona in un video, e di sostituire il soggetto inizialmente ripreso con quello di cui sono state prodotte le immagini: in assenza di competenze tecniche, l'unico requisito richiesto per la realizzazione dei contenuti deepfake è rappresentato da uno smartphone o da un computer.^[13] Inoltre, essendo le immagini dei cittadini comuni sempre più facili da reperire attraverso i siti dei social media, come Facebook e Instagram, la creazione di contenuti deepfake sessualmente espliciti ha iniziato ad influenzare non solo le personalità pubbliche ma anche i privati: un numero crescente di deepfake ha ad oggetto persone lontane dalle luci dei riflettori. Il risultato è un nuovo e preoccupante fenomeno attraverso cui soggetti ignari possono essere posti al centro di contenuti video sessualmente espliciti artificialmente realizzati: secondo l'ultimo report effettuato da Deeptrace^[14] nel 2019, tra tutte le tipologie di video realizzati attraverso la tecnologia deepfake, il 96% è rappresentato da contenuti di carattere pornografico^[15].

Data la predominanza di deepfake a carattere pornografico^[16] e le potenzialità dannose relative alla produzione e alla diffusione di questi contenuti, il focus del presente lavoro sarà proprio questa tipologia di materiale digitale che, in virtù della sua natura altamente realistica, rischia di renderlo il veicolo ideale per la realizzazione di una nuova tipologia di offesa ai diritti inviolabili degli individui: i deepfake sessualmente espliciti sono infatti in grado di realizzare nuove forme di vergogna sociale^[17], solo parzialmente sovrapponibili a quelle realizzate dal fenomeno del c.d. revenge porn^[18], che vanno al di là dei confini geografici, a velocità enormi e con una platea di soggetti potenzialmente

infinita.

2. Il background tecnico dei contenuti deepfake

L'analisi delle potenziali conseguenze dannose legate alla creazione e alla diffusione di contenuti deepfake, nonché il tentativo di immaginare una possibile risposta del legislatore ai rischi legati al fenomeno in oggetto, non può prescindere da una – seppur succinta – analisi del contesto tecnico alla base della creazione di questa tipologia di media artificialmente realizzati e su come lo stesso possa essere utilizzato per la creazione di contenuti sessualmente espliciti. La creazione di contenuti deepfake, come a breve si dirà, rappresenta una specifica applicazione del machine learning^[19], un sistema di A.I. focalizzato sullo sviluppo di algoritmi che si perfeziona attraverso l'elaborazione di grandi quantità di dati, la cui analisi, quindi, rappresenta un antecedente logico necessario utile a comprendere come lo stesso possa essere utilizzato per la creazione dei contenuti oggetto del presente lavoro. Per capire il funzionamento del machine learning, occorre distinguere due elementi caratterizzanti il concetto di intelligenza artificiale: l'autonomia e l'auto apprendimento.^[20]

L'autonomia è la capacità dell'A.I. di prendere decisioni e agire in modo indipendente, senza controllo o influenza esterna, e dipende dalla complessità del rapporto tra la macchina e l'ambiente. L'auto-apprendimento, invece, è la capacità di apprendere dall'esperienza, con l'utilizzo di tecniche di apprendimento come l'apprendimento automatico, il ragionamento meccanico e la robotica^[21].

Alla luce di questi due aspetti è possibile individuare due categorie di intelligenza artificiale: quella ristretta, utilizzata per compiti specifici, e quella generale, in grado di adattarsi in modo autonomo e risolvere qualsiasi compito. Possono essere individuati due approcci distinti per l'intelligenza artificiale: il ragionamento logico, che si basa su una visione "top-down" del problema e consente di descrivere precisamente un contesto specifico, ma che richiede alla macchina di conoscere molte regole e di essere allenata su numerosi casi, risultando così poco adatto in contesti più complessi; e l'apprendimento automatico, che adotta un approccio "bottom-up", partendo dai dati disponibili per comprendere l'ambiente circostante e agire in modo coerente^[22]. L'apprendimento automatico, a cui è riconducibile la creazione di contenuti deepfake, in particolare, consente ai sistemi di migliorare le proprie prestazioni imparando automaticamente dall'esperienza, costruendo un proprio modello a partire dall'analisi dei dati^[23].

I dati forniti vengono analizzati tramite algoritmi specifici, e il modello generato viene utilizzato per fare previsioni e valutazioni sui nuovi casi. L'Auto Machine Learning, utilizzato dalle reti neurali per la creazione di contenuti deepfake, rappresenta un'ulteriore

evoluzione dell'intelligenza artificiale, che consente la codifica automatica di nuove informazioni nella banca dati, permettendo ai sistemi di problem solving di affrontare situazioni complesse in modo autonomo e raccogliendo dati non precedentemente forniti dal programmatore o elaborati dal modello di apprendimento iniziale^[24]. In tal modo, viene a crearsi un modello in grado di elaborare soluzioni innovative e autonome dalle conoscenze del programmatore.

Come si evidenzierà a breve, i sistemi di A.I. utilizzati per la creazione di contenuti deepfake prescindono dalla capacità dell'utente di realizzare autonomamente il contenuto, un aspetto che ne amplifica potenzialmente la diffusione. Il programma di A.I. dotato di algoritmi di machine learning è in grado di apprendere dall'ambiente circostante, utilizzando dati che elabora e memorizza, e di modificare le sue prestazioni per adattarsi alle conseguenze dell'apprendimento. In altre parole, il sistema è in grado di imparare in modo autonomo attraverso l'esperienza e di migliorare le sue prestazioni sulla base di ciò che ha imparato.

Questa tecnologia non richiede una programmazione predefinita, ma permette alle macchine di migliorare costantemente grazie all'esperienza. La comprensione della tecnologia alla base della creazione dei contenuti deepfake si completa poi attraverso l'analisi del concetto di deep learning, da cui gli stessi prendono il nome. Il deep learning è un tipo di rete neurale artificiale molto profonda, addestrata utilizzando il metodo del back-propagation^[25]: la rete neurale è composta da diversi strati che includono un livello di input, uno o più layer nascosti e uno di output.

Ogni strato è costituito da nodi che rappresentano i neuroni di un cervello umano e il lavoro di ciascuno strato è di ricevere, elaborare e trasmettere informazioni agli strati successivi. La rete neurale è adattiva, il che significa che può modificare la sua struttura grazie all'esperienza accumulata tramite tentativi ed errori. In particolare, tale metodologia di apprendimento sfrutta gli errori commessi precedentemente dal sistema correggendoli: ogni volta che la macchina commette un errore, utilizza algoritmi di back-propagation per rivedere le sue connessioni e migliorare l'output finale.

In sostanza, il deep learning è un metodo di apprendimento automatico particolarmente sofisticato che consente alle macchine di migliorare continuamente le proprie prestazioni attraverso l'esperienza e l'adattamento. Ricostruito in questi termini il background tecnico, può essere ora analizzato come lo stesso venga sfruttato per la creazione di contenuti deepfake.

La creazione di deepfake si basa su due sistemi di intelligenza artificiale ad apprendimento automatico che agiscono in “competizione” fra di loro: le reti generative

avversarie (d'ora in poi GAN - generative adversarial network)^[26]. Le reti neurali, come visto, funzionano in modo simile al cervello umano poiché in grado di elaborare informazioni in modo più veloce e preciso man mano che vengono esposti e apprendono un numero crescente di informazioni.

Come noto, infatti, più il cervello umano è esposto a determinate azioni o informazioni, come calciare un pallone o imparare il testo di una nuova canzone, più velocemente e accuratamente è in grado di replicarle.

Le reti neurali adoperate per la creazione di contenuti deepfake, utilizzano lo stesso concetto: prendono i dati e li dividono in piccoli pezzi (bite), quindi analizzano i rapporti tra quei pezzi per capire di cosa si tratta^[27].

Per fare un esempio, attraverso le reti neurali, il computer sul quale è stato installato il sistema di intelligenza artificiale analizza due foto di cani e rileva che si tratta di animali diversi, ma entrambi cani. Successivamente, memorizza la 'formula' matematica dell'idea di un cane, cioè le caratteristiche comuni alle due immagini: quattro zampe, orecchie triangolari, una forma simile a un muso, una coda e un manto peloso. In questo modo, il sistema è in grado di replicare queste caratteristiche in un nuovo contenuto, laddove richiesto dall'utente finale.

Tuttavia, le prima rete neurale, detta "generatore", rappresenta solo metà del percorso e senza la seconda rete, detta "discriminatore", i deepfake non sarebbero così realistici. I GAN sono quindi la combinazione di due reti neurali in ruoli contrapposti: la prima rete neurale crea il video o l'audio falsificato cercando di replicare l'insieme di dati che le viene fornito, come le immagini della persona ritratta^[28].

Successivamente, sia l'insieme di dati originale che il deepfake appena creato vengono inseriti in una seconda rete neurale che seleziona quali video dell'insieme di dati forniti sono reali.

Quando il discriminatore è in grado di riconoscere il deepfake, il generatore può 'imparare' come il discriminatore ha determinato la falsità e correggere eventuali errori; capisce le differenze tra il video reale e il tentativo di falsificazione precedente per migliorare le sue prestazioni e riprodurre un video o un audio più vicino all'originale dell'insieme di dati.

Per tornare all'esempio precedente, la rete neurale generatore prende la "formula del cane" e la applica per creare ciò che pensa sia la risposta per "cane", basandosi su tutti i cani che

il suo creatore gli ha mostrato in passato. La seconda rete neurale è stata anch'essa addestrata su immagini di cani reali: determina, quindi, se ciò che vede è un cane reale, secondo la sua comprensione, o no.

Per creare contenuti deepfake sessualmente espliciti, i GAN vengono alimentati con dataset contenenti video, immagini esplicite a sfondo sessuale o registrazioni vocali. Inoltre, ai GAN vengono forniti dataset con immagini, video o registrazioni vocali della persona che sarà riprodotta nel video o nella registrazione. Più dati di una persona vengono esposti alla rete neurale, più precisamente essa è in grado di riprodurre i gesti, i suoni e le espressioni facciali durante la creazione di un video deepfake. Ad esempio, se una raccolta di immagini digitali di un soggetto venisse fornita alla rete neurale, essa sarebbe in grado di generare un'immagine del medesimo soggetto, sostanzialmente indistinguibile dalle immagini reali precedentemente fornite.^[29]

Le reti neurali utilizzate per la creazione di deepfake, inoltre, non operano esclusivamente all'interno di categorie predefinite: una volta che le caratteristiche morfologiche del viso di un soggetto sono state apprese dal modello di intelligenza artificiale, quest'ultimo è in grado di combinare, ritagliare e adattare tali caratteristiche all'interno di un video in cui il soggetto appare in una scena sessuale. Quindi, il fatto che non esistano immagini o video pornografici reali del soggetto non rappresenta un ostacolo per i sistemi generatori di deepfake laddove agli stessi venga richiesto di crearli^[30].

Questo complesso meccanismo è oggi alla portata di tutti, grazie a piattaforme online che, in assenza di competenze tecniche, permettono a chiunque possieda uno smartphone di generare contenuti deepfake^[31]. La comprensione del fenomeno appena descritto e la rapidità della sua diffusione evidenziano la necessità che il legislatore adotti una normativa in grado di contrastare i rischi legati all'utilizzo diffuso degli strumenti per la creazione di contenuti deepfake, la cui realizzazione non può prescindere dall'analisi dei beni potenzialmente lesi dalla loro creazione e, soprattutto, dalla loro divulgazione.

3. Il bene giuridico leso dalla diffusione di deepfake sessualmente espliciti: premessa

L'analisi dei beni giuridici potenzialmente lesi dalla diffusione di contenuti deepfake sessualmente espliciti affonda le sue radici nell'evoluzione della categoria delle offese contro la libertà sessuale. Abbandonando l'obsoleta visione pubblica delle offese alla sfera sessuale, che le qualificava come danni alle regole sociali, è ormai un assunto indiscusso che queste violazioni abbiano una natura esclusivamente personale^[32], intaccando la sfera intima legata all'espressione della libertà sessuale, una dimensione di estrema riservatezza personale, alla quale il diritto penale dovrebbe avvicinarsi con cautela e precisione^[33]. Il contesto diventa ancora più complesso se analizziamo queste violazioni nell'era digitale,

in cui le tecnologie dell'informazione e della comunicazione hanno assunto un ruolo centrale nelle esperienze individuali, incluse quelle sessuali. In questo scenario, è fondamentale considerare come l'uso erotico del corpo sia cambiato nel corso del tempo.

Per comprendere meglio la natura dell'offesa derivante dalla diffusione di contenuti deepfake sessualmente espliciti, appare opportuno esaminare gli studi criminologici e sociali che offrono un approccio concettuale alla questione, tenendo conto della dimensione sociale e tecnologica in cui tali condotte possono verificarsi e che, nell'ultimo decennio, hanno analizzato le conseguenze fisiche e psichiche sulle vittime di abusi digitali. Tra gli studi criminologici più rilevanti vi è la cosiddetta teoria del digital embodiment^[34], che si basa sull'analisi critica del corpo come oggetto delle dinamiche di potere nella vita digitale^[35]. La teoria del digital embodiment si concentra sull'idea che le esperienze digitali non siano separate da quelle fisiche, ma piuttosto che ne costituiscano un'estensione. In altre parole, ciò che accade nel mondo digitale ha un impatto diretto e tangibile sulla vite delle persone e sui loro corpi. Questa teoria sfida il dualismo mente-corpo di origine cartesiana, suggerendo che le esperienze digitali siano forme di 'incarnazione' in cui la persona e il suo corpo sono attivamente coinvolti.

Il superamento del dualismo mente-corpo trasforma il corpo in esperienza, che può quindi essere violata anche in assenza di atti che lo coinvolgano nella sua integrità materiale^[36]. Tale teoria, suggerendo l'impossibilità di distinguere il reale dal virtuale, ci permette di comprendere come anche le immagini, sebbene artificialmente create come nel caso dei deepfake, possano avere rilevanti conseguenze sul benessere psico-fisico delle persone coinvolte, superando così la concezione secondo cui ciò che avviene online sia distinto da quanto avviene offline^[37]. Come si avrà modo di analizzare a breve, le condotte di cui ci si sta occupando, sebbene realizzate online, sono in grado di produrre danni tangibili quanto altre forme di aggressione che si verificano al di fuori della dimensione digitale. Il risultato di tale teoria è rappresentato dalla creazione della categoria del c.d. "danno sessuale tecno-sociale", attraverso la quale si evidenzia che i casi di violenza online non sono diversi, in termini di danno percepito dalle vittime, rispetto alle violenze subite nella realtà fisica^[38].

L'approccio vittimologico alla materia, suggerito dalla teoria in analisi, e che come noto rappresenta una delle spinte che portarono alla riforma dei reati sessuali del 1996^[39], ci permette di evidenziare come i beni giuridici immateriali siano legati alle percezioni e alle esperienze soggettive che le vittime hanno del danno.

L'analisi delle condotte connesse ai contenuti deepfake rende evidente come, sebbene la giurisprudenza abbia seguito l'evoluzione socioculturale nel campo dei reati sessuali, si sia ormai verificata una frizione con il perimetro di stretta legalità delineato dall'apparato

normativo vigente, che rende necessario aggiornare e adeguare la legislazione alla realtà sociale e tecnologica in cambiamento, attraverso una più organica analisi della criminalità sessuale legata alla sfera digitale. L'analisi delle condotte offensive mostra l'inadeguatezza dell'attuale panorama normativo nel tutelare i soggetti da condotte che, sebbene realizzate online, in assenza quindi di un coinvolgimento del corpo nella sua dimensione materiale, siano in grado di produrre effetti dannosi del tutto assimilabili a quelli delle condotte realizzate nella realtà materiale.

In tal senso, al fine di evidenziare come l'attuale quadro normativo dia rilevanza in tema di reati sessuali esclusivamente alla violazione della corporeità intesa come oggetto materiale offeso dalla condotta anti-giuridica, appare opportuno, prima di analizzare i danni derivanti dalle condotte connesse ai deepfake sessualmente espliciti, volgere il nostro sguardo verso l'intero apparato normativo di tutela della sfera sessuale, per evidenziarne i limiti alla luce dell'approccio vittimologico proposto dalla teoria dell'incarnazione digitale.

4. La libertà sessuale nell'era digitale

A seguito della riforma del 1996, con la quale il legislatore ha completamente modificato il framework normativo in materia di reati sessuali, abbandonando l'inquadramento di tali condotte all'interno della categoria dei reati contro la moralità pubblica e il buon costume e collocandole all'interno dei delitti contro la persona^[40], l'attuale normativa in materia di tutela penale della sfera sessuale è quasi completamente costruita intorno alla fattispecie di cui all'art. 609-bis c.p. che, come noto, contiene al proprio interno quattro diverse ipotesi di reato: la costrizione a compiere o subire atti sessuali con violenza o minaccia, con abuso di autorità, con abuso delle condizioni di inferiorità fisica o psichica della persona offesa, con inganno della stessa per essersi l'agente sostituito ad altra persona.

Tralasciando le discussioni generate in dottrina dalla fattispecie sulla permanenza all'interno della stessa del modello costrittivo^[41], appare decisamente più utile al fine di dimostrare l'inadeguatezza dell'attuale apparato normativo nel cogliere le sfide portate dall'evoluzione tecnologica, l'analisi di un altro aspetto inerente il reato di cui all'art. 609-bis: la nozione di "atto sessuale". Il concetto di "atto sessuale", sul quale si impernia la fattispecie di violenza sessuale^[42], ha infatti subito, negli ultimi anni, una reinterpretazione ad opera della dottrina e della giurisprudenza, nel tentativo di adattarlo all'evoluzione della sessualità nella società post-moderna^[43], che, proprio in virtù dell'avvento delle tecnologie, ha comportato una digitalizzazione dell'atto sessuale, svincolandolo dalla materialità classica del termine derivante dall'accoglimento dell'accezione oggettiva dello stesso, ancorata ai dati derivanti dalle scienze medico-tecnologiche. Nonostante parte della letteratura abbia evidenziato come il

concetto di "atto sessuale" sia suscettibile di espandersi in base al mutamento socioculturale che segna le pratiche sessuali, ancora oggi è possibile individuare un minimo comune denominatore su cui sembra potersi costruire un accordo tra dottrina^[44] e giurisprudenza: l'atto sessuale implica un coinvolgimento del corpo^[45] della vittima in relazione alle zone considerate erogene dalla scienza, dal costume o dal comune modo di sentire.

Tale visione, come si avrà modo di analizzare di qui a breve, rischia però di creare vuoti di tutela in relazione a condotte che, seppur non coinvolgendo il corpo nella sua materialità, sono in grado di lederlo nella sua dimensione complessiva, così come suggerito dalla teoria del digital embodiment.

Nonostante, infatti, negli ultimi anni si siano sviluppati orientamenti interpretativi tesi a estendere il concetto di atto sessuale in materia di violenza sessuale, tale da comprendere comportamenti estrinsecatesi nel cyberspace mediante immagini e video, la giurisprudenza maggioritaria continua a ritenere quale dato minimo imprescindibile il necessario "coinvolgimento del corpo" per identificare gli atti lesivi della libertà sessuale. Tale requisito pone non pochi problemi di tutela in relazione a tutta una serie di condotte, che sebbene possano dirsi offensive della libertà sessuale, provocando danni alla persona offesa del tutto assimilabili a quelli ingenerati dalle condotte di violenza sessuale, ciononostante, in assenza di un "coinvolgimento del corpo", non possono essere ricondotti alla fattispecie di cui all'art. 609-bis c.p.

A tal proposito, possono essere individuate due tipologie di condotte che evidenziano i limiti dell'apparato normativo vigente: la produzione non consensuale di materiale sessuale, alla cui categoria può essere ricondotta la creazione di contenuti deepfake sessualmente espliciti e la diffusione non consensuale di materiale sessuale che, come noto, ha trovato una propria regolamentazione attraverso l'inserimento all'interno del codice penale della fattispecie di cui all'art. 612-ter^[46]. Salvo quanto detto in ordine all'introduzione di una specifica fattispecie di reato per la seconda condotta^[47], è evidente che in presenza di un impianto normativo a tutela della libertà sessuale totalmente imperniato sulla fattispecie di violenza sessuale, la possibilità di proteggere i beni giuridici lesi dalla diffusione di deepfake sessualmente espliciti è rappresentata dalla riconducibilità o meno di tale condotta all'interno del reato di cui all'art. 609-bis e quindi dalla qualificabilità di tale tipologia di condotta quale compimento di un atto sessuale.

Tale limite dimostra l'inadeguatezza dell'attuale framework normativo: è fuor di dubbio, infatti, che tali tipologie di condotte, pur non potendo qualificarsi come violenza sessuale, siano lesive della libertà di autodeterminazione sessuale della persona offesa, la quale può subire aggressioni anche da condotte diverse da quelle previste dall'art. 609-bis.

Comportamenti che non coinvolgono direttamente il corpo della vittima possono comunque essere offensivi per la sua libertà sessuale, come a breve si dirà analizzando i danni evidenziati in letteratura derivanti dalla diffusione di deep fake. Invece di concentrarsi sulla violazione della corporeità come oggetto materiale, quindi, l'intervento penale dovrebbe mirare a tutelare la libertà sessuale. A tal proposito, i limiti dell'attuale apparato normativo, come appena evidenziato, emergono dai dubbi interpretativi, anche in ordine al bene giuridico tutelato, sollevati in dottrina dal primo contatto avuto dalla legislazione italiana con il materiale audiovisivo sessualmente esplicito realizzato artificialmente, una forma rudimentale di deepfake: la pedopornografia virtuale.

5. Il primo contatto del legislatore con i deepfake: l'art. 600-quater.1 c.p.

Il fenomeno dei deepfake, sebbene relativamente recente, essendo sorto, come evidenziato, in virtù dell'evoluzione delle tecnologie di A.I., ha delle radici che possono essere ricondotte a un predecessore concettuale nel contesto della c.d. pedopornografia virtuale, disciplinata dal legislatore mediante il reato di cui all'art. 600-quater.1 c.p., introdotto dall'art. 4, L. 6.2.2006 n. 38, recante "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"^[48]. La pedopornografia virtuale coinvolge la manipolazione e la creazione di immagini e video che mostrano minori coinvolti in atti sessuali, mediante l'utilizzo di strumenti di grafica avanzati. L'analisi di questa forma di abuso digitale può offrire preziose chiavi interpretative per comprendere i deepfake e gli strumenti necessari per contrastarli efficacemente, nonché aiutarci a individuare i beni giuridici lesi da tale fenomeno.

Prioritariamente rispetto all'analisi del dibattito dottrinale generato in dottrina in ordine all'individuazione dell'interesse tutelato dal reato di pedopornografia virtuale, occorre definire i contorni della fattispecie, onde evidenziare come il concetto di pedopornografia virtuale fatto proprio dal legislatore con la disciplina appena richiamata, sia caratterizzato da un'insufficiente determinatezza che, oltre a influire sull'individuazione delle condotte riconducibili alla fattispecie delittuosa, rende difficoltosa proprio la corretta individuazione del bene giuridico tutelato dalla norma.

L'estensione dell'ambito di applicabilità della disciplina contenuta negli artt. 600-ter e 600-quater c.p. alle condotte riguardanti materiale pornografico virtuale fu determinata da atti sovranazionali e, in particolare, un decisivo impatto sul legislatore ebbe la decisione quadro n. 2004/68/GAI, elaborata a seguito della Convention on Cybercrimes di Budapest del 2001^[49], in cui vennero individuate tre diverse categorie di pornografia infantile, l'ultima delle quali direttamente riconducibile al concetto di pedopornografia virtuale, definita come "immagini realistiche di un bambino inesistente implicato o coinvolto in una condotta sessualmente esplicita". Tale definizione, quindi, riconduceva nell'ambito

della pedopornografia virtuale anche quella avente ad oggetto immagini o video sessualmente espliciti ritraenti minori inesistenti.

Il legislatore interno, però, nel dare attuazione alla decisione quadro, non ha fornito una definizione del concetto di "pedopornografia virtuale" sufficientemente determinata: non è chiaro, infatti, se la definizione di pedopornografia virtuale debba includere solo i materiali multimediali derivati da immagini di minori reali riconoscibili o se debba estendersi alla cosiddetta "pedopornografia apparente", ovvero immagini di adulti che in virtù delle proprie caratteristiche somatiche sembrano minori, e alla "pedopornografia totalmente virtuale", creata attraverso la realizzazione artificiale di minori coinvolti in attività sessualmente esplicite, in assenza di alcun coinvolgimento di minori reali.

È evidente che tale indeterminatezza, come detto in precedenza, oltre a influire direttamente sull'individuazione delle condotte riconducibili alla fattispecie di reato, pone dei seri dubbi circa l'individuazione del bene tutelato dalla norma.

A seguito dell'entrata in vigore della normativa, parte della dottrina, anche richiamando il testo della Decisione quadro del 2004, la quale, come detto, faceva esplicito riferimento "alle immagini pedopornografiche di un bambino inesistente", propose un'interpretazione della fattispecie particolarmente estensiva, tale da ricomprendervi anche i casi di pedopornografia interamente virtuale: tale impostazione veniva giustificata anche sulla base della necessità di dare un'interpretazione conforme della norma alla decisione quadro.^[50] L'interpretazione estensiva della fattispecie, fatta propria anche dalla giurisprudenza di legittimità,^[51] ha trovato però obiezioni da parte di altri autori che hanno sottolineato come tale ricostruzione introducesse sostanzialmente un delitto senza vittima, sprovvisto di offensività e teso a punire esclusivamente la tendenza 'immorale' dell'autore della condotta^[52].

Secondo parte della dottrina, non sarebbero neppure fondate le deduzioni circa la sussistenza di un obbligo di interpretazione conforme alla decisione quadro: sebbene, infatti, la citata decisione quadro, nell'invitare gli Stati membri a introdurre strumenti idonei a punire la detenzione di pornografia infantile, abbia dato all'art. 3 una definizione della stessa particolarmente ampia, tale da ricomprendere anche la pedopornografia apparente e la pedopornografia virtuale, un'analisi del testo stesso della stessa decisione evidenzia come il legislatore sovranazionale avesse previsto la possibilità per gli Stati membri di esentare da responsabilità penale le condotte connesse alla pedopornografia c.d. apparente e interamente virtuale, riconoscendo la minore gravità di tali ipotesi. Non si può inoltre non evidenziare che la successiva Direttiva 2011/92/UE del 13 dicembre 2011, la quale ha sostituito integralmente la precedente decisione quadro, ha rimosso completamente il riferimento ai bambini "inesistenti", affinando la definizione e fornendo

un quadro più preciso. Tale direttiva, infatti, pur mantenendo sostanzialmente inalterata la definizione di pornografia minorile, ha escluso la pedopornografia totalmente virtuale dal campo di applicazione delle sanzioni penali. Ha inoltre introdotto una causa di non punibilità per i casi di pornografia apparente, a condizione che la produzione e la detenzione del materiale ottenuto siano destinate a un uso strettamente personale.

La suggerita interpretazione, volta a escludere dall'ambito del penalmente rilevante la pedopornografia apparente e quella totalmente virtuale, trova inoltre supporto nella collocazione sistematica della fattispecie che, coerentemente con la sua finalità di tutelare lo sviluppo fisico, psicologico, morale e sociale del minore, è inserita nell'alveo dei reati contro la personalità individuale: tale scelta, insieme alla più recente evoluzione della normativa sovranazionale, esprime la volontà del legislatore di proteggere la libertà e l'integrità del minore, escludendo dunque che la fattispecie di cui all'art. 600-quater 1 c.p. possa essere utilizzata per contrastare condotte moralmente riprovevoli, ma incapaci di ledere gli interessi di un minore reale.

L'individuazione del bene giuridico tutelato dalla fattispecie, come enunciato in premessa, è fortemente influenzata da quanto finora espresso in ordine alla corretta definizione dell'elemento oggettivo della fattispecie e, in particolare, circa l'interpretazione del concetto di pedopornografia virtuale.

La dottrina maggioritaria, alla luce delle considerazioni fatte, ritiene che l'unica interpretazione possibile della norma sia quella restrittiva, volta a escludere dall'ambito del punibile le condotte inerenti materiale pedopornografico totalmente virtuale o parzialmente virtuale, ma ottenuto mediante l'utilizzo di parti di minori non riconoscibili: ciò infatti permetterebbe di escludere dall'alveo del punibile condotte non idonee a provocare un danno al minore, coerentemente con quanto prescritto dal preambolo della L. n. 269/1998 che, come visto, individua quale interesse tutelato dalla norma proprio l'integrità del minore.

Laddove infatti il materiale pedopornografico virtuale fosse realizzato mediante l'utilizzo di immagini del minore ritraenti elementi non riconoscibili, neppure dal minore stesso, non potrebbe verificarsi una lesione dell'integrità del minore: secondo tale orientamento, quindi, il bene giuridico tutelato dalla norma sarebbe rinvenibile nel concetto di "onorabilità sessuale".

Tale concetto rappresenta una delle espressioni del più ampio bene giuridico dell'integrità personale del minore: alla base della predetta interpretazione si cela infatti l'idea che le condotte inerenti alla pedopornografia virtuale – utilizzando immagini di minori riconoscibili – ledano il corretto sviluppo della personalità del minore: come si è detto in

precedenza, analizzando il concetto di danno sessuale tecno-sociale, infatti, condotte realizzate totalmente online in assenza di un coinvolgimento del corpo nella sua dimensione materiale, sono in grado di produrre danni tangibili quanto altre forme di aggressione che si realizzano al di fuori della dimensione digitale.

Dalla diffusione di un contenuto multimediale che sovraimpone il corpo di un minore riconoscibile^[53] su quello corpo di una persona all'interno di un contesto pornografico, infatti, potrebbe derivare una lesione per la reputazione del minore e, di conseguenza, una lesione della sua stessa capacità di sviluppare rapporti sociali e di costruire la propria sessualità^[54]. Laddove invece venisse ritenuto integrato il reato in analisi anche in presenza di contenuti totalmente virtuali, adottando quindi la definizione più estensiva del concetto di pedopornografia virtuale^[55], a essere tutelato dalla norma non sarebbe più il singolo minore, bensì il minore inteso come categoria e la finalità perseguita dalla fattispecie sarebbe quella di evitare che i fanciulli vengano utilizzati quale strumento di soddisfacimento degli adulti. Abbracciando questa seconda interpretazione, quindi, il bene giuridico tutelato dalla norma non sarebbe l'integrità del singolo minore, ma la dignità dell'intera categoria^[56].

Tale interpretazione sembrerebbe però nulla di più che una ragione per giustificare l'uso del diritto penale per educare la collettività alla moralità^[57]. A quanto detto può essere aggiunto, inoltre, che l'interpretazione estensiva qui analizzata sembra basarsi su un assunto discutibile, secondo cui la diffusione di materiale pedopornografico totalmente virtuale sarebbe in grado di innescare una "spinta criminogena" non controllabile dal pedofilo che, di conseguenza, finirebbe per agire contro minori reali, attentando alla loro integrità psico-fisica. Tale tesi non si confronta con la possibilità che proprio il materiale pedopornografico totalmente virtuale potrebbe fungere da deterrente, offrendo al pedofilo uno strumento per appagare le sue pulsioni senza coinvolgere attivamente minori reali^[58].

Le considerazioni qui effettuate con l'analisi della pedopornografia virtuale, gettano le basi per una comprensione più approfondita del fenomeno dei deepfake sessualmente espliciti. Come si è avuto modo di evidenziare, l'indeterminatezza del termine "pedopornografia virtuale" ha portato a serie implicazioni non solo per l'identificazione delle condotte penalmente rilevanti, ma anche per l'individuazione del bene giuridico tutelato dalla norma.

L'esperienza fornita dal dibattito dottrinale e giurisprudenziale ingenerato dall'introduzione del reato di cui all'art. 600-quater.1 c.p., potrà essere utilizzata al fine di costruire una risposta legislativa al fenomeno dei deepfake che, partendo da una corretta analisi degli interessi lesi dalla creazione e diffusione di tale materiale, sia in grado di individuare con sufficiente determinatezza le condotte da perseguire.

Per determinare in modo efficace il bene giuridico da tutelare attraverso una normativa volta a contrastare i deepfake sessualmente espliciti, è indispensabile effettuare un'analisi dei danni derivanti dalla diffusione di tale materiale. L'attento esame del pregiudizio causato dai deepfake consentirà al legislatore di delineare la più adeguata protezione giuridica.

6. I danni derivanti dalla diffusione di deepfake sessualmente espliciti: gli embodied harm

Al fine di analizzare i danni derivanti dalla creazione e diffusione di deepfake sessualmente espliciti, occorre evidenziare che, sebbene essi rappresentino un fenomeno recente, possono essere ricondotti nella più ampia categoria elaborata dalla letteratura scientifica dei c.d. "image-based sexual abuse"^[59], nella quale rientrano tutte quelle azioni che implicano la creazione, la distribuzione o la minaccia di divulgare immagini o video sessualmente espliciti senza il consenso della persona raffigurata. I deepfake sessualmente espliciti rappresentano una sofisticata variante di questo genere di abusi, in cui le immagini non vengono semplicemente rubate o condivise senza consenso, ma vengono artificialmente create o modificate per mostrare la vittima in contesti sessuali che non ha mai vissuto^[60].

Nonostante la gravità e la portata di tale fenomeno, la ricerca scientifica in merito è ancora agli albori. Tuttavia, i primi risultati degli studi condotti forniscono una preziosa testimonianza dei danni che la diffusione di questa tipologia di materiale può arrecare.

L'analisi di questi risultati preliminari è dunque fondamentale per una comprensione approfondita del fenomeno e per lo sviluppo di una normativa efficace. Tali studi, ricollegandosi alla già citata teoria del digital embodiment, riconoscono come l'identità digitale non sia più separabile da quella fisica, ma ne rappresenti un'estensione. In questa prospettiva, i deepfake sessualmente espliciti provocano danni che la letteratura scientifica definisce "embodied", ossia incarnati, in quanto i traumi subiti nell'ambito digitale si riflettono concretamente sulla vita quotidiana e sul benessere delle vittime.

Tale affermazione nasce dal superamento della dicotomia tra danni fisici e virtuali che, fino a qualche anno fa, dominava la letteratura accademica e la comprensione sociale^[61]. Gli studiosi inquadrano i danni virtuali causati dagli image-based sexual abuse, come aventi effetti reati e tangibili sul piano fisico e psicologico delle vittime^[62]: recenti ricerche evidenziano come le vittime di questa tipologia di abusi subiscano danni analoghi a quelli delle vittime di violenza sessuale fisica; emergono infatti episodi di stress post-traumatico, ansia, depressione e perdita di autostima, i quali rappresentano la dimostrazione che,

come descritto dalla teoria del digital embodiment, i traumi fisici non sempre sono il risultato di aggressioni fisiche.

Tale approdo rappresenta l'evoluzione di quanto già affermato dalla letteratura scientifica prima dell'avvento delle moderne tecnologie: in passato, infatti, le persone che avevano subito molestie sessuali per mezzo, ad esempio, di chiamate oscene indesiderate, esitavano a definire le loro esperienze come abuso, nonostante avessero subito danni emotivi, fisici e sociali^[63].

La letteratura scientifica evidenzia come oggi lo stesso problema venga sollevato nel contesto dei deepfake sessualmente espliciti: le vittime di image-based sexual abuse, al pari di quelle di violenza sessuale tradizionale, riportano esperienze di umiliazione e trauma che vengono esacerbate da una sensazione di perdita di controllo del proprio corpo, causando conseguenze negative per la salute e lo sviluppo di strategie di coping inadeguate^[64].

La letteratura scientifica sottolinea che, sebbene non sia possibile definire tali abusi virtuali come equivalenti alle forme tradizionali di violenza sessuale, i risultati emersi dagli studi condotti sulle vittime di abusi virtuali dimostrano l'estensione e la gravità dei danni ingenerati da questa tipologia di condotte, con la necessità che queste ricevano lo stesso livello di considerazione, comprensione e riconoscimento^[65]. La letteratura scientifica ha quindi stabilito che esiste un continuum tra gli image-based sexual abuse e le altre forme di violenza sessuale^[66]. Basandosi sulla ancora limitata letteratura riguardante le esperienze vissute dalle vittime di deepfake sessualmente espliciti, infatti, è possibile individuare alcune caratteristiche comuni ad entrambe le tipologie di abusi, come ad esempio il concetto di "intrusione": le vittime riferiscono di aver subito conseguenze a livello emotivo, fisiologico, professionale, nelle relazioni sentimentali e praticamente in ogni singolo aspetto della loro vita^[67]. Come si è avuto modo di accennare, nonostante la rilevanza e l'attualità del fenomeno, la letteratura scientifica riguardante i deepfake sessualmente espliciti è ancora in fase di sviluppo, con uno sguardo particolare verso l'approfondimento delle esperienze vissute da chi si trova a esserne vittima. Recentemente, uno studio fenomenologico^[68] ha svolto un'indagine focalizzata proprio su questa prospettiva, esplorando le esperienze delle vittime di image-based sexual abuse e, più specificatamente, di deepfake sessualmente espliciti.

Tale studio ha coinvolto 58 individui, invitati a partecipare a interviste semi-strutturate. Tra questi, il 63% ha riferito di aver subito abusi legati a deepfake sessualmente espliciti. Le riflessioni emerse da questo corpus di interviste confermano quanto già anticipato dalla teoria del digital embodiment e dagli studi sugli image-based sexual abuse: l'analisi ha infatti rivelato come le condotte legate alla diffusione di deepfake causino un'interferenza

permanente nelle relazioni delle vittime con se stesse e con gli altri, risultando in un danno irreparabile che permea tutti gli aspetti della loro vita, sia online che offline.

Le esperienze delle vittime sono rappresentate come profondamente personali e invasive, tali da causare risposte emotive e fisiologiche immediate. Queste reazioni includono shock, disgusto, nausea, ansia e attacchi di panico, simili a quelle riscontrate dalla letteratura scientifica nei casi di violenza sessuale. A caratterizzare le risposte fisiologiche delle vittime è inoltre la persistenza dell'abuso rappresentato dalla diffusione di contenuti deepfake sessualmente espliciti: a differenza di quanto avviene a seguito di un trauma fisico, il materiale audiovisivo abusivo continua a esistere e circolare online, rendendo le vittime perpetuamente esposte al rischio di un rinnovato trauma ogni volta che il materiale viene visualizzato e condiviso. Oltre alle conseguenze psicologiche immediate, lo studio evidenzia le ripercussioni a lungo termine sulla vita personale, professionale e sociale delle vittime. Queste ripercussioni possono includere problemi di autostima, difficoltà nelle relazioni, perdita di fiducia negli altri, ritiro sociale e impatti sulla carriera. In alcuni casi estremi, l'esperienza traumatica ha portato anche a pensieri suicidi^[69].

Un'ulteriore caratteristica emersa dallo studio è l'esperienza di 'immobilizzazione tonica' vissuta dalle vittime, una reazione comune in situazioni di estremo pericolo o stress, spesso associata ai casi di violenza sessuale^[70]. La ricerca in analisi, inoltre, sottolinea come i deepfake sessualmente espliciti presentino delle caratteristiche uniche che li rendono particolarmente dannosi per le vittime: in particolare, la capacità di proliferazione infinita e la persistenza del materiale abusivo su Internet porta le vittime a vivere un'esperienza di abuso perpetua.

Nonostante l'attuale carenza di informazioni in ordine alle conseguenze causate dalla divulgazione di deepfake sessualmente espliciti, i risultati di queste preliminari ricerche confermano quanto già evidenziato in passato dagli studi empirici condotti sulle vittime di image-based sexual abuse, secondo i quali tali tipologie di condotte sono in grado di provocare danni che trascendendo il digitale, si manifestano profondamente nella vita quotidiana delle vittime, minando la loro salute fisica, psicologica e il loro benessere sociale. Gli studi analizzati dimostrano, quindi, come il danno patito dalle vittime di deepfake sessualmente espliciti sia della stessa natura di quello vissuto dalle vittime di violenza sessuale: tale dato rende evidente che, valorizzando la prospettiva vittimologica, sia possibile affermare l'esistenza di un continuum tra le condotte in analisi e quelle di violenza sessuale. Sebbene non sia possibile ricondurre tali condotte al concetto di violenza sessuale, è quindi possibile sostenere che le stesse vadano a ledere lo stesso bene giuridico: la libertà sessuale della vittima^[71]. Tale circostanza potrebbe rappresentare la base dalla quale costruire una normativa volta a contrastare il fenomeno in analisi.

7. La libertà sessuale quale bene giuridico leso dalla diffusione di deepfake sessualmente espliciti

Come si è avuto modo di constatare analizzando i contrasti dottrinali sorti a seguito dell'introduzione del reato di cui all'art. 600-quater.1. c.p., l'individuazione del bene giuridico da tutelare ha rilevanti conseguenze, producendo i propri effetti tanto sulla conformazione strutturale della fattispecie incriminatrice quanto sull'interpretazione del dato normativo e rappresenta, quindi, un antecedente logico necessario al fine di costruire una legislazione in grado di contrastare efficacemente le condotte oggetto del presente lavoro.^[72]

L'analisi degli studi empirici sui danni provocati dalla diffusione di deepfake sessualmente espliciti sembra confermare quanto detto in premessa circa la necessità di ripensare alla libertà sessuale quale bene giuridico nell'era post-moderna alla luce della teoria dell'incarnazione digitale: affermare la sussistenza di un continuum tra gli image-based sexual assault e la condotte di violenza sessuale non significa, infatti, affermare la piena sovrapposibilità fra i due fenomeni, bensì constatare che gli stessi pur differendo in ordine ai rispettivi elementi costitutivi, ledano il medesimo bene giuridico, ovvero la libertà sessuale della vittima^[73].

Non sembrano cogliere nel segno le obiezioni mosse da parte della dottrina a tale affermazione^[74]: seppure nella creazione e diffusione di deepfake sessualmente espliciti la vittima non venga costretta a compiere atti sessuali che coinvolgano il proprio corpo nella sua dimensione materiale, la creazione e diffusione non consensuale di materiale sessualmente esplicito, ottenuto mediante la sovrapposizione del proprio volto su corpi altrui, incide comunque sulla libertà del soggetto immortalato di decidere le condizioni e le modalità con cui esprimere la propria sessualità.

Tale libertà, come si è avuto modo di evidenziare, infatti, ben può assumersi violata pur in assenza di un coinvolgimento del corpo: quando l'immagine di un individuo viene utilizzata senza il suo consenso al fine di creare un deepfake sessualmente esplicito, egli perde il controllo su come la sua identità viene rappresentata o utilizzata in un contesto sessuale. Questo assunto trova conferma in quanto sostenuto dalla dottrina maggioritaria in materia di pedopornografia virtuale, la cui introduzione è stata motivata dalla circostanza, evidenziata dagli studi empirici, che la produzione di materiale sessualmente esplicito virtuale ottenuto tramite l'utilizzo di minori possa ledere il corretto sviluppo della loro personalità, provocando gravi conseguenze sia sul piano fisico che psichico^[75].

Le indagini empiriche, mostrando come i danni psicologici e fisici subiti dalle vittime di tali condotte siano comparabili a quelli causati da altri reati contro la libertà sessuale,

evidenziano chiaramente che, sebbene la diffusione di questo materiale possa provocare danni reputazionali significativi, il nucleo della questione legata ai deepfake sessualmente espliciti risiede nella violazione della libertà sessuale del soggetto coinvolto, un aspetto che va ben oltre il semplice carattere diffamatorio di tali contenuti^[76]. A tal proposito, appare opportuno evidenziare come il primo approccio normativo al problema da parte dell'Unione Europea non sembra tenere conto delle evidenze qui analizzate: anche se negli ultimi anni le istituzioni europee hanno manifestato un crescente interesse verso i deepfake, adottando numerose raccomandazioni e risoluzioni del Parlamento europeo che ne trattano esplicitamente il fenomeno^[77], il recente Regolamento sull'Intelligenza Artificiale^[78], pur includendo due disposizioni relative ai deepfake, non sembra affrontare adeguatamente le problematiche reali legate all'utilizzo di questa tecnologia per produrre contenuti sessualmente espliciti^[79]. Il regolamento citato, infatti, all'art. 53, par. 3, si limita a prevedere un obbligo di trasparenza in capo ai creatori di deepfake, obbligandoli a rendere evidente che il contenuto multimediale è stato artificialmente manipolato.

Tuttavia, alla luce delle riflessioni precedenti, emergono chiaramente le criticità di tale approccio: come sottolineato da parte della dottrina, questa disposizione rischia di risultare inefficace nel raggiungere l'obiettivo di disincentivare la produzione di deepfake dannosi, tra cui sicuramente figurano anche quelli sessualmente espliciti.

È evidente, infatti, che laddove il soggetto autore dei deepfake fosse intenzionato ad arrecare danno a un soggetto determinato o alla società, questi probabilmente utilizzerebbe delle tecniche tali da non rendere di facile identificazione la propria identità^[80]. Quest'approccio, peraltro, sembra prendere in considerazione quale bene giuridico lesa dalla creazione di deepfake esclusivamente la reputazione del soggetto rappresentato, contrastandone la lesione obbligando il creatore del contenuto a evidenziarne la natura falsa. Come brillantemente evidenziato dagli studi empirici, però, il danno percepito dalle vittime di deepfake sessualmente espliciti, non essendo legato esclusivamente alla reputazione e, in generale, alla dimensione sociale, si verifica indipendentemente dalla natura realistica del contenuto e perfino quando esso sia evidentemente falso^[81].

Lo strumento europeo sembra essere stato concepito principalmente per affrontare i deepfake disinformativi, che colpiscono beni giuridici differenti da quelli lesi dai deepfake sessualmente espliciti. Questi ultimi, come evidenziato in precedenza, sono in diretta continuità con altre forme di aggressione sessuale.

8. Considerazioni conclusive

Nell'affrontare il problema rappresentato dai deepfake, è importante riconoscere la vastità e la diversità delle loro forme. Regolamentazioni generalizzate, come quella proposta

dall'Unione Europea all'interno del Regolamento sull'Intelligenza Artificiale, pur rappresentando un primo tentativo di gestire il fenomeno, si rivelano insufficienti nel cogliere le peculiarità di alcune forme particolarmente dannose, come nel caso dei deepfake sessualmente espliciti. È evidente che la complessità del panorama attuale richieda una revisione dei metodi e degli strumenti legali impiegati per tutelare la libertà sessuale.

La crescente diffusione dei deepfake sessualmente espliciti pone una sfida significativa per il legislatore, che è chiamato a sviluppare soluzioni innovative in grado di rispondere alle specifiche dinamiche di questo fenomeno.

La teoria del digital embodiment e i contributi degli studi empirici offrono un valido supporto a questa riflessione, dimostrando come il confine tra realtà fisica e digitale si stia progressivamente indebolendo. Esse evidenziano come le aggressioni digitali possano produrre effetti concreti e tangibili sulle vittime, equiparabili a quelli derivanti da violenze fisiche. In questo senso, il fenomeno dei deepfake sessualmente espliciti potrebbe offrire al legislatore l'opportunità di rivedere il concetto di libertà sessuale nell'era post-moderna, affrontando in modo sistematico l'intera categoria degli image-based sexual abuse. Ciò richiederebbe l'adozione di una normativa che tuteli la libertà sessuale non solo nella sua dimensione materiale, ma anche in quella virtuale, riconoscendo la gravità delle aggressioni digitali e la necessità di proteggere la dignità e l'autodeterminazione sessuale delle vittime in un contesto tecnologicamente evoluto.

Note e riferimenti bibliografici

- [1] S. COLE, We are truly fucked: everyone is making AI-Generated fake porn now, in <https://motherboard.vice.com>, 24.01.2018, nel quale l'autore descrive come nel 2017 un utente anonimo di Reddit abbia postato numerosi video sessualmente espliciti su internet con lo pseudonimo "deepfake", ivi compreso un video dell'attrice Daisy Ridley ottenuto artificialmente attraverso l'utilizzo di un'intelligenza artificiale usata per scambiare il video dell'attrice con quello di una pornostar. Vedi anche K. DOLD, Face-Swapping Porn: How a Creepy Internet Trend Could Threaten Democracy, in www.rollingstone.com, 17.04.2018.
- [2] O. SCHWARTZ, You Thought Fake News Was Bad?: Deep Fakes Are Where Truth Goes to Die, in www.theguardian.com, 12.11.2018.
- [3] T. MAK, All Things Considered: Technologies to Create Fake Audio and Video Are Quickly Evolving, in www.npr.org, 3.04.2018.
- [4] Il termine deepfake prende il nome dall'utente di Reddit che per primo ha introdotto video modificati sessualmente espliciti su Internet. Il termine è una combinazione di due concetti: deep, dal concetto di deep learning, un aspetto dell'intelligenza artificiale che si occupa di emulare l'approccio di apprendimento che gli esseri umani usano per acquisire determinati tipi di conoscenza; e fake, dal concetto di fake news, ovvero una notizia inaccurata o sensazionalistica creata per attirare l'attenzione, fuorviare, ingannare o danneggiare la reputazione di qualcuno. Vedi anche J. VINCENT, Why We Need a Better Definition of 'Deepfake', in www.theverge.com, 22.11.2019.
- [5] Non è rinvenibile nella letteratura scientifica una definizione di intelligenza artificiale univoca. Nel 1968, Marvin Minsky, scienziato e matematico statunitense specializzato nel campo dell'intelligenza artificiale, la definisce nel suo libro *Semantic information processing* come «la scienza di far fare alle macchine cose che richiederebbero intelligenza se fatte dall'uomo». Nel regno dell'intelligenza artificiale rientra quindi ogni tipo di comportamento intelligente: dal gioco degli scacchi alla comprensione dei racconti, dalle scoperte matematiche alle diagnosi mediche. È inoltre possibile distinguere una definizione scientifica da una filosofica, di intelligenza artificiale: secondo gli scienziati, la stessa è lo studio degli agenti che ricevono percezioni dall'ambiente ed eseguono azioni. Lo scopo è realizzare diverse tecniche per permetterlo. Secondo la filosofia, invece, l'intelligenza artificiale è il campo dedicato alla costruzione di animali/persone artificiali che appaiono come animali o come persone. La definizione scientifica è inclusa in questa. In tema, si veda in tal senso J. KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Roma, 2017, 4 ss.
- [6] A. HAUSER, M. Ruef, Deepfake - An Introduction, in www.scip.ch, 24.03.2018.
- [7] N. HENRY, A. POWELL, Embodied Harms: Gender, Shame and Technology Facilitated Sexual Violence, in *Violence Against Women*, 2015, 21, 6, 1 ss.
- [8] Il Deep Learning è una tipologia di intelligenza artificiale che simula le modalità con le quali gli esseri umani acquisiscono nuove conoscenze. Sui dettagli in ordine al suo funzionamento vedi infra. par. 2
- [9] Sul concetto di riservatezza sessuale quale bene giuridico tutelato dall'incriminazione della pornografia non consensuale si v. 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 *Riv. it. proc. pen.*, 2019, 4, 2045 ss.
- [10] Reddit è tra i primi dieci siti web più popolari negli Stati Uniti e tra i primi venti al mondo e si è autodefinito come la prima pagina di internet, in questi termini si esprimono J. WIDMAN, What Is Reddit?: A Beginner's Guide to the Front Page of the Internet, in www.digitaltrends.com, 22.05.2019. Esso è sostanzialmente una raccolta di forum web, noti anche come "subreddit", in cui comunità di utenti condividono notizie e contenuti o commentano post su argomenti specifici che spaziano dal semplice all'inusuale. Il nome di un subreddit inizia colloquialmente con "r/", mimando la struttura dell'URL di Reddit. Su r/shakespeare, ad esempio, gli utenti discutono di William Shakespeare e delle sue opere, mentre su r/birdswitharms pubblicano immagini di uccelli con le braccia.
- [11] D. HAWKINS, Reddit Bans 'Deepfakes', Pornography Using the Faces of Celebrities Such as Taylor Swift and Gal Gadot, in www.washingtonpost.com, 8.02.2018.

[12] K. ROOSE, Here Come the Fake Videos Too, in www.nytimes.com, 4.03.2018.

[13] A. DODGE, Using Fake Video Technology to Perpetuate Intimate Partner Abuse, in www.cpedv.org, 2019.

[14] Deeptrace è un sito web nato nel 2019 con l'obiettivo di monitorare la diffusione dei contenuti deepfake su Internet in modo tale da fornire agli utenti della rete e alle istituzioni le statistiche necessarie a comprendere il fenomeno. Il sito web è consultabile al seguente link: www.deeptracetechnology.com.

[15] H. AJDER, G. PATRINI, F. CAVALLI, L. CULLEN, The State of Deepfakes, in www.deeptracelabs.com, 2019.

[16] D. HARDWELL, Fake-porn videos are being weaponized to harass and humiliate women: everybody is a potential target, in www.washingtonpost.com, 18.12.2019. Nel contributo l'autore illustra anche perché non sia corretto utilizzare il termine "pornografia", che sottintende un consenso alla creazione e alla diffusione del materiale.

[17] La vergogna sociale derivante dalla diffusione non consensuale di materiale sessualmente esplicito è stata analizzata da M. MATTIA, "Revenge porn" e suicidio della vittima: il problema della divergenza tra 'voluto' e 'realizzato' rispetto all'imputazione oggettiva degli eventi psichici, in www.laegislazionepenale.eu, 18.07.2019, 13 ss.

[18] Termine coniato dalla dottrina anglosassone per indicare la divulgazione non consensuale, dettata da finalità vendicative, di immagini intime raffiguranti l'ex partner. Si v. C. LOTTA, 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, in *Consulta online*, 2019, 2, 331 ss. e C. PARODI, La tutela della persona nella realtà telematica: revenge porn e cyberstalking, in www.magistraturaindipendente.it, 2.02.2020.

[19] A. L. SAMUEL, Some studies in machine learning using the game of checkers, in *IBM Journal of research and development*, 1959, 12, 2 ss.

[20] Sulla storia della nascita dell'intelligenza artificiale, si veda G. ITALIANO, *Intelligenza artificiale: passato, presente, futuro*, in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Pizzetti, Torino, 2018, 206 ss. e S. RUSSELL, P. NORVIG, *Artificial intelligence. A modern approach*, Edimburgo, 2016.

[21] D. IMBRUGLIA, L'intelligenza artificiale (IA) e le regole. Appunti., in www.medialaws.eu, 4.02.2020.

[22] S. QUINTARELLI, *Intelligenza artificiale: cos'è davvero, come funziona, che effetti avrà*, Torino, 2020, 33 ss.

[23] G. CONTISSA, 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, 4, 4 ss.

[24] M. B. MAGRO, *Decisione umana e decisione robotica un'ipotesi di responsabilità da procreazione robotica*, in www.laegislazionepenale.eu, 10.05.2020.

[25] P. STONE, R. BROOKS, R. CALO, O. ETZIONI, G. HAGER, J. HIRSCHBERG, S. KALYANAKRISHNAN, E. KAMAR, S. KRAUS, K. LEYTON-BROWN, D. PAKERS, W. PRESS, A. SAXENIAN, J. SHAH, M. TAMBE, A. TELLER, *Artificial intelligence and life in 2030, Report of the 2015 Study Panel*, Stanford, 2016, consultabile in <https://apo.org.au>

[26] D. YADAV, S. SALMANI, Deepfake: A Survey on Facial Forgery Technique Using Generative Adversarial Network, in *International Conference on Intelligent Computing and Control Systems (ICCS)*, 2019, 18, 852 ss.

[27] D. GUERA, E. DELP, Deepfake Video Detection Using Recurrent Neural Networks, atti del quindicesimo IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) del 27-28 novembre 2018, consultabile in <https://ieeexplore-ieee.org>.

[28] T. KIRCHENGAST, Deepfakes and image manipulation: criminalization and control, in *Information & Communications technology law*, 2020, 29, 3, 308 ss.

[29] D. GUERA, E. DELP, op. cit.

- [30] B. MARR, *The Best (And Scariest) Examples Of AI-Enabled Deepfakes*, in www.forbes.com, 22.07.2019.
- [31] Si prenda ad esempio l'applicazione per smartphone Wombo che, utilizzando una versione rudimentale della tecnologia analizzata, applica alle immagini la tecnologia lip-sync per creare video satirici e che, nel 2021, è stata scaricata più di 2 milioni di volte nelle prime due settimane dopo il suo lancio. Si v. S. ASARCH, *Wombo.ai lets users make silly deepfakes videos of their friend or celebrities Singing Songs*, in www.insider.com, 12.03.2021.
- [32] M. VIZZARDI, *La violenza sessuale (art. 609-bis)*, in *I delitti contro la persona. Libertà personale, sessuale e morale, domicilio e segreti*, a cura di Piergallini, Viganò, Vizzardi, Verri, Milano, 2015, 47 ss.
- [33] B. PANATTONI, *Violazione "incorporee" della sfera sessuale. Possibili evoluzioni ed insidie nell'ambito dei reati sessualmente connotati*, in *Arch. pen.*, 2022, 3, 2 ss.
- [34] L'utilizzo di tale teoria per ripensare alle aggressioni sessuali effettuate nell'era digitale è stato suggerito da B. PANATTONI, op. cit., 4 ss. Le considerazioni dell'autrice sono perfettamente adattabili all'analisi dei beni giuridici potenzialmente lesi dalle condotte in materia di deepfake sessualmente espliciti e rappresentano la base concettuale del presente lavoro. Si rimanda al suo contributo per una più approfondita analisi circa il rapporto tra la teoria del digital embodiment e i reati sessuali.
- [35] A. POWELL, N. HENRY, *Sexual Violence in a Digital Age*, Londra, 2017, 49 ss.
- [36] E. GROSZ, *Volatile Bodies: Toward a Corporeal Feminism*, Bloomington, 1994, 120 ss. V. anche K. PLUMMER, *La sociologia della sessualità e il ritorno del corpo*, in *Rassegna Italiana di Sociologia*, 2002, 3.
- [37] In tal senso si esprime M. WHITE, *Networked Bodies and Extended Corporealities: Theorizing the Relationship between the Body, Embodiment, and Contemporary New Media*, in *Feminist Studies*, 2009, 35, 615 ss. Secondo il quale le estensioni digitali della persona ottenute attraverso i mezzi informatici non possono essere considerate "corporali".
- [38] Su tale aspetto ci si soffermerà infra nel par. 6 nel quale verrà analizzato il concetto di embodied harm.
- [39] L'approccio vittimologico come motore propulsivo della riforma è analizzato da L. PICOTTI, *Il delitto sessuale: da sfogo "non autorizzato" della libidine a "rapporto interpersonale" illecito. Spunti di riflessione sull'evoluzione e la riforma dei reati sessuali*, Padova, 1996, 419 ss.
- [40] L. PICOTTI, *Profili generali di diritto penale sostanziale*, in *La violenza sessuale a cinque anni dall'entrata in vigore della Legge n. 66/96. Profili giuridici e criminologici*, a cura di Cadoppi, Padova, 2001, 20 ss.
- [41] Secondo il quale al fine di ritenere integrato il reato è necessario che vi sia violenza e minaccia e, quindi, la persistente prevalenza della tutela della libertà sessuale in senso negativo, da più parti avversata nell'ottica di accogliere un modello consensualistico, secondo il quale possa essere ritenuta sufficiente la manifestazione del dissenso affinché possa dirsi integrata un'ipotesi di violenza sessuale, in tal senso si veda G. FLORA, *La tutela della libertà sessuale ed i tormenti di cupido nell'era postmoderna*, in *Criminalia*, 2018, 180 ss.
- [42] In tal senso si v. Vizzardi, op. cit.
- [43] L. GOISIS, *La violenza sessuale: profili storici e criminologici. Una storia di genere*, in *Dir. pen. cont.*, 31.10.2012.
- [44] Per un'analisi approfondita sul tema si v. M. VIZZARDI, *Violenza sessuale senza coinvolgimento del corpo della vittima?*, in *Dir. pen. cont.*, 2017, 2, 57 ss.
- [45] Sull'opportunità di parlare di coinvolgimento del corpo piuttosto che di contatto fisico si v. L. PICOTTI, *La violenza sessuale via whatsapp*, in *Diritto di Internet*, 2020, 4, 683 ss.
- [46] Sull'introduzione dell'art. 612-ter si v. P. DI NICOLA TRAVAGLINI, F. MENDITTO, *Codice rosso: il contrasto alla violenza di genere: dalle fonti sovranazionali agli strumenti applicativi: commento alla Legge 19 luglio 2019, n. 69*, Milano, 2020.
- [47] Il cui bene giuridico secondo la dottrina maggioritaria è comunque da identificarsi nella riservatezza sessuale, in tal senso si veda G.M. CALETTI, op. cit., 2040 ss.

- [48] Su cui si v. A. MANNA, F. RESTA, I delitti pedopornografia, alla luce della legge 38/2006, una tutela virtuale, in *Diritto dell'Internet*, 2006, 6, 221 ss.
- [49] La Convenzione di Budapest del 2001 ha come obiettivo la determinazione di una politica comune nell'ambito territoriale degli Stati parte nella lotta ai crimini informatici. Si v. R. BIANCHI, Commento art. 600-quater.1, in *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, a cura di Cadoppi, Padova, 2006, 248 ss.
- [50] V. MANES, L'incidenza delle "decisioni-quadro" sull'interpretazione in materia penale: profili di diritto sostanziale, in *Cass. pen.*, 2006, 3, 1150 ss. nonché F. VIGANO', *Recenti sviluppi in tema di rapporti fra diritto comunitario e diritto penale*, in *Dir. pen. e proc.*, 2005, 1437 ss.
- [51] A. CHIBELLI, La Cassazione alle prese con il delitto di pornografia minorile virtuale: lo 'strano caso' della pedopornografia a fumetti, in *Dir. pen. cont.*, 2017, 6, 290 ss.
- [52] Su tale aspetto si v. C. SOTIS, Il caso Pupino: profili sostanziali, in *AA.VV.*, *L'interpretazione conforme al diritto comunitario in materia penale*, a cura di Sgubbi e Manes, Bologna, 2007, 49 ss..
- [53] Come evidenziato da parte della dottrina, infatti, laddove le immagini pedopornografiche siano state realizzate mediante parti non riconoscibili di minori, queste dovrebbero essere equiparate a quelle totalmente virtuali in termini di offensività e quindi andare esenti da incriminazione. In questi termini si esprime G. COCCO, *Può costituire reato la detenzione di pornografia minorile?*, in *Riv. it. dir. e proc. pen.*, 2006, 3, 889 e M. MONTELEONE, *Lo sfruttamento sessuale dei bambini e la pedopornografia nella l. 6 febbraio 2006, n. 38*, in *Giur. Di Merito*, 2007, 2196.
- [54] S. DELSIGNORE, Art. 600 ter-Pornografia minorile, in *Trattato di diritto penale - Parte speciale, VIII, I delitti contro l'onore e la libertà individuale*, a curia di Manna, Papa, Canestrari e Cadoppi, Torino, 2010, 409 ss.
- [55] O. DI GIOVINE, Art. 600 quater.1, in *Codice penale 5° ed.*, a cura di Padovani, Milano, 2011, 4205 ss.
- [56] L. PISTORELLI, *Attenzione spostata sulla perversione del reato*, in *Guida dir.*, 2006, 9, 51 ss.
- [57] M. DONINI, "Danno" e "offesa" nella c.d. tutela penale dei sentimenti. Note su morale e sicurezza come beni giuridici, a margine della categoria dell' "offense" di Joel Feinberg, in *Laicità, valori e diritto penale. The Morals Limits of the Criminal Law*, a cura di Cadoppi, Milano, 2010, 83.
- [58] In questi termini A. PECCIOLI, *Reati contro la libertà sessuale*, in *Manuale di diritto penale. Parte speciale 1*, a cura di Antolisei, Milano, 2016, 210.
- [59] N. HENRY, C. MCGLYNN, A. FLYNN, K. JOHNSON, A. POWELL, A. J. SCOTT, *Image-based sexual abuse. A study on the causes and consequences of non-consensual nude or sexual imagery*, Londra, 2021, 17 ss.
- [60] C. MCGLYNN, K. KOHNSON, E. RACKLEY, N. HENRY, N. GAVEY, A. FLYNN, A. POWELL, *It's Torture for the Souls: The Harms od Image-Based Sexual Abuse*, in *Social & Legal Studies*, 2021, 30, 4, 541 ss.
- [61] T. MCKINLAY, T. LAVIS, "Why did she send it in the first place? Victim Blame in the Context of 'Revenge Porn'", in *Psychiatry, Psychology and Law*, 2022, 27, 3, 386 ss.
- [62] N. HENRY, A. POWELL, *op. cit.*, 55 ss.
- [63] L. KELLY, *The continuum of Sexual Violence*, in *Women, Violence, and Social Control*, a cura di Hanmer e Maynard, Londra, 1987, 47 ss.
- [64] V. ROUSAY, *Sexual deepfakes and Image-based sexual abuse: Victim-Survivor Experiences and Embodied Harms*, Harvard University, aprile 2023, consultabile in <https://URL>
- [65] Y. RUVALCABA, A. A. EATON, *Nonconsensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men*, in *Psychology of Violence*, 2020, 10, 1, 15 ss.
- [66] C. MCGLYNN, E. RACKLEY, R. HOUGHTON, *Beyond Revenge Porn: The Continuum of Image-Based Sexual Abuse*, in *Feminist Legal Studies*, 2017, 25, 25 ss.

[67] A. MCFLYNN, A. POWELL, A. J. SCOTT, E. CAMA, Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse, in *The British Journal of Criminology*, 2022, 62, 6, 1244 ss.

[68] Con studio fenomenologico si intende un metodo di studio di recente sviluppo, impiegato per esaminare il modo in cui le persone danno senso e reagiscono alle esperienze della loro vita, nato per studiare ambiti considerati difficilmente investigabili attraverso i tradizionali metodi quantitativi. Per approfondire si veda J. A. SMITH, Evaluating the contribution of interpretative phenomenological analysis, in *Health Psychology Review*, 2011, 5, 1, 9 ss. e L. SASSO, A. BAGNASCO, L. GHIROTTI, La ricerca qualitativa. Una risorsa per i professionisti della salute, Milano, 2015, 7 ss.

[69] S. BATES, Revenge Porn and Mental Health, in *Feminist Criminology*, 2017, 12, 1, 22 ss.

[70] M. J. BOVIN, S. JAGER-HYMAN, S. D GOLD, B. P. MARX, D. M. SLOAN, Tonic Immobility Mediates the Influence of Peritraumatic Fear and Perceived Inescapability on Posttraumatic Stress Symptom Severity among Sexual Assault Survivors, in *Journal of Traumatic Stress*, 2008, 21, 4, 402 ss.

[71] S. BLOOM, No vengeance for “revenge porn” victims: Unraveling why this latest femalecentric, intimate-partner offense is still legal, and why we should criminalize it, in *Fordham Urban Law Journal*, 2014, 42, 233, 275 ss.

[72] M. VIZZARDI, op. cit., 61 ss.

[73] B. PANATTONI, op. cit. 23 ss.

[74] Non ritiene sia possibile ritenere gli image-based sexual assault lesivi della libertà sessuale N. AMORE, La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall’art. 612-ter c.p., in www.lalegislazionepenale.eu, 20.01.2020.

[75] Vedi supra par. 5

[76] In tal senso si veda C. MCGLYNN, E. RACKLEY, L. HOUGHTON, , op. cit., 36, secondo i quali <<while these acts of abuse are without doubt egregious breaches of privacy, conceptualising the harm in this way inhibits recognition of the gendered, sexualised and abusive nature of the practices of image-based sexual abuse>>

[77] In particolare si fa riferimento alla Raccomandazione del Parlamento europeo del 13 marzo 2019 al Consiglio e al vicepresidente della Commissione e alla Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale.

[78] Per una preliminare analisi sul Regolamento dell’Unione Europea in materia di Intelligenza Artificiale citato si veda D. MESSINA, La proposta di regolamento europeo in materia di Intelligenza Artificiale: verso una “discutibile tutela individuale di tipo consumer-centric nella società dominata dal “pensiero artificiale”, in www.medialaws.eu, 30.09.2022.

[79] Per un’analisi approfondita dei rapporti fra il Regolamento sull’Intelligenza Artificiale e i deepfake si veda M. CAZZANIGA, Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai deepfakes, in medialaws.eu, 14.06.2023. Nel contributo l’autrice si sofferma sui deepfake utilizzati per diffondere notizie false.

[80] M. VAN JUIJSTEE, P. VAN BOHEEMEN, D. DAS, L. NIERLING, J. JAHEL, M. KARABOGA, M. FATUN, L. KOOL, J. GERRITSEN, Tackling deepfakes in European policy, in <https://www.europarl.europa.eu>, Luglio 2021.

[81] A. E. WALDMAN, A Breach of Trust: Fighting Nonconsensual Pornography, in *Iowa Law Review*, 2017, 102, 709, 10. Secondo l’autore, infatti, il danno per le vittime si verificherebbe << whether therepresentation is text-based, picture-based, or in video form such as deepfakes, and even when the fake pornographic representation is neither exactly real nor exactly make-believe the harm is nonetheless profoundly, compellingly, and emotionally true>>

Bibliografia

AMORE N., La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall’art. 612-ter c.p., in www.lalegislazionepenale.eu, 20.01.2020.

BATES S., Revenge Porn and Mental Health, in *Feminist Criminology*, 2017, 12, 1, 22 ss.

BIANCHI R., Commento art. 600-quater.1, in *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, a cura di Cadoppi, Padova, 2006, 248 ss.

BLOOM S., No vengeance for “revenge porn” victims: Unraveling why this latest femalecentric, intimate-partner offense is still legal, and why we should criminalize it, in *Fordham Urban Law Journal*, 2014, 42, 233, 275 ss.

BOVIN M. J., S. JAGER-HYMAN, S. D GOLD, B. P. MARX, D. M. SLOAN, Tonic Immobility Mediates the Influence of Peritraumatic Fear and Perceived Inescapability on Posttraumatic Stress Symptom Severity among Sexual Assault Survivors, in *Journal of Traumatic Stress*, 2008, 21, 4, 402 ss.

CALETTI G. M., Libert  e riservatezza sessuale all’epoca di internet. L’art. 612-ter c.p. e l’incriminazione della pornografia non consensuale, in *Riv. it. proc. pen.*, 2019, 4, 2045 ss.

CAZZANIGA M., Una nuova tecnica (anche) per veicolare disinformazione: le risposte europee ai deepfakes, in *medialaws.eu*, 14.06.2023.

CHIBELLI A., La Cassazione alle prese con il delitto di pornografia minorile virtuale: lo ‘strano caso’ della pedopornografia a fumetti, in *Dir. pen. cont.*, 2017, 6, 290 ss.

COCCO G., Pu  costituire reato la detenzione di pornografia minorile?, in *Riv. it. dir. e proc. pen.*, 2006, 3, 889

CONTISSA G, LASAGNI G., SARTOR G., Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo, in *Diritto di Internet*, 2019, 4, 4 ss.

DELSIGNORE S., Art. 600 ter-Pornografia minorile, in *Trattato di diritto penale - Parte speciale, VIII, I delitti contro l’onore e la libert  individuale*, a curia di Manna, Papa, Canestrari e Cadoppi, Torino, 2010, 409 ss.

DI GIOVINE O., Art. 600 quater.1, in *Codice penale 5° ed.*, a cura di Padovani, Milano, 2011, 4205 ss.

DI NICOLA TRAVAGLINI P., F. MENDITTO, *Codice rosso: il contrasto alla violenza di genere: dalle fonti sovranazionali agli strumenti applicativi: commento alla Legge 19 luglio 2019, n. 69*, Milano, 2020.

DONINI M., “Danno” e “offesa” nella c.d. tutela penale dei sentimenti. Note su morale e sicurezza come beni giuridici, a margine della categoria dell’ “offense” di Joel Feinberg, in *Laicit , valori e diritto penale. The Morals Limits of the Criminal Law*, a cura di Cadoppi, Milano, 2010, 83.

FLORA G., La tutela della libert  sessuale ed i tormenti di cupido nell’era postmoderna, in *Criminalia*, 2018, 180 ss.

GOISIS L., La violenza sessuale: profili storici e criminologici. Una storia di genere, in *Dir. pen. cont.*, 31.10.2012.

GROSZ E., *Volatile Bodies: Toward a Corporeal Feminism*, Bloomington, 1994, 120 ss.

HENRY N, POWELL A., *Embodied Harms: Gender, Shame and Technology Facilitated Sexual Violence, in Violence Against Women*, 2015, 21, 6, 1 ss.

HENRY N., C. MCGLYNN, A. FLYNN, K. JOHNSON, A. POWELL, A. J. SCOTT, *Image-based sexual abuse. A study on the causes and consequences of non-consensual nude or sexual imagery*, Londra, 2021, 17 ss.

IMBRUGLIA D., L’intelligenza artificiale (IA) e le regole. Appunti., in *www.medialaws.eu*, 4.02.2020.

ITALIANO G., *Intelligenza artificiale: passato, presente, futuro*, in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Pizzetti, Torino, 2018, 206 ss.

KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo*, Roma, 2017, 4 ss.

KELLY L., *The continuum of Sexual Violence*, in *Women, Violence, and Social Control*, a cura di Hanmer e Maynard, Londra, 1987, 47 ss.

KIRCHENGAST T., *Deepfakes and image manipulation: criminalization and control*, in *Information &*

Communications technology law, 2020, 29, 3, 308 ss.

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, in *Consulta online*, 2019, 2, 331 ss.

MAGRO M. B., Decisione umana e decisione robotica un’ipotesi di responsabilità da procreazione robotica, in www.laegislazionepenale.eu, 10.05.2020.

MANES V., L’incidenza delle “decisioni-quadro” sull’interpretazione in materia penale: profili di diritto sostanziale, in *Cass. pen.*, 2006, 3, 1150 ss.

MANNA A., RESTA F., I delitti pedopornografia, alla luce della legge 38/2006, una tutela virtuale, in *Diritto dell’Internet*, 2006, 6, 221 ss.

MATTIA M., “Revenge porn” e suicidio della vittima: il problema della divergenza tra ‘voluto’ e ‘realizzato’ rispetto all’imputazione oggettiva degli eventi psichici, in www.laegislazionepenale.eu, 18.07.2019, 13 ss.

MCFLYNN A., POWELL A., SCOTT A. J., CAMA E., Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse, in *The British Journal of Criminology*, 2022, 62, 6, 1244 ss.

MCGLYNN C., RACKLEY E., HOUGHTON R., Beyond Revenge Porn: The Continuum of Image-Based Sexual Abuse, in *Feminist Legal Studies*, 2017, 25, 25 ss.

MCGLYNN C., K. KOHNSON, E. RACKLEY, N. HENRY, N. GAVEY, A. FLYNN, A. POWELL, It’s Torture for the Souls: The Harms od Image-Based Sexual Abuse, in *Social & Legal Studies*, 2021, 30, 4, 541 ss.

MESSINA D., La proposta di regolamento europeo in materia di Intelligenza Artificiale: verso una “discutibile tutela individuale di tipo consumer-centric nella società dominata dal “pensiero artificiale”, in www.medialaws.eu, 30.09.2022.

MONTELEONE M., Lo sfruttamento sessuale dei bambini e la pedopornografia nella l. 6 febbraio 2006, n. 38, in *Giur. Di Merito*, 2007, 2196.

PANATTONI B., Violazione “incorporee” della sfera sessuale. Possibili evoluzioni ed insidie nell’ambito dei reati sessualmente connotati, in *Arch. pen.*, 2022, 3, 2 ss.

PARODI C., La tutela della persona nella realtà telematica: revenge porn e cyberstalking, in www.magistraturaindipendente.it, 2.02.2020.

PECCIOLI A., Reati contro la libertà sessuale, in *Manuale di diritto penale. Parte speciale 1*, a cura di Antolisei, Milano, 2016, 210.

PICOTTI L., Il delitto sessuale: da sfogo “non autorizzato” della libidine a “rapporto interpersonale” illecito. Spunti di riflessione sull’evoluzione e la riforma dei reati sessuali, Padova, 1996, 419 ss.

PICOTTI L., La violenza sessuale via whatsapp, in *Diritto di Internet*, 2020, 4, 683 ss.

PICOTTI L., Profili generali di diritto penale sostanziale, in *La violenza sessuale a cinque anni dall’entrata in vigore della Legge n. 66/96. Profili giuridici e criminologici*, a cura di Cadoppi, Padova, 2001, 20 ss.

PISTORELLI L., Attenzione spostata sulla perversione del reato, in *Guida dir.*, 2006, 9, 51 ss.

PLUMMER K., La sociologia della sessualità e il ritorno del corpo, in *Rassegna Italiana di Sociologia*, 2002, 3.

POWELL A., HENRY N., *Sexual Violence in a Digital Age*, Londra, 2017, 49 ss.

QUINTARELLI S., *Intelligenza artificiale: cos’è davvero, come funziona, che effetti avrà*, Torino, 2020, 33 ss.

ROUSAY V., *Sexual deepfakes and Image-based sexual abuse: Victim-Survivor Experiences and Embodied Harms*, Harvard University, aprile 2023, consultabile in {https/URL}

RUSSELL S., NORVIG P., *Artificial intelligence. A modern approach*, Edimburgo, 2016.

RUVALCABA Y., EATON A. A., Nonconsensual pornography among U.S. adults: A sexual scripts framework on victimization, perpetration, and health correlates for women and men, in *Psychology of Violence*, 2020, 10, 1, 15 ss.

SAMUEL A. L., Some studies in machine learning using the game of checkers, in *IBM Journal of research and development*, 1959, 12, 2 ss.

SASSO L., A. BAGNASCO, L. GHIROTTI, *La ricerca qualitativa. Una risorsa per i professionisti della salute*, Milano, 2015, 7 ss.

SMITH J. A., Evaluating the contribution of interpretative phenomenological analysis, in *Health Psychology Review*, 2011, 5, 1, 9 ss.

SOTIS C., Il caso Pupino: profili sostanziali, in AA.VV., *L'interpretazione conforme al diritto comunitario in materia penale*, a cura di Sgubbi e Manes, Bologna, 2007, 49 ss.

T. MCKINLAY, T. LAVIS, "Why did she send it in the first place? Victim Blame in the Context of 'Revenge Porn'", in *Psychiatry, Psychology and Law*, 2022, 27, 3, 386 ss.

VIGANO' F., Recenti sviluppi in tema di rapporti fra diritto comunitario e diritto penale, in *Dir. pen. e proc.*, 2005, 1437 ss.

VIZZARDI M., La violenza sessuale (art. 609-bis), in *I delitti contro la persona. Libertà personale, sessuale e morale, domicilio e segreti*, a cura di Piergallini, Viganò, Vizzardi, Verri, Milano, 2015, 47 ss.

VIZZARDI M., Violenza sessuale senza coinvolgimento del corpo della vittima?, in *Dir. pen. cont.*, 2017, 2, 57 ss.

WALDMAN A. E., A Breach of Trust: Fighting Nonconsensual Pornography, in *Iowa Law Review*, 2017, 102, 709, 10.

WHITE M., Networked Bodies and Extended Corporealities: Theorizing the Relationship between the Body, Embodiment, and Contemporary New Media, in *Feminist Studies*, 2009, 35, 615 ss.

YADAV D., SALMANI S., Deepfake: A Survey on Facial Forgery Technique Using Generative Adversarial Network, in *International Conference on Intelligent Computing and Control Systems (ICCS)*, 2019, 18, 852 ss.

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
<https://rivista.camminodiritto.it/articolo.asp?id=10957>