“RISPONDIMI VELOCEMENTE”

ANALISI MULTIDISCIPLINARE
DELLA SEXTORTION MASCHILE IN ITALIA

REPORT 2025

ASSOCIAZIONE PERMESSONEGATO

A cura di:

Edel Margherita Beckman, laureata in Giurisprudenza e specializzata in Criminologia clinica e Vittimologia, si occupa di violenza di genere e criminologia digitale, con particolare attenzione alla condivisione non consensuale di materiale intimo e al cyberbullismo. Il suo lavoro esplora l'intersezione tra tecnologia e relazioni umane, analizzando come gli strumenti digitali possano amplificare dinamiche di controllo e abuso. È attiva a livello aziendale in progetti internazionali di cybersecurity e svolge attività di formazione e prevenzione nelle scuole, promuovendo una cultura del consenso e decostruendo gli stereotipi di genere. Dal 2020 fa parte del team di PermessoNegato e dal 2024 è responsabile dell'area formazione.

Ilaria Lavarini, laureata in Psicologia Clinica e Dinamica, con pluriennale esperienza nell'ambito del disagio socio-economico e psicologico. Ha collaborato con realtà come Caritas Italiana, la Casa Internazionale delle Donne di Roma e CAV (centri antiviolenza), operando nella tutela dei soggetti più vulnerabili. Dal 2022 è volontaria di PermessoNegato. Attualmente, sta ampliando le sue competenze con un Master in Risorse Umane HR *Management & Innovation*.

Matilde Bellingeri, avvocato penalista del foro di Milano. Dal 2021 al 2025 ha fatto parte del team legale di PermessoNegato. Parallelamente all'attività forense, si dedica alla formazione giuridica presso istituti scolastici di secondo grado, contribuendo alla diffusione della cultura della legalità tra i più giovani. Attualmente è dottoranda di ricerca in Diritto Penale presso l'Università degli Studi di Verona.

Noemi Tentori, laureata in Sicurezza dei Sistemi e delle Reti Informatiche, si occupa di cyber-security, antifraud e business continuity management in ambito aziendale. Dal 2021 è volontaria di PermessoNegato, attraverso cui si occupa anche di prevenzione ed educazione all'uso delle nuove tecnologie all'interno degli istituti scolastici. Appassionata di *Open Source Intelligence*, i suoi interessi personali si spostano anche su argomenti quali la reputazione dell'individuo online, il trattamento dei dati sensibili mezzo Internet e l'*hate speech*.

Citazione consigliata: Beckman, E. M., Lavarini, I., Bellingeri, M., & Tentori, N. (2025, maggio). *"Rispondimi velocemente": Analisi multidisciplinare della sextortion maschile in Italia*

INDICE

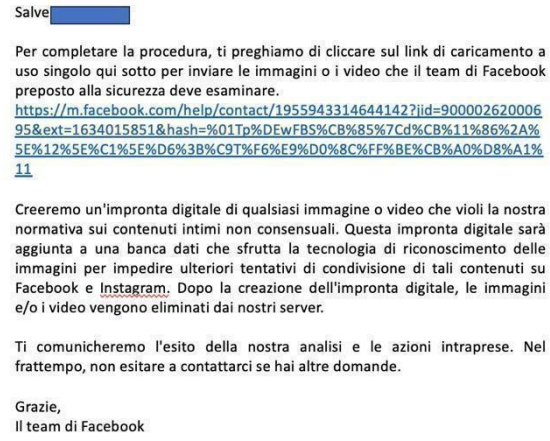
PERMESSONEGATO

PermessoNegato è un'organizzazione non-profit fondata a Milano alla fine del 2019, con l'obiettivo di offrire supporto alle vittime di condivisione non consensuale di materiale intimo, un reato che negli ultimi anni ha acquisito sempre maggiore visibilità e gravità. Fin dalla sua nascita, PermessoNegato si è distinta come una delle principali realtà nazionali ed internazionali impegnate in questo campo, rispondendo alle esigenze delle vittime con un **approccio multidisciplinare** che combina supporto tecnologico, legale e psicologico. Ad oggi, l'organizzazione ha assistito **oltre 4.000 vittime**, creando un network di professionisti qualificati per aiutare le persone a rimuovere contenuti intimi diffusi senza il loro consenso, proteggendo la loro reputazione online e fornendo un supporto gratuito e immediato. Le vittime contattano PermessoNegato da tutto il mondo e, per rispondere a queste esigenze globali, questa realtà offre supporto in diverse lingue, garantendo un aiuto accessibile a chiunque ne abbia bisogno, indipendentemente dalla loro provenienza. La diffusione non consensuale di materiale intimo è un reato di natura complessa che necessita di un intervento integrato per essere affrontato adeguatamente. Per questo motivo, il team di PermessoNegato è composto da esperti con diverse formazioni professionali, tra cui avvocati, psicologi, criminologi, esperti di reputazione online e sicurezza informatica.

I principali servizi offerti dall'organizzazione, comprendono:

1. **Rimozione preventiva:** PermessoNegato è stata la prima associazione in Europa ad attivare il servizio di rimozione preventiva, un'iniziativa che ha permesso alle vittime o potenziali tali di caricare i propri contenuti intimi attraverso un *link*, fornito all'associazione da Facebook, e in seguito condiviso da PermessoNegato con la persona interessata. Qualora questi contenuti fossero stati pubblicati su Facebook e Instagram, sarebbero stati automaticamente rimossi, e sarebbe stato impossibile caricarli nuovamente. A partire dal 2023, le vittime e le potenziali vittime vengono reindirizzate ai siti **Stop.NCII** per gli adulti e **Take it Down** per i minorenni; entrambi i portali permettono di avviare autonomamente la procedura di rimozione preventiva. La principale novità è l'adesione di molte piattaforme all'iniziativa, che permette una copertura molto più ampia in caso di pubblicazione non consensuale di contenuti intimi. Il processo, che ricalca quello adottato precedentemente, inizia con la selezione, dal proprio dispositivo, delle immagini o dei video intimi per i quali si desidera calcolare l'*hashing*. Successivamente, StopNCII.org genera un'impronta digitale, chiamata "*hash*", per ciascuno di essi. È importante sottolineare che solo l'*hash* viene inviato al sito, mentre il contenuto originale rimane intatto e non viene caricato online. Una volta completata con successo la registrazione del caso, l'utente riceve un numero identificativo, che consente di monitorare lo stato della richiesta. Le società aderenti al

programma confrontano l'*hash* con i loro sistemi e, nel caso in cui vengano trovate corrispondenze, procedono con la rimozione dei contenuti.



Salve [redacted]

Per completare la procedura, ti preghiamo di cliccare sul link di caricamento a uso singolo qui sotto per inviare le immagini o i video che il team di Facebook preposto alla sicurezza deve esaminare.
https://m.facebook.com/help/contact/1955943314644142?iid=900002620006 95&ext=1634015851&hash=%01Tp%DEwFBS%CB%85%7Cd%CB%11%86%2A% 5E%12%5E%C1%5E%D6%3B%C9T%F6%E9%D0%8C%FF%BE%CB%A0%D8%A1% 11

Creeremo un'impronta digitale di qualsiasi immagine o video che violi la nostra normativa sui contenuti intimi non consensuali. Questa impronta digitale sarà aggiunta a una banca dati che sfrutta la tecnologia di riconoscimento delle immagini per impedire ulteriori tentativi di condivisione di tali contenuti su Facebook e Instagram. Dopo la creazione dell'impronta digitale, le immagini e/o i video vengono eliminati dai nostri server.

Ti comunicheremo l'esito della nostra analisi e le azioni intraprese. Nel frattempo, non esitare a contattarci se hai altre domande.

Grazie,
Il team di Facebook

Fig.1: Procedura utilizzata fino al 2022

Fig. 2: Piattaforma StopNCII.org per i maggiorenni

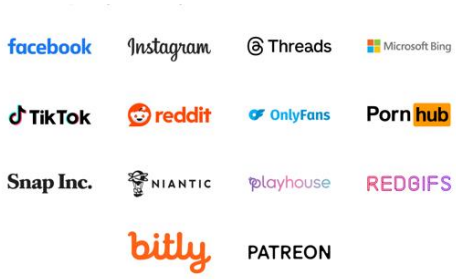


Fig.3: Partner aderenti a StopNCII.org

Fig. 4: Piattaforma Take it Down per i minorenni

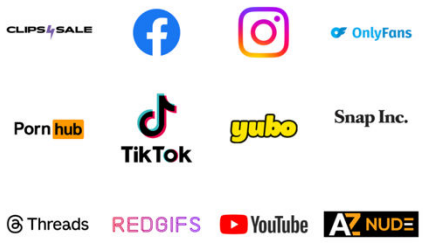


Fig. 5: Partner aderenti a Take it Down

2. **Rimozione di contenuti già pubblicati e segnalazione account**: Nel contrasto alla diffusione illecita di contenuti intimi già pubblicati online, l'associazione si impegna attivamente nella segnalazione degli stessi alle piattaforme digitali, richiedendone l'immediata rimozione dei link forniti dalle vittime. PermessoNegato ha costruito, nel

tempo, una rete di collaborazione efficace anche con numerose piattaforme di contenuti per adulti, riuscendo a ottenere risultati significativi soprattutto grazie alla partnership con Aylo, uno dei principali attori del settore. Purtroppo, molti siti porno (soprattutto quelli non moderati o poco regolamentati) possono diventare terreno fertile per la diffusione di questo tipo di contenuti, alimentando dinamiche di violenza, ricatto e umiliazione pubblica. Per questo motivo, si ritiene fondamentale non solo agire a posteriori con la rimozione, ma anche lavorare in sinergia con le piattaforme per promuovere una maggiore responsabilità nella gestione e nel controllo dei materiali caricati dagli utenti. Una parte fondamentale del lavoro dell'associazione consiste nell'intervenire attivamente per **segnalare** (principalmente a Meta) **gli account che diffondono contenuti illeciti o che minacciano di farlo**, chiedendone la disabilitazione immediata.

3. **Orientamento legale e cautelamento forense:** L'associazione offre a ciascuna vittima un colloquio legale gratuito con uno degli Avvocati del team, che non potrà rappresentare la persona in giudizio, ma la guiderà durante un primo momento di orientamento che si è spesso rivelato fondamentale per le persone che si rivolgono a PermessoNegato. Questo confronto aiuta a **chiarire i propri diritti**, comprendere i passi successivi dal punto di vista legale e superare i timori legati a una possibile **seconda vittimizzazione**, un'esperienza purtroppo comune tra chi subisce violenza digitale. Nel caso in cui la persona decida di avviare un percorso legale, PermessoNegato fornisce un supporto anche per l'attivazione del cautelamento forense, un servizio utile a **certificare legalmente la presenza online di contenuti illeciti o diffamatori** tramite una procedura riconosciuta a livello giuridico. Questo passaggio è importante per tutelarsi e raccogliere prove valide in sede giudiziaria. Il servizio è reso possibile grazie alla collaborazione con partner esterni specializzati.

4. **Supporto psicologico:** Infine, sempre attraverso i nostri partner, l'associazione mette a disposizione un servizio di supporto psicologico gratuito, per chiunque senta il bisogno di un aiuto professionale nel gestire l'impatto emotivo dell'esperienza vissuta.

PermessoNegato collabora con importanti aziende e piattaforme globali per offrire un supporto concreto alle vittime di condivisione non consensuale di materiale intimo. Tra i partner principali figurano Meta (proprietaria di Facebook, Instagram e WhatsApp), Aylo (proprietario di piattaforme per adulti, come ad esempio Pornhub), TikTok e Google. Queste collaborazioni permettono all'organizzazione di ottenere un intervento tempestivo e diretto per rimuovere i contenuti dannosi e di sensibilizzare l'opinione pubblica sull'importanza di tutelare la privacy e la dignità delle persone online.

LA CONDIVISIONE NON CONSENSUALE DI MATERIALE INTIMO

La condivisione non consensuale di materiale intimo, spesso definita erroneamente *Revenge Porn*, identifica la diffusione di immagini o video intimi, destinati a rimanere privati, senza il consenso delle persone rappresentate. In Italia il reato è disciplinato ai sensi dell'**articolo 612-ter del Codice Penale**. È importante chiarire che il termine *Revenge Porn* è limitante e impreciso, poiché suggerisce che il fenomeno sia sempre legato a una sorta di vendetta (traduzione appunto della parola inglese *revenge*), mentre in realtà può coinvolgere molteplici motivazioni, tra cui la coercizione, la manipolazione psicologica, l'estorsione e il semplice desiderio di umiliare o danneggiare qualcuno. Il termine *Revenge Porn* non è solo limitante, ma anche fuorviante. Non tutte le vittime sono coinvolte in dinamiche di vendetta, e spesso non si tratta di un fenomeno legato esclusivamente alle relazioni intime o a una rottura sentimentale. Utilizzare la corretta terminologia "Condivisione non consensuale di materiale intimo" o *Image-Based Sexual Abuse* in inglese, aiuta a riconoscere la gravità del crimine e a **evitare di ridurre e banalizzare l'esperienza della vittima**. Questo tipo di linguaggio è più adeguato a sottolineare la natura violenta e lesiva del reato, che può avere un impatto devastante sulla vita delle persone coinvolte. Un altro fenomeno parte della condivisione non consensuale di materiale intimo è la ***sextortion***, che si identifica con la minaccia di diffondere contenuti intimi per **estorcere denaro, beni o altri favori (spesso di natura sessuale) dalle vittime**. La *sextortion* è perpetrata tramite internet e social media, dove gli autori delle minacce ottengono materiale compromettente (ad esempio, foto o video intimi) e usano tale materiale minacciando le vittime di pubblicarlo online e/o inviarlo a familiari e amici, se non ottengono quanto richiesto. Negli ultimi anni, PermessoNegato ha riscontrato un **aumento significativo** del numero di **vittime di sesso maschile** coinvolte in casi di *sextortion*. Questo ha evidenziato la necessità di maggiori studi e analisi sul fenomeno, non solo da un punto di vista statistico, ma anche legale, psicologico e criminologico.

LIMITI DELLA RICERCA

Nel presente report si è scelto di esplorare principalmente il fenomeno delle **vittime di sesso maschile di *sextortion***, un gruppo che, come verrà evidenziato, è stato tradizionalmente poco studiato, sia in Italia che all'estero. Per motivi di tutela della privacy e della sicurezza delle vittime, quando queste contattano PermessoNegato chiedendo supporto, vengono raccolti solo i dati strettamente necessari per offrire aiuto immediato e mirato. Di conseguenza, molte informazioni potenzialmente utili agli scopi della ricerca, come dettagli specifici sul *modus operandi* dei criminali, i profili psicologici delle vittime, o le caratteristiche precise dei contesti in cui si verificano i reati, risultano ad oggi sconosciuti. Questa decisione di limitare la raccolta di dati deriva dalla necessità di proteggere le vittime da ulteriori traumi psicologici e rischi legati alla divulgazione non necessaria delle loro informazioni personali. Infatti, molte delle persone

che si rivolgono a PermessoNegato lo fanno in uno stato di **panico, vergogna e vulnerabilità**, rendendo essenziale rispettare il loro desiderio di anonimato e riservatezza. A causa di questa restrizione, molte variabili, cruciali per una comprensione approfondita e per una più completa analisi del fenomeno, rimangono ad oggi parzialmente inesplorate.
Infatti, in questo momento, non esistono ricerche significative in Italia e le indagini internazionali sul tema sono limitate[1]. La scarsità di dati e studi specifici rende particolarmente difficile tracciare un quadro preciso dell'entità e delle caratteristiche di questo fenomeno nel contesto globale. Tale mancanza di letteratura può rappresentare una barriera nella comprensione della portata del problema, e nella creazione di politiche preventive e di supporto adeguate. Un'altra limitazione significativa riguarda la sottostima dei dati sui reati a sfondo sessuale in generale. Il numero di casi denunciati è sempre inferiore rispetto alla reale incidenza di tali reati, in gran parte a causa della mancanza di denuncia da parte delle vittime, che spesso non si sentono in grado di farsi avanti per motivi legati alla paura, alla vergogna o al timore di non essere credute. Questa sottostima rende più complessa l'analisi del fenomeno, poiché i dati raccolti non rappresentano l'intero universo delle vittime di questa tipologia di reati.

Anonimizzazione dei dati e natura del campione

Le informazioni analizzate in questo report provengono esclusivamente dalle segnalazioni ricevute da PermessoNegato. Si tratta di un campione auto-selezionato, costituito da vittime che hanno contattato spontaneamente l'associazione in cerca di supporto. Di conseguenza, i dati raccolti non possono essere considerati rappresentativi dell'intera popolazione maschile colpita dal fenomeno; offrono tuttavia uno **spaccato significativo**, utile per evidenziare tendenze emergenti, criticità ricorrenti e bisogni ancora inascoltati.
Fin dal primo momento, tutte le informazioni sono state anonimizzate, senza mai raccogliere dati personali identificativi. L'intero processo è stato condotto nel massimo rispetto della riservatezza delle vittime e in conformità con il Regolamento Generale sulla Protezione dei Dati (**GDPR – Regolamento UE 2016/679**). L'obiettivo non è mai stato tracciare profili individuali, ma comprendere il fenomeno nella sua complessità, mantenendo sempre al centro la tutela e la dignità delle persone coinvolte.
In questa ricerca sono stati inseriti anche *screenshot* anonimizzati, forniti direttamente dalle vittime al momento della segnalazione. Tutti gli elementi identificativi sono stati rimossi con estrema cura e i materiali vengono utilizzati esclusivamente a fini di studio e analisi, garantendo il pieno rispetto della privacy e della sicurezza delle persone rappresentate.
Pur mantenendo la protezione delle vittime come priorità assoluta, PermessoNegato riconosce l'importanza, per il futuro, di estendere la raccolta dati in modo più sistematico.

[1] Per ulteriori approfondimenti: *R.J. Notté, Exploring the impact of sextortion on adult males: A narrative approach, Technology in Society, Volume 78, 2024*

Migliorare le pratiche di supporto e creare un ambiente ancora più sicuro e rassicurante potrà favorire la raccolta di informazioni più ampie e dettagliate. Questo permetterà di monitorare meglio l'evoluzione del fenomeno, comprenderne più a fondo le dinamiche e sviluppare strategie di intervento ancora più efficaci. Ogni eventuale ampliamento nella raccolta dati sarà comunque sempre guidato dal rispetto rigoroso della privacy e del benessere delle vittime, che continueranno a rappresentare il fulcro di ogni azione.

PROFILI LEGALI

Con il termine *sextortion*, da un punto di vista giuridico, ci si vuole riferire alla condotta attraverso la quale il soggetto agente prospetta alla vittima la rivelazione di notizie o la propalazione di immagini di natura sessuale, lesive della sua dignità, della sua reputazione o del suo diritto alla riservatezza, in modo da costringerla a fare o non fare qualcosa.
Le modalità attraverso le quali può estrinsecarsi la condotta sono le più diverse, generalmente si possono distinguere casi in cui le immagini sono acquisite mediante un'attività di *hacking* (il cyber-criminale effettua un accesso non autorizzato al sistema informatico in uso alla vittima, prelevando dal suo computer o dal altri dispositivi o servizi di cloud storage immagini o video sessualmente espliciti), da casi in cui le condotte di *sextortion* vedono un maggior coinvolgimento della vittima sin dalle sue prime fasi.
Nella prima ipotesi, la vittima viene contattata dal cyber-criminale solo al fine di essere ricattata con le immagini ottenute, generalmente attraverso e-mail o messaggi dal contenuto minatorio con richiesta di pagamento per evitare il caricamento online dei file multimediali.
Nella seconda, il cyber-criminale con l'obiettivo di procurarsi le rappresentazioni multimediali della vittima instaura con essa un rapporto confidenziale, adescandola in spazi virtuali quali social network, chat e siti di *dating*, attraverso un profilo falso creato ad hoc. Come si vedrà più avanti, il tema sessuale viene introdotto in maniera graduale in modo da sensibilizzare la vittima e indurla a scambiare informazioni personali e immagini sessualmente esplicite o a contenuto intimo, le quali saranno successivamente oggetto della condotta estorsiva.

Il reato di *sextortion* in Italia

Tale reato **non esiste nel nostro ordinamento giuridico**. La condotta descritta astrattamente può ricadere, a seconda delle modalità specifiche con le quali viene commessa, entro il perimetro di alcuni reati previsti dal Codice penale (art. 629 c.p. - estorsione, art. 595 c.p. - diffamazione, art. 615 bis c.p. - interferenze illecite nella vita privata, art. 610 c.p. - violenza privata, art. 612 c.p. - minacce).
Generalmente, tale fenomeno viene ricondotto nell'ambito del **reato di estorsione**, la cui condotta tipica consiste nel costringere qualcuno mediante violenza o minaccia *"a fare o ad omettere qualcosa"*. Il reato di estorsione è un delitto posto a tutela del patrimonio e della

libertà morale del soggetto passivo. Quando la condotta estorsiva rientra nell'ambito della c.d. *sextortion*, oltre al patrimonio e alla libertà morale della persona offesa dal reato, vengono violati il diritto all'identità personale, alla riservatezza e alla protezione dei dati personali.
Ai fini della sua configurabilità, tale reato deve necessariamente essere commesso mediante violenza o minaccia. L'evento del delitto è costituito dai quattro seguenti elementi:

- lo stato altrui di coazione psichica,
- l'atto di disposizione del soggetto passivo (il *"fare"* o *"omettere"* qualcosa),
- il danno arrecato alla vittima,
- profitto ingiusto, proprio o altrui.

L'elemento oggettivo del reato: la condotta estorsiva

Valutando la limitata casistica giurisprudenziale, unitamente ai dati di PermessoNegato, si può notare che il delitto di estorsione (nella sua forma di *sextortion*) viene prevalentemente commesso ponendo in essere una violenza psicologica nei confronti della vittima, attraverso la prospettazione di un male futuro, ovverosia la minaccia di subire la diffusione di immagini o video di natura intima (o di informazioni strettamente personali).
La minaccia può assumere qualsiasi forma purché sia concretamente idonea a costringere la vittima a compiere l'atto di disposizione. Essa può essere manifestata anche tramite mezzi di comunicazione a distanza, inclusi i sistemi informatici.
Un caso di *sextortion* online giunto alla Corte di Cassazione è quello descritto nella sentenza del 5 novembre 2016, n. 6017[2], dove l'imputato è stato ritenuto responsabile della commissione di più delitti di tentata estorsione, per aver cercato di ottenere il pagamento di una somma di denaro da parte della persona offesa prospettandole, attraverso messaggi di posta elettronica, di rendere pubblica la loro relazione omosessuale.

La condotta estorsiva deve essere tale da provocare nella vittima uno **stato psicologico di coazione**, ossia una significativa limitazione della sua libertà morale. Nel caso specifico della *sextortion* è difficile immaginare casi concreti in cui si possa negare l'idoneità coercitiva della minaccia di diffusione di immagini o video di natura intima. A ciò si aggiunga che, come noto, ogni interazione via *social network* o tramite sito web si rivolge, per definizione, ad una platea potenzialmente infinita di destinatari, con la conseguenza che il contenuto compromettente immesso online diviene sostanzialmente ineliminabile. Non solo la cancellazione di un dato da un sito internet non è facile da effettuare, ma può risultare addirittura inefficace se si considera che ogni dato può essere riprodotto in altri siti o nelle memorie cache per esigenze tecniche, e può comunque essere rintracciato, oppure essere stato copiato/salvato da altro utente, a sua volta in grado di immetterlo nuovamente in rete in qualsiasi momento.

[2] La sentenza è disponibile al seguente sito web: www.personaedanno.it

Ai fini della configurazione del reato la coazione psicologica (la minaccia) deve indurre la vittima a "*fare o ad omettere qualcosa*". L'atto di disposizione della vittima deve provocare **un ingiusto profitto** per l'autore della condotta, o per altri, con relativo danno economico per la vittima (o per altri soggetti). L'elemento dell'ingiusto profitto deve consistere in una qualunque utilità o vantaggio che l'autore intende conseguire, anche di natura non patrimoniale, il quale deve essere ingiusto, ovvero basato su una pretesa non tutelata dall'ordinamento, né direttamente né indirettamente.

Il danno conseguente deve essere stato provocato dall'atto di aver fatto o omesso qualcosa e deve assumere un contenuto patrimoniale, anche indiretto, ovvero comportare un qualche tipo di diminuzione economica o l'inutilizzabilità di una cosa (purché apprezzabile da un punto di vista patrimoniale). A titolo di esempio si consideri che in una sua decisione la Corte di Cassazione (Cass. pen. n. 44408/2016) ha ritenuto configurato il delitto di tentata estorsione nella condotta di un soggetto che aveva minacciato la vittima del reato di divulgare un video hard che la ritraeva, se non si fosse dimessa dall'incarico di assessore comunale, in modo da consentire all'agente, quale primo dei candidati non eletti, di subentrargli nel consesso comunale. In tal caso il danno economico è stato ritenuto di tipo indiretto ovverosia consistente nella perdita di compensi o indennità legate alla carica ricoperta. Una recente pronuncia della Corte di Cassazione (Cass. pen. n. 14075/2025) ha condiviso l'orientamento citato, stabilendo che l'elemento dell'ingiusto profitto debba essere individuato in qualsiasi vantaggio, non solo di tipo economico, che l'autore del reato intenda conseguire, non collegato ad un diritto.

L'elemento soggettivo del reato e il momento della consumazione

Il reato di estorsione è punito a titolo di dolo generico. Ciò significa che, ai fini della condanna, deve essere raggiunta la prova del fatto che il soggetto agente avesse la piena coscienza e volontà di costringere un'altra persona a compiere un atto di disposizione patrimoniale, con danno altrui e un conseguente ingiusto profitto per sé stesso (o per altri soggetti).
Il delitto si configura nel momento e nel luogo in cui si realizzano gli eventi del profitto ingiusto con altrui danno. Per quanto riguarda l'estorsione sessuale commessa con modalità informatiche, si pongono questioni peculiari in tutti i casi in cui il pagamento, che rappresenta il profitto ingiusto con altrui danno, avviene tramite procedure telematiche (es. bonifico, utilizzo di carta di credito, moneta elettronica, carta prepagata). In questi casi si ha un intervallo temporale e spaziale tra l'evento del profitto e quello del danno, con le relative difficoltà di individuazione del momento e del luogo di commissione del reato.

La questione è dibattuta. Se, da un lato, secondo una pronuncia del Tribunale di Perugia (Trib. Perugia, 26 giugno 2017[3]) in via di principio, la competenza territoriale si dovrebbe radicare nel luogo in cui l'agente consegue il profitto, cioè nel luogo di effettiva riscossione o spendita della somma accreditata. D'altro lato l'orientamento condiviso nella citata sentenza non è univoco. Altre pronunce successive (si veda, per tutti Cass. pen. n. 491954/2019[4]) affermano il principio secondo il quale nel delitto di truffa, quando il profitto è conseguito mediante accredito su carta di pagamento ricaricabile, nella specie "postepay", il tempo e il luogo di consumazione del reato sono quelli in cui la persona offesa ha provveduto al versamento del denaro sulla carta. Pertanto, ai fini della competenza per territorio dell'organo giudicante, si deve considerare il luogo in cui la vittima ha effettuato il pagamento.
Si segnala altresì che se il pagamento dovesse avvenire tramite bonifico ordinario (ipotesi sostanzialmente estranea alla casistica di PermessoNegato), allora la competenza sarebbe quella del Giudice del luogo ove avverrebbe l'accredito del denaro, in quanto non vi sarebbe contemporaneità tra lo spoglio e l'impossessamento.

Normative internazionali

Si è visto come in Italia la sextortion non è ancora riconosciuta come reato autonomo, ma viene perseguita attraverso una combinazione di norme esistenti, come l'estorsione, la violazione della privacy e la diffusione illecita di materiale intimo. Questa frammentazione normativa può rendere più complessa la denuncia e la qualificazione giuridica del reato.
Al contrario, alcuni paesi hanno adottato approcci più specifici:

- **Filippine:** la *Cybercrime Prevention Act* (Republic Act No. 10175) del 2012 affronta i crimini informatici, inclusi quelli a sfondo sessuale. Sebbene non menzioni esplicitamente la "sextortion", le sue disposizioni coprono comportamenti simili, come l'estorsione online e la diffusione non consensuale di materiale intimo.
- **Stati Uniti:** a livello federale, non esiste una legge specifica sulla sextortion, ma diversi stati hanno introdotto normative pertinenti. Ad esempio, in California, il ***Penal Code § 647j(4)*** criminalizza la diffusione non consensuale di immagini intime, noto come "revenge porn", che può includere casi di sextortion. In Texas, il ***Penal Code § 16.05*** punisce la divulgazione illegale di comunicazioni elettroniche, applicabile in contesti di sextortion.
- **Canada:** il codice penale canadese è stato aggiornato per includere reati come la distribuzione non consensuale di immagini intime. Un caso recente ha visto la

[3] Per maggiori approfondimenti: https://archiviodpc.dirittopenaleuomo.org/pdf-viewer/?file=%2Fpdf-fascicoli%2FDPC_2_2018.pdf#page=216
[4] Per maggiori approfondimenti: https://www.giurisprudenzapenale.com/wp-content/uploads/2019/07/cass-pen-ssuu-2019-28911.pdf

condanna di un uomo per aver estorto immagini sessualmente esplicite a un minore, evidenziando l'applicazione efficace di queste leggi[5].

L'introduzione di un **reato specifico di sextortion in Italia** potrebbe offrire numerosi vantaggi:

- **chiarezza giuridica:** una definizione precisa aiuterebbe le vittime a comprendere meglio i propri diritti e le modalità di denuncia;
- **raccolta dati:** consentirebbe una raccolta più accurata di statistiche, fondamentale per sviluppare politiche di prevenzione efficaci, oltreché la creazione di una casistica giurisprudenziale dedicata;
- **sensibilizzazione:** permetterebbe al fenomeno di diventare più visibile, contribuendo a ridurre lo stigma associato, soprattutto tra le vittime che spesso esitano a denunciare.
- **protezione delle vittime:** fornirebbe strumenti legali più adeguati per proteggere tutte le vittime e per perseguire efficacemente i colpevoli

I MEZZI DI ACQUISIZIONE DELLA PROVA

Prima di procedere con la denuncia-querela, è di fondamentale importanza raccogliere le evidenze che possano sostenere la sussistenza del reato prima che il materiale venga rimosso dalla rete, seppur questo potrebbe essere emotivamente doloroso per la vittima.

L'acquisizione forense

L'entrata in vigore della legge 48/2008[6] ha rappresentato un passo fondamentale per l'adeguamento del sistema processual-penalistico italiano agli standard europei in materia di raccolta, conservazione e utilizzo delle prove digitali.
In particolare, l'art. 8 della suddetta legge stabilisce che l'autorità giudiziaria può disporre l'acquisizione di informazioni contenute in un sistema informatico o telematico *"adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"*. Ciò nella convinzione che, qualora la fase dell'acquisizione e quella della conservazione siano improntate a **regole uniformi e rigorose**, nella successiva fase di valutazione da parte del giudice, gli elementi di prova raccolti potranno essere considerati **idonei a provare i fatti della causa**. La copia che viene prodotta seguendo questi specifici protocolli prende il nome di **copia forense** ed è tipicamente effettuata da esperti forensi digitali o professionisti accreditati, ma in alcuni casi, possono essere coinvolti anche enti giuridici o altre figure professionali, a seconda della giurisdizione e della natura dell'indagine.

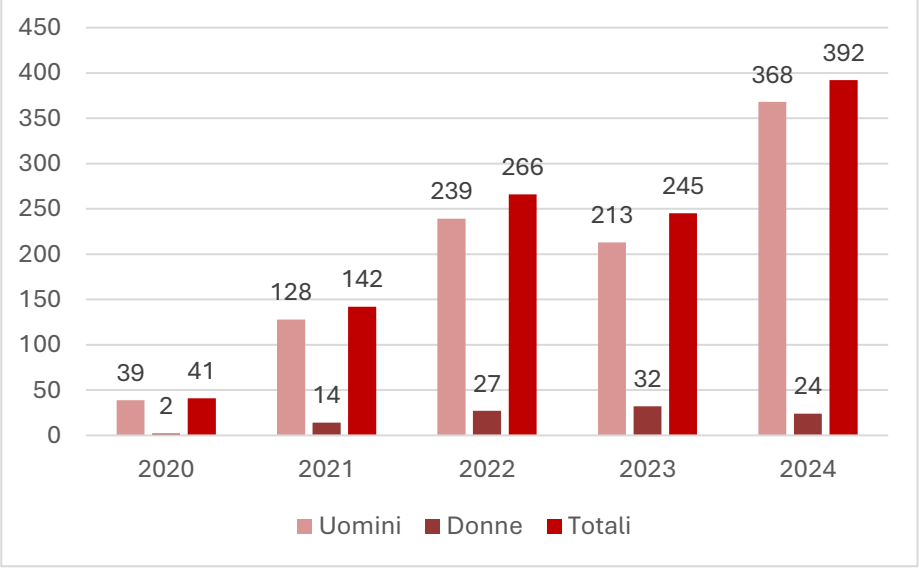
[5] https://www.sfchronicle.com/crime/article/sextortion-sentence-contra-costa-20055506.php
[6] https://www.parlamento.it/parlam/leggi/08048l.htm

La valenza probatoria degli *screenshot*

La modalità più immediata e alla portata dell'utilizzatore medio di un dispositivo elettronico, rimane tuttavia la cattura dello schermo del computer o dello smartphone (*screenshot*).
La Corte di Cassazione, con la recente pronuncia n. 34212/2024, ha confermato l'orientamento giurisprudenziale secondo cui gli *screenshot* hanno pieno valore di prova in giudizio. Ciò, in quanto, uno *screenshot* è idoneo a catturare l'esatto momento in cui il messaggio viene ricevuto o l'immagine viene inviata, garantendo in tal modo la prova della sua esistenza e del suo contenuto. Si segnala che in caso di dubbio sulla autenticità dello *screenshot* il Giudice può disporre il sequestro del cellulare (dell'imputato o della persona offesa) per permettere le dovute verifiche tecniche. Fondamentale dunque è la conservazione delle chat nella memoria del proprio dispositivo e, per una sicura conservazione a lungo periodo, si suggerisce il salvataggio anche su un supporto esterno. Se si conserva il file originale lo stesso non potrà essere oggetto di facili contestazioni dibattimentali.

I DATI

Il presente studio si basa sui dati raccolti dall'associazione nel periodo compreso tra **gennaio 2020 e dicembre 2024**, riguardanti il numero di **vittime di *sextortion* italiane**[7] **e non** che si sono rivolte a PermessoNegato per chiedere supporto. Tali dati documentano un **totale di 1.086 casi**, partendo da 41 registrati nel 2020 fino ad arrivare a 392 nel 2024, con un progressivo incremento (fatta eccezione per il 2023 durante il quale è stato registrato un leggero calo), a conferma di un fenomeno che, nel corso degli anni, ha mostrato una costante espansione.



[7] Con vittime italiane si intendono le persone che hanno contattato l'associazione e interagito lingua italiana

Fig.6: Vittime di Sextortion che hanno contattato PermessoNegato nel quadriennio

Fig.7: Genere e nazionalità

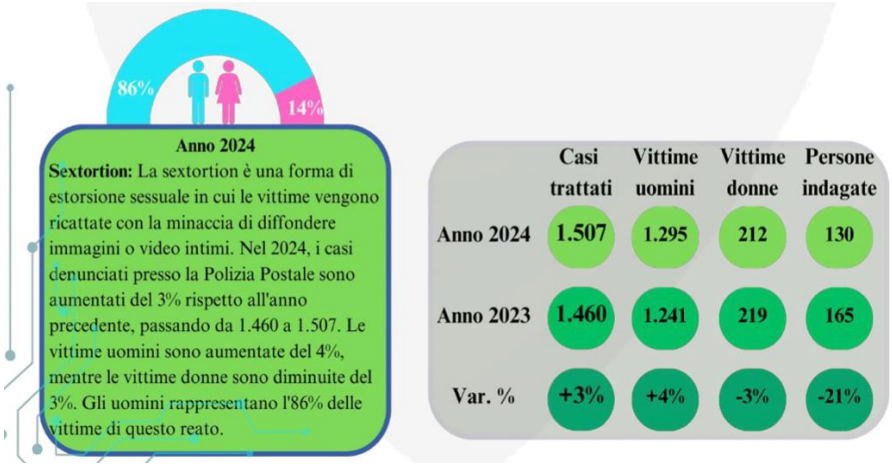
Uno degli obiettivi primari della ricerca è **sensibilizzare** l'opinione pubblica sull'aumento delle vittime di sesso maschile di *sextortion* e sul reato in generale. Sebbene il fenomeno della condivisione non consensuale di materiale intimo sia storicamente associato in modo predominante alle donne, i dati raccolti suggeriscono un incremento significativo anche tra gli uomini nei soli casi specifici di *sextortion*.

È fondamentale sottolineare come, nel caso della *sextortion* online, il **quadro tradizionale cambi radicalmente**. I dati raccolti da PermessoNegato, insieme ad altre fonti come i report della Polizia Postale, evidenziano una netta inversione rispetto ai reati di condivisione non consensuale più "classici": la grande maggioranza delle vittime di *sextortion* è costituita da uomini. Si tratta di una differenza marcata e non marginale, che impone di ripensare approcci e strategie di intervento. Nonostante questo mutamento specifico, resta comunque vero che, nel complesso dei crimini legati alla diffusione non consensuale di materiale intimo, le donne continuano a rappresentare la quasi totalità delle vittime.
Diversi studi[8] confermano che il genere femminile rimane, nella maggior parte dei casi, il bersaglio principale di queste forme di violenza, e che questo dato, purtroppo, non mostra segni di inversione. Il genere dunque si conferma come una variabile determinante, con profonde implicazioni per le politiche di prevenzione, sensibilizzazione e supporto alle vittime.
Un ulteriore elemento che emerge dalla ricerca è l'urgenza di potenziare le attività di prevenzione, specialmente in un contesto in cui l'uso dei social media si diffonde in fasce di età sempre più giovani, come verrà approfondito nei paragrafi successivi.

Uno degli aspetti che più colpisce nell'analisi dei casi di *sextortion* è la **difficoltà nell'identificare un target specifico di vittime**, oltre all'aumento dei casi di vittime di sesso

[8] Per approfondimenti sul tema:
1. European Institute for Gender Equality: https://eige.europa.eu/mk
2. Revenge Porn Helpline: https://revengepornhelpline.org.uk
3. Report sulla condivisione non consensuale di materiale intimo: https://www.permessonegato.it/wp-content/uploads/2024/09/PermessoNegato_IBSA2023_Report_ITA.pdf

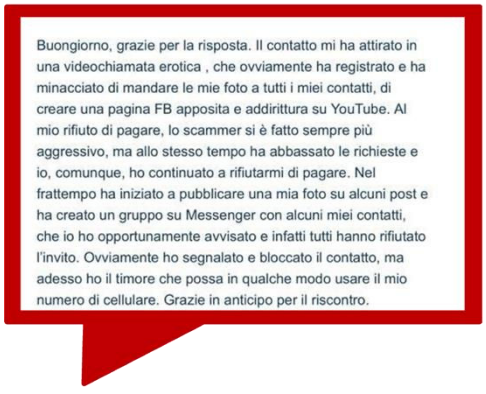
maschile**.** L'esperienza maturata negli anni mostra con chiarezza come non esista un unico profilo riconoscibile: PermessoNegato è stata contattata da persone di età molto diverse, (escludendo i minori, **dai 18 fino ai 75 anni**), senza una prevalenza marcata in una fascia anagrafica rispetto a un'altra. Le vittime provengono da contesti sociali, culturali e geografici eterogenei, appartengono a differenti orientamenti sessuali, sono italiane e straniere, sposate, conviventi, single o in situazioni relazionali complesse. Alcune di loro avevano familiarità con l'uso dei social media e delle tecnologie digitali, altre molto meno. Questa varietà di profili ci restituisce un **quadro estremamente diversificato**, che rende evidente la natura trasversale del fenomeno. Il fenomeno della *sextortion* si configura dunque come un reato non legato a una categoria ristretta di individui, ma come una minaccia potenzialmente rivolta a chiunque faccia uso, anche occasionale, di strumenti digitali. Questa caratteristica rappresenta una sfida importante, non solo dal punto di vista della prevenzione, ma anche rispetto alla costruzione di strumenti di supporto efficaci, capaci di rispondere ai bisogni di vittime molto diverse tra loro per età, esperienze, sensibilità e risorse personali.



Fonte: Report annuale 2024 della Polizia Postale e per la Sicurezza Cibernetica[9]

LE FASI DELL'ADESCAMENTO

Nel corso degli anni sono stati individuati alcuni schemi ricorrenti che possono essere visti come un processo strutturato che segue una serie di fasi predeterminate, ognuna delle quali mira a manipolare progressivamente il bersaglio, creando una **relazione virtuale di fiducia** che permette di giungere al fine desiderato: il ricatto. Dai racconti delle persone che si sono messe in contatto con l'associazione, sono state individuate diverse fasi seguite durante l'adescamento:


Buongiorno, grazie per la risposta. Il contatto mi ha attirato in una videochiamata erotica , che ovviamente ha registrato e ha minacciato di mandare le mie foto a tutti i miei contatti, di creare una pagina FB apposita e addirittura su YouTube. Al mio rifiuto di pagare, lo scammer si è fatto sempre più aggressivo, ma allo stesso tempo ha abbassato le richieste e io, comunque, ho continuato a rifiutarmi di pagare. Nel frattempo ha iniziato a pubblicare una mia foto su alcuni post e ha creato un gruppo su Messenger con alcuni miei contatti, che io ho opportunamente avvisato e infatti tutti hanno rifiutato l'invito. Ovviamente ho segnalato e bloccato il contatto, ma adesso ho il timore che possa in qualche modo usare il mio numero di cellulare. Grazie in anticipo per il riscontro.

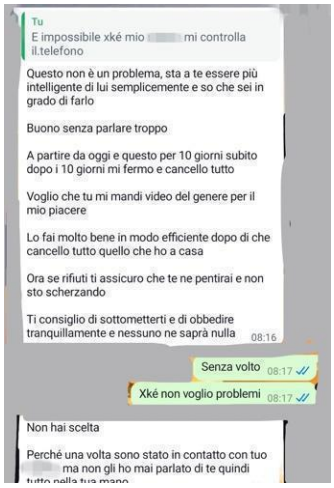
[9] https://www.poliziadistato.it/statics/40/2024-report-def.-sppsc.pdf

1. **Creazione del primo contatto,** che solitamente avviene tramite piattaforme di social media, chat online, o anche applicazioni di incontri. Questo momento si basa principalmente sulla costruzione di una **relazione apparentemente genuina**, che mira a stabilire un collegamento iniziale tra il truffatore e la vittima. Questo tipo di approccio consiste nel presentarsi come una persona affidabile, comprensiva, e interessata al benessere della vittima. Le domande iniziali sono quindi focalizzate su aspetti personali generici, che spesso vanno a **carpire informazioni sensibili** dalla vittima, come dettagli sulle sue abitudini, sui suoi amici o sui suoi interessi. Questi dati vengono acquisiti non solo direttamente dalla vittima durante la conversazione, ma anche dai **social network**, dove la vittima può lasciare tracce del proprio profilo e della propria vita privata (ad esempio, lista di amici, foto, dettagli sulla vita quotidiana). L'uso delle informazioni personali è un **elemento chiave** nel processo di costruzione della "falsa intimità", che può essere sfruttata anche per compiere altre azioni fraudolente (Spender, 2012). In quasi la totalità dei casi le vittime vengono adescate da profili apparentemente femminili, caratterizzati da immagini di donne particolarmente attraenti o ritratte in pose provocanti. L'utilizzo del corpo femminile come strumento di manipolazione non è solo un atto di inganno, ma una forma di sfruttamento che alimenta dinamiche di dominio e controllo. La scelta di utilizzare queste immagini per scopi manipolatori non solo riduce la donna a un oggetto desiderato, ma alimenta una visione distorta e stereotipata della figura femminile. In un contesto in cui il corpo femminile viene costantemente esposto e manipolato per attrarre attenzioni e raccogliere consensi, l'uso di immagini false a fini di adescamento contribuisce a perpetuare una visione svilente. Questo fenomeno va oltre la semplice violazione della privacy: si inserisce in un contesto più ampio di mercificazione del corpo femminile, dove il valore della donna viene ridotto a un'idea estetica e sessualizzata che perde la sua umanità e diventa un mezzo per manipolare gli altri. Inoltre, l'utilizzo di queste immagini provoca una distorsione delle relazioni interpersonali e una pericolosa visione delle donne come strumenti di soddisfazione per il desiderio maschile. Ciò non solo favorisce l'oggettivazione del corpo femminile, ma contribuisce anche al rafforzamento di una cultura che favorisce l'uso del corpo femminile per scopi puramente utilitaristici.

2. **Evoluzione della conversazione verso temi erotici:** Una volta stabilito un primo contatto e ottenute sufficienti informazioni personali, il truffatore inizia a **introdurre gradualmente tematiche più intime**, mirando a far abbassare le difese all'altro. Questo passaggio può essere compreso utilizzando il concetto di **desensibilizzazione**, che è un meccanismo attraverso cui il truffatore cerca di far sembrare naturale l'avanzamento della conversazione verso temi più erotici o sessuali. La **manipolazione psicologica** inizia a prendere piede quando il criminale utilizza il calore emozionale di una conversazione apparentemente "intima" per condurre il discorso verso la sessualizzazione. Questa parte del processo si inserisce nel concetto di ***gaslighting*** (Schechter, 2002), un fenomeno psicologico che implica far dubitare una persona della propria percezione della realtà. In questo caso, la vittima viene gradualmente convinta che la conversazione sia naturale o addirittura auspicabile, nonostante la progressiva violazione dei confini personali.

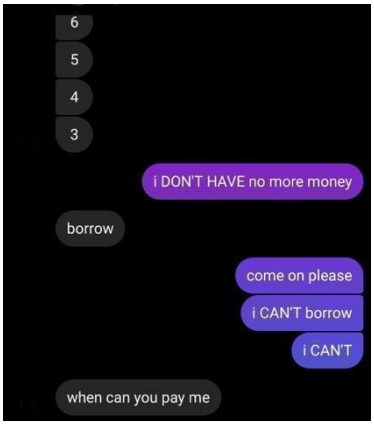
3. **Registrazione e ricatto:** Nel momento in cui la vittima si è lasciata coinvolgere in una conversazione di natura intima, questa solitamente viene **registrata di nascosto,** approfittando della vulnerabilità e della perdita di inibizioni della stessa. Una volta ottenuto il materiale compromettente (in genere foto inviate dalla vittima o registrazioni audio o video di natura sessuale), il truffatore utilizza la **minaccia** di rendere pubbliche queste informazioni per costringere la vittima a esaudire le sue richieste. La dinamica appena descritta suggerisce che la relazione tra criminale e vittima diventi un gioco di potere, in cui il truffatore esercita un controllo diretto sulla vita della stessa, minacciando di esporre la sua intimità se non ottiene ciò che vuole. In questo contesto, l'**isolamento sociale** della vittima, spesso reso possibile dalla sua vulnerabilità online e dalla mancanza di supporto immediato, contribuisce ad aumentare l'efficacia del ricatto.

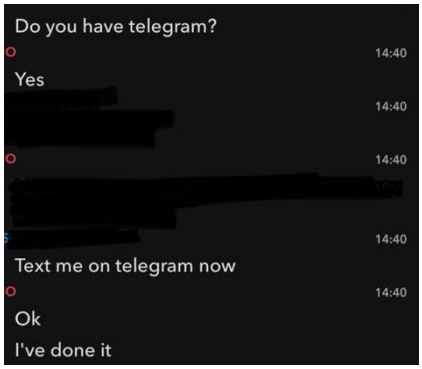
L'approccio alle vittime attraverso l'uso di **social media** e altre piattaforme online è legato alla natura **virtuale** della relazione che il truffatore costruisce. La sociologia delle tecnologie dell'informazione (Turkle, 2011) ha evidenziato come la distanza fisica e la mediazione tecnologica possano ridurre la percezione di "pericolo" e di **controllo sociale**, aumentando la vulnerabilità delle persone. In un contesto di anonimato online, le vittime spesso abbassano la guardia e agiscono in modo più spontaneo o disinibito, mentre il truffatore approfitta di questa **disconnessione emotiva** per manipolare e ottenere il proprio vantaggio. Si osserva una differenza significativa nel trattamento riservato alle vittime in base al genere: mentre agli uomini viene frequentemente richiesto denaro in cambio del silenzio o della non diffusione di materiale compromettente, alle donne viene invece quasi sempre chiesto l'invio di ulteriori immagini intime. Questa dinamica rivela nuovamente un aspetto profondamente radicato di **sfruttamento del corpo femminile** e di **oggettivazione sessuale** (Fredrickson & Roberts, 1997), in cui il valore della vittima viene ricondotto alla sua dimensione sessuale e alla disponibilità del proprio corpo come merce di scambio. Questa distinzione può essere letta come una forma di **sessismo strutturale**, che non solo oggettifica la donna, ma ne rafforza la vulnerabilità in quanto soggetto considerato primariamente per il suo corpo e non per il suo potere economico, come accade invece nel caso degli uomini. Si tratta quindi di una doppia violenza: una **digitale e sessuale**, ma anche **culturale**, che riflette e amplifica le disuguaglianze di genere già presenti nella società.



PIATTAFORME COINVOLTE E GUADAGNI

L'analisi dei casi di *sextortion* oggetto di questo report ha portato alla formulazione di una teoria inquietante: dietro molti di questi crimini potrebbe esserci una vera e propria **organizzazione criminale strutturata**. In particolare, la metodologia di adescamento delle vittime presenta molteplici somiglianze tra i vari casi, sia di italiani che di non italiani, suggerendo l'esistenza di un piano ben definito e condiviso da parte degli autori del reato. Una caratteristica comune di numerosi casi di *sextortion* è l'uso di più piattaforme per raggiungere lo scopo finale: ottenere denaro. L'analisi del fenomeno ha evidenziato uno schema ricorrente che si è evoluto negli ultimi anni: la vittima viene inizialmente adescata su un

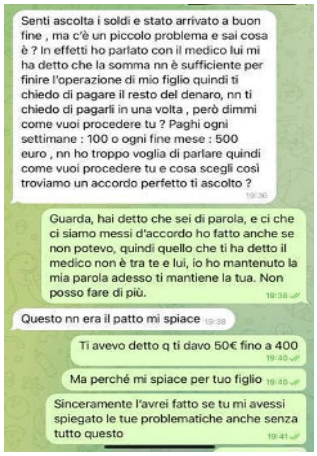




social network che fornisce informazioni personali facilmente accessibili, come Instagram o Facebook, dove l'autore può costruire un rapporto di fiducia. Dopo una conversazione iniziale che appare innocente, l'aggressore spinge la vittima a spostarsi su un'altra piattaforma, come Telegram. Questo cambio di piattaforma risulta fondamentale, in quanto Telegram, a differenza delle piattaforme appartenenti al gruppo Meta (Facebook, Instagram, Whatsapp), non è regolamentato per contrastare il fenomeno della condivisione non consensuale di materiale intimo e non offre alcuna risposta alle richieste di aiuto. Questo passaggio da una piattaforma più "sicura" ad una "non sicura" è un punto cruciale del *modus operandi*. In pratica, l'aggressore sfrutta la possibilità di ottenere informazioni personali su una piattaforma, ma commette il reato su un'altra, dove sa che non ci saranno interventi di alcun tipo. L'utilizzo di più piattaforme per il perpetrarsi di questo crimine è un fenomeno relativamente recente e può essere interpretato come una strategia evolutiva degli autori, che cercano di aggirare i controlli e le misure di sicurezza. Tuttavia, va sottolineato che, ad oggi, l'utilizzo di una sola piattaforma resta il metodo prevalente, dato che risulta più rapido ed efficace per i carnefici. Analizzando i dati disponibili, in **501 casi** è stata utilizzata una sola piattaforma, mentre in **290 casi** sono state impiegate due piattaforme, in **53 casi** tre piattaforme, e in **242 casi** le vittime non hanno fornito all'associazione informazioni riguardo il numero di piattaforme coinvolte. Le piattaforme maggiormente utilizzate sono quelle appartenenti al gruppo Meta (in oltre la metà dei casi), Telegram e app di dating. Inoltre, nel periodo **2021-2022,** si è riscontrato l'utilizzo di altre applicazioni di messaggistica, come Google Hangouts. Un aspetto interessante emerso nel **2024** è l'adozione di Discord, con **10 casi documentati**, suggerendo che anche i videogiochi e le piattaforme di chat ad essi collegate stiano diventando terreno fertile per la proliferazione di questi crimini. Un altro aspetto significativo che emerge riguarda il guadagno che gli autori dei crimini riescono a ottenere. Va precisato che le informazioni disponibili sono scarne e si basano esclusivamente sui racconti delle vittime, molte delle quali sono restie a condividere dettagli riguardanti i pagamenti effettuati. Ad oggi, sappiamo con certezza che **133 vittime hanno pagato somme di denaro agli aggressori, per un totale di circa 45.453 euro**, somma che è stata versata attraverso diversi metodi di pagamento online, tra cui **PayPal, Western Union, MoneyGram e Tip Tap.** È interessante sottolineare come questi metodi di pagamento siano spesso

istantanei, facilitando l'operato dei carnefici. Nonostante ciò, va evidenziato che, in base alle informazioni raccolte, i carnefici hanno richiesto un totale di **392.482 euro** dalle vittime. Ciò suggerisce che ci potrebbero essere molti più casi di vittime che hanno ceduto al ricatto, ma che non hanno condiviso tale informazione.

Un aspetto ricorrente nelle dinamiche di *sextortion* è la richiesta iniziale di cifre elevate (spesso superiori ai **1.000 euro**), seguita da una contrattazione che abbassa la somma richiesta. Questo stratagemma ha lo scopo di dare alla vittima l'illusione di avere il controllo della situazione, ma in realtà si tratta di un processo di estorsione. È importante notare come i carnefici, durante la fase di ricatto, adottino una strategia di minaccia estremamente aggressiva. Essi inviano continuamente screenshot contenenti collage di foto di amici e familiari della vittima, minacciando di pubblicare tali immagini se il pagamento non avviene immediatamente. In molti casi, i carnefici impostano un *countdown* per accentuare il senso di urgenza. Inoltre, sono stati rilevati schemi linguistici simili nelle minacce, con frasi scritte in italiano ma che risultano essere tradotte in modo approssimativo, suggerendo spesso un'origine non locale degli autori del reato. Le vittime vengono inoltre sommerse da chiamate e messaggi provenienti da numeri diversi, creando un forte stato di stress psicologico che li porta spesso a cedere. Tuttavia, è fondamentale non pagare in quanto non rappresenta una soluzione. Infatti, nei casi in cui le vittime hanno pagato, le minacce non sono cessate, ma bensì i carnefici sono tornati rapidamente alla carica, richiedendo somme ancora più elevate.



Il ruolo delle piattaforme

Il **principio di immunità condizionata** per gli intermediari, introdotto dalla direttiva e-Commerce del 2000, stabilisce che i prestatori di servizi online **non sono legalmente responsabili** per i contenuti pubblicati dagli utenti, purché non abbiano conoscenza effettiva dell'illecito, rimuovano tempestivamente i contenuti illegali una volta informati e svolgano un ruolo neutrale, senza controllo attivo sui contenuti.

Il Digital Services Act (DSA)[10], entrato successivamente in vigore nel 2023, ha mantenuto tale principio ma - a differenza della direttiva e-Commerce che si concentrava sull'immunità reattiva (post segnalazione) – ha introdotto alcuni **obblighi proattivi** per le piattaforme con

[10] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

oltre 45 milioni di utenti mensili nell'UE (*VLOP - Very Large Online Platforms*). Queste sono infatti chiamate a diventare **attori centrali nella lotta ai contenuti illeciti**, bilanciando libertà di espressione e tutela degli utenti. Le violazioni del DSA possono comportare sanzioni fino al 6% del fatturato globale annuo della piattaforma.

DINAMICHE RELAZIONALI TRA VITTIMA MASCHILE E PERSECUTORE

Il meccanismo della *sextortion* si fonda su una dinamica di controllo progressivo. Dopo aver ottenuto inizialmente il consenso – spesso in contesti relazionali intimi o manipolativi – il ricattatore sfrutta la fiducia della vittima per instaurare un ciclo di minacce e richieste. Il campione preso in esame è stato analizzato con l'obiettivo di indagare le dinamiche relazionali tra vittima e persecutore. L'approccio utilizzato è stato di tipo **analitico transazionale**, secondo il modello proposto da Eric Berne (1949). In particolare, è stato applicato il modello psicologico del **Triangolo Drammatico**[11] di Stephen B. Karpman (1968), che descrive le dinamiche interpersonali disfunzionali che si instaurano nei conflitti sociali. Tale modello evidenzia come gli individui assumano, inconsapevolmente, **ruoli complementari** all'interno delle interazioni, perpetuando schemi relazionali **disadattivi**.

I tre ruoli fondamentali individuati da Karpman – la Vittima, il Persecutore e il Salvatore – si influenzano reciprocamente in un ciclo reiterativo. La **Vittima** si percepisce come impotente, incapace di affrontare autonomamente le difficoltà e tende a cercare un intervento esterno per risolvere i propri problemi. Manifesta atteggiamenti passivi e può sviluppare sentimenti di ingiustizia o risentimento, finendo spesso per incolpare il persecutore o aspettarsi l'intervento di un salvatore. Il **Persecutore** assume invece un atteggiamento critico, aggressivo o autoritario nei confronti della vittima, esercitando pressioni o colpevolizzandola. Questo ruolo può essere espresso attivamente – attraverso minacce, rimproveri o comportamenti coercitivi – oppure passivamente, mediante atteggiamenti svalutanti o manipolatori. Il **Salvatore**, infine, interviene per aiutare la vittima spesso senza che gli venga richiesto, finendo per alimentare la dipendenza della stessa. In alcuni casi può trarre gratificazione dal proprio ruolo di soccorritore, ma rischia di sottrarre alla vittima la possibilità di sviluppare autodeterminazione. Qualora l'aiuto non venga accolto o non porti i risultati sperati, il Salvatore può trasformarsi in Vittima – se si sente incompreso – oppure in Persecutore, se inizia a provare frustrazione o critica.

[11] Per maggiori approfondimenti: https://karpmandramatriangle.com

Applicazione del Triangolo Drammatico di Karpman alla *Sextortion*

Nel contesto della *sextortion*, la vittima ricopre il ruolo di chi subisce direttamente la minaccia o il ricatto. Vive un forte senso di impotenza e si sente intrappolata in una situazione in cui il persecutore detiene il controllo. In molti casi, la **vittima** arriva a interiorizzare la colpa, considerando sé stessa responsabile di quanto accaduto e sviluppando così una forma di **auto-persecuzione**. Questo stato psicologico è spesso caratterizzato da vergogna, senso di colpa e paura, emozioni alimentate sia dalla manipolazione del persecutore, sia dalla propria tendenza a rimanere intrappolata in stati d'animo negativi reiterati. Il **persecutore**, dal canto suo, assume un comportamento volto a esercitare pressione psicologica attraverso minacce, come la diffusione di immagini intime, allo scopo di ottenere benefici personali – siano essi economici, sessuali o di altro tipo. Psicologicamente, giustifica le sue azioni attraverso una mentalità di superiorità o un bisogno di controllo, mostrando scarso o nullo livello di empatia verso la sofferenza della vittima. In alcune circostanze, il persecutore può assumere anche il ruolo di **salvatore**. Questo avviene quando, manipolando ulteriormente la vittima, le offre una "via d'uscita", ad esempio promettendo di non divulgare il materiale compromettente in cambio della soddisfazione delle sue richieste. Tale comportamento, pur assumendo la forma apparente dell'aiuto, rappresenta in realtà una raffinata **strategia di controllo**, poiché mantiene viva l'illusione di un possibile sollievo senza però restituire alla vittima la reale libertà.

Strategie di coping adottate dalle vittime

L'applicazione del modello teorico elaborato da Lazarus e Folkman (1984) consente di comprendere le reazioni psicologiche che le vittime di *sextortion* mettono in atto. Secondo questi autori, lo **stress** è il risultato di una relazione percepita tra individuo e ambiente in cui la persona ritiene che le proprie risorse siano insufficienti a fronteggiare la situazione. La *sextortion,* infatti, si configura come un evento ad alto impatto emotivo e stressogeno, e le risposte delle vittime possono variare significativamente. Alcune persone adottano un coping focalizzato sul **problema**, cercando cioè di affrontare direttamente la **minaccia**. Questo può tradursi nella denuncia del ricattatore alle autorità competenti, nel blocco dei canali di contatto o nella richiesta di supporto tecnico e legale. Altre vittime, invece, sviluppano strategie di coping focalizzate sulle **emozioni**. In questo caso, l'attenzione è rivolta alla gestione del **carico emotivo**, che può includere ansia, paura, senso di colpa e vergogna. Tali strategie comprendono il ricorso al supporto sociale, alla ristrutturazione cognitiva o ad attività che favoriscano il contenimento emotivo. Vi sono, infine, casi in cui prevale un coping **evitante**, in cui la persona rifiuta di affrontare la realtà, si isola o – nei casi più gravi – può arrivare a

comportamenti autolesivi. Questo tipo di risposta, seppur comprensibile come reazione difensiva iniziale, rischia di aggravare il disagio e di prolungare lo stato di vulnerabilità psicologica.

CONSEGUENZE PSICOLOGICHE DELLA *SEXTORTION* A BREVE E LUNGO TERMINE

La *sextortion* ha conseguenze psicologiche significative, che si manifestano sia nel breve che nel lungo periodo. Il danno psichico subito dalle vittime si configura spesso come **trauma complesso**, poiché l'esperienza racchiude elementi di abuso relazionale, violazione dell'intimità e perdita di controllo sulla propria immagine corporea e identitaria (Courtois & Ford, 2020).

Conseguenze a breve termine

Nel breve periodo, le vittime possono sviluppare una sintomatologia acuta, con quadri clinici dominati da ansia intensa, attacchi di panico, insonnia, irritabilità e pensieri intrusivi legati all'evento traumatico. La paura della divulgazione del materiale sessualmente esplicito agisce come un fattore di stress costante, che produce una condizione di **ipervigilanza** e **senso di impotenza** (Chatzittofis et al., 2020). Frequenti sono anche reazioni dissociative, manifestazioni psicosomatiche e alterazioni dell'umore. In molti casi si osservano sentimenti di vergogna, senso di colpa e colpevolizzazione interna, che possono ostacolare la richiesta di aiuto e portare al ritiro sociale (Feinstein et al., 2014). In questa fase, la sofferenza psicologica è spesso aggravata dalla percezione di **giudizio** da parte dell'ambiente sociale o familiare, e dalla difficoltà a raccontare l'accaduto per timore di ulteriori **stigmatizzazioni**.

Conseguenze a lungo termine

Una delle peculiarità della *sextortion* risiede nella sua natura di **esposizione permanente**. Il timore di eliminare definitivamente il materiale compromettente, o anche solo la minaccia della sua riemersione, agiscono come una continua fonte di riattivazione del trauma (Shapiro, 2018; Carletto et al., 2016).
Per questa ragione, le vittime sviluppano, a lungo termine, quadri di **Disturbo da Stress Post-Traumatico (PTSD)** che, proprio per la sua natura ricorsiva, viene definito nella recente letteratura come ***perpetual trauma loop***.
Questo concetto descrive profondamente l'**esperienza traumatica** associata alla *sextortion*, non è infatti l'evento singolo (la diffusione o la minaccia di diffusione) a determinare il danno principale, bensì la cronicizzazione della minaccia, che mantiene l'individuo in uno stato di allerta costante (De Santisteban et al., 2020).

Questa condizione si traduce in una **riattivazione ciclica** del trauma a livello cognitivo (pensieri intrusivi e ipervigilanza), emotivo (ansia, vergogna, impotenza) e somatico (attivazione neurofisiologica dello stress). La sola possibilità che il materiale possa riemergere, anche a distanza di anni, è sufficiente a mantenere attiva la risposta da stress post-traumatico (Rapkoch, 2024).
Per questa ragione, la *sextortion* non può essere considerata un **evento isolato**, ma va compresa come una forma di esposizione traumatica continua, in cui il confine tra passato, presente e futuro risulta costantemente sfumato.
Questo perpetuo stato di vulnerabilità, in assenza di un adeguato supporto psicologico, rende estremamente difficile per le vittime ripristinare un senso di controllo e sicurezza nella propria vita.

POSSIBILI INTERVENTI TERAPEUTICI

Il riconoscimento delle conseguenze psicologiche della *sextortion* è fondamentale per progettare **interventi terapeutici mirati**. È necessario un approccio integrato che comprenda la **stabilizzazione emotiva**, la **ristrutturazione cognitiva**, il l**avoro sulla vergogna** e il potenziamento dell'**autoefficacia**.

Terapia Cognitivo-Comportamentale (CBT)

La terapia cognitivo-comportamentale è ampiamente utilizzata nel trattamento dei traumi psicologici e dell'ansia derivante da forme di **coercizione sessuale**. Si basa sulla ristrutturazione dei **pensieri disfunzionali** e sulla riduzione dei sintomi emotivi attraverso tecniche di esposizione graduata e riformulazione cognitiva (Beck, 2011). Nel contesto della *sextortion*, la CBT ha l'obiettivo di decostruire la **vergogna** e il **senso di colpa** che la vittima può provare (Feinstein et al., 2014), sostituendo gli schemi di pensiero negativi con convinzioni più adattive e favorendo così una riduzione dell'autocolpevolizzazione. Inoltre, l'approccio include l'impiego di tecniche di *problem-solving*, utili a migliorare il senso di controllo percepito sulla situazione.

EMDR e trattamento dei sintomi post-traumatici

L'Eye Movement Desensitization and Reprocessing (EMDR) si è dimostrato efficace nel trattamento del Disturbo da Stress Post-Traumatico (PTSD) e nei casi di trauma relazionale (Shapiro, 2018). Questo approccio terapeutico consente alle vittime di *sextortion* di rielaborare i ricordi traumatici in modo meno disturbante, favorendo una riduzione dei sintomi di iperattivazione emotiva e dei flashback. Studi recenti (Carletto et al., 2016) hanno evidenziato come l'EMDR sia in grado di diminuire significativamente i livelli di **ansia** e **depressione** in soggetti che hanno vissuto esperienze di **abuso psicologico** e **minacce online**.

Terapia basata sulla Mindfulness

La *Mindfulness-Based Stress Reduction* (MBSR) e la *Mindfulness-Based Cognitive Therapy* (MBCT) rappresentano strumenti utili per aiutare le vittime a gestire lo **stress emotivo** e a migliorare la **regolazione delle emozioni** (Kabat-Zinn, 1990). Entrambi gli approcci si concentrano sullo sviluppo della consapevolezza del momento presente e sulla riduzione della ruminazione negativa. Ciò risulta particolarmente efficace per le vittime di *sextortion* che, a causa della minaccia costante di divulgazione dei contenuti intimi, sviluppano frequentemente **ansia anticipatoria** e **pensieri intrusivi** (Segal, Williams & Teasdale, 2018).

Interventi sulla regolazione emotiva e sull'autoefficacia

Molte vittime di *sextortion* sperimentano livelli intensi di vergogna e paura del giudizio sociale, che spesso si traducono in **isolamento** e in un peggioramento del disagio psicologico (Levin et al., 2022). In questi casi, interventi terapeutici basati sull'*Acceptance and Commitment Therapy* (ACT) hanno dimostrato efficacia nell'aiutare i pazienti ad accettare le proprie emozioni senza cercare di evitarle o amplificarle, favorendo lo sviluppo dell'**autoaccettazione** (Hayes, Strosahl & Wilson, 2016).

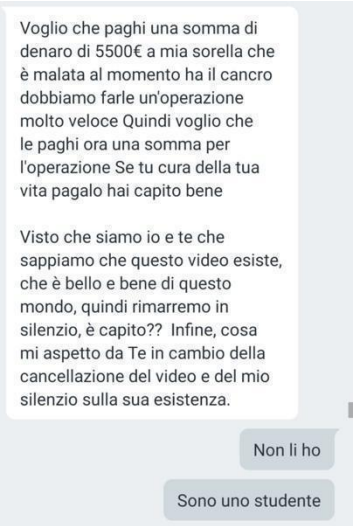
Il processo di recupero psicologico richiede anche il rafforzamento dell'**autoefficacia** personale. Secondo Bandura (1997), il senso di autoefficacia è un fattore determinante per superare eventi stressanti e ridurre il rischio di sviluppare *PTSD*. A tal fine, programmi terapeutici centrati sulla resilienza, come la *Resilience Training Therapy,* possono offrire un supporto valido per aiutare le vittime a ricostruire la fiducia in sé stesse e a sviluppare strategie volte a prevenire future vulnerabilità (Southwick & Charney, 2012).

Approccio integrato e supporto sociale

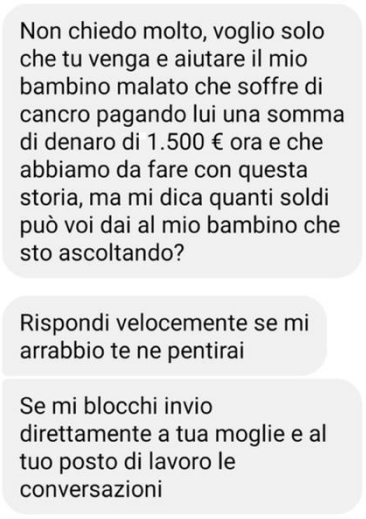
Per affrontare in modo efficace le conseguenze psicologiche della *sextortion*, è spesso necessario un **approccio terapeutico integrato**, che combini più modelli clinici. Il supporto sociale svolge un ruolo essenziale come **fattore protettivo**: il coinvolgimento della rete familiare o di gruppi di supporto può facilitare i processi di recupero e contrastare il rischio di **ritiro sociale** (Cohen & Wills, 1985). Inoltre, la **Terapia Sistemica** può rivelarsi utile per analizzare e riorganizzare le dinamiche relazionali, favorendo la prevenzione di ulteriori episodi di vittimizzazione (Minuchin, 1974).

PUOI AIUTARE IL MIO BAMBINO?

Uno degli schemi più insidiosi nei ricatti economici online è quello che fa leva su **presunte emergenze mediche** legate a figure familiari vulnerabili, in particolare figli molto piccoli o madri gravemente malate. L'obiettivo del ricattatore è ottenere denaro attraverso la costruzione di una narrativa fittizia, spesso dettagliata, che riesce a manipolare efficacemente le emozioni della vittima. Sebbene la persona malata sicuramente non esista, l'utilizzo della malattia come giustificazione è tutt'altro che casuale e risponde a dinamiche psicologiche, sociali e criminologiche ben precise. Nel periodo monitorato Permesso Negato ha rilevato **45 richieste di denaro destinate**, a detta del ricattatore, **alle cure dei figli o altro parente malato.**



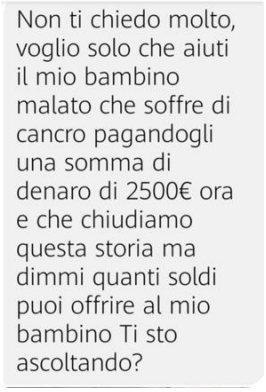
Dal punto di vista psicologico, questo tipo di schema attiva quello che è noto come *trigger empatico primario*, ovvero un meccanismo automatico che spinge l'individuo a rispondere con compassione e solidarietà di fronte alla sofferenza, in particolare se rappresentata da categorie ritenute socialmente "sacre" o "protette", come i bambini e le madri. Il senso di urgenza e responsabilità morale viene amplificato dalla narrazione, che spesso fa leva su dettagli drammatici, foto, nomi, orari di visite mediche e countdown legati a operazioni salvavita, che creano un falso senso di immediatezza e ineluttabilità. In queste condizioni, il comportamento della vittima può essere inquadrato come una risposta a uno *shock morale indotto*, ovvero un'azione precipitosa motivata da un'improvvisa pressione emotiva e sociale.



Sociologicamente, la narrazione costruita sfrutta stereotipi e archetipi culturali profondamente radicati: il bambino malato rappresenta l'innocenza violata, mentre la madre malata incarna il sacrificio e la sofferenza silenziosa. Queste figure evocano immediatamente una responsabilità collettiva, e permettono al ricattatore di bypassare le difese razionali dell'interlocutore. Si osserva qui un'applicazione deviata del principio della *moral suasion*, in cui si fa leva su valori condivisi per indurre comportamenti altruistici, anche in assenza di verifica dei fatti.

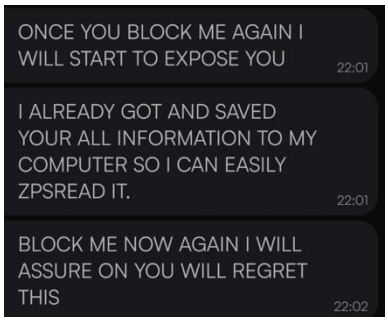
Dal punto di vista criminologico, è possibile inquadrare questo fenomeno all'interno di più cornici teoriche. La **Routine Activity Theory** (Cohen e Felson, 1979), che descrive il crimine come l'incontro tra un autore motivato, una vittima disponibile e l'assenza di un guardiano efficace, trova piena applicazione nel contesto digitale: le piattaforme online offrono un

ambiente perfetto dove il criminale può incontrare vittime esposte, spesso senza strumenti o riferimenti per riconoscere il raggiro. Parallelamente, la **Neutralization Theory** (Sykes e Matza, 1957) spiega come gli autori del reato giustifichino le proprie azioni attraverso meccanismi cognitivi di deresponsabilizzazione, ad esempio sostenendo interiormente che "non stanno davvero danneggiando nessuno" o che "le persone sono abbastanza ricche da poter donare qualcosa".



La struttura narrativa dei ricatti di questo tipo segue *pattern* ben riconoscibili: un primo approccio emotivamente neutro, seguito da una graduale costruzione della storia clinica, l'introduzione della richiesta economica e infine l'escalation della pressione psicologica, spesso accompagnata da messaggi manipolatori ("sei l'unica persona che può salvare mia figlia") o da sensi di colpa indotti ("se non mi aiuti, morirà ed è colpa tua"). In diversi casi documentati, l'aggressore invia ripetutamente messaggi, immagini strazianti e registrazioni vocali, bombardando la vittima fino alla rottura della resistenza.

È utile inoltre sottolineare che questo tipo di dinamica rientra tra quelle che nella letteratura criminologica sono definite **truffe a leva affettiva** (*emotional scams*), una sottocategoria delle truffe relazionali in cui il fine è meramente economico ma il mezzo è una costruzione empatica e relazionale falsa. In questi casi, l'autore del reato non solo ottiene un vantaggio finanziario, ma esercita anche un controllo psicologico sulla vittima, spesso lasciandola in uno stato di colpa o vergogna che le impedisce di denunciare quanto accaduto.



Infine, l'utilizzo della figura della madre o del figlio malato può essere letto anche come parte di una **strategia di manipolazione**: il ricattatore proietta sulla vittima la vulnerabilità dell'altro (madre o bambino), sperando che questa si identifichi con il dolore rappresentato. Questo meccanismo è tanto più efficace quanto più la vittima ha vissuto, nella propria esperienza personale, situazioni di fragilità familiare, perdita o malattia.

MINORI

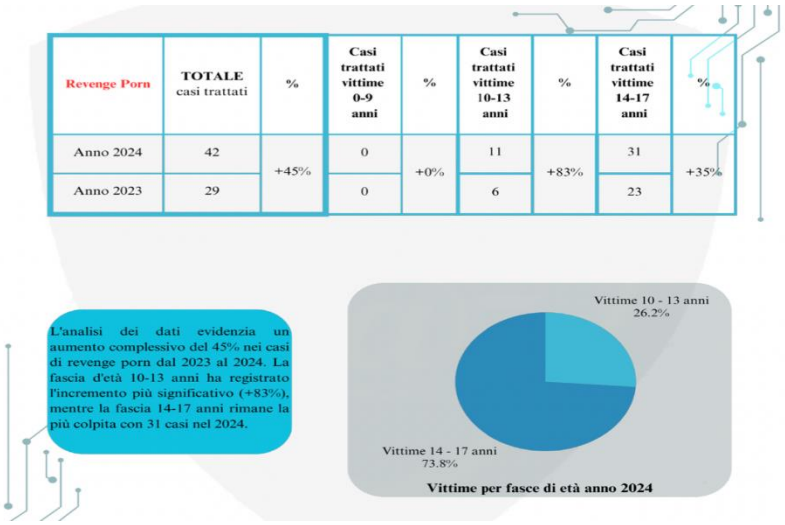
Nel quadriennio preso in esame, sono stati **meno di 100** i minori che si sono rivolti a PermessoNegato per chiedere aiuto. Un numero sorprendentemente basso, che può essere attribuito a diversi fattori: il senso di vergogna, il tentativo di gestire autonomamente la situazione, la paura della reazione dei genitori o, in alcuni casi, potrebbe anche esserci stato il timore che dichiararsi minorenni potesse impedire l'accesso all'aiuto senza il coinvolgimento diretto degli adulti. Considerando i dati emersi da altre ricerche sul tema, è ragionevole ritenere che i numeri raccolti non riflettano pienamente l'entità del fenomeno tra i più giovani.

Al contrario, tutto lascia pensare che i casi effettivi siano significativamente più numerosi di quelli formalmente emersi.

Nel 2024 Save the Children, pubblicò il report "*Le ragazze stanno bene? Indagine sulla violenza di genere onlife in adolescenza*"[12]; sulla base del sondaggio condotto da IPSOS nel gennaio 2024 su un campione di 800 giovani di età compresa tra 14 e 18 anni con quote rappresentative dell'universo di riferimento per genere, età e area geografica, la maggior parte dei ragazzi e delle ragazze intervistati (54%) ritiene che chi invia foto intime sia consapevole dei rischi che corre, incluso quello che le immagini possano essere diffuse a terzi. Il 27% degli intervistati non vede nulla di sbagliato nel richiedere foto intime alla persona con cui si ha una relazione intima, anche ripetutamente durante la giornata, mentre il 34% crede che ricevere foto intime non richieste sia un segnale di interesse da parte della persona che le invia. Quasi la metà degli adolescenti (49%) è in disaccordo con questa visione; tuttavia, il pensiero che l'invio di foto intime non richieste possa essere un'indicazione di interesse è abbastanza diffuso, in particolare tra i ragazzi che hanno o sono in una relazione (48%), rispetto alle ragazze con la stessa esperienza (29%). Gli adolescenti sembrano avere una certa consapevolezza dei rischi legati all'invio di foto intime: il 54% degli intervistati concorda almeno in parte sul fatto che chi invia queste immagini accetta i rischi, incluso quello che le foto possano essere condivise. Questo risultato suggerisce che, sebbene ci sia stata una buona diffusione dell'informazione riguardo i pericoli della condivisione di immagini online, la consapevolezza non sembra ancora sufficiente a dissuadere completamente dall'intraprendere tali pratiche. Per quanto riguarda le nuove forme di relazioni intime, la ricerca e la creazione di amicizie tramite i social è un fenomeno molto diffuso tra gli adolescenti. Il 73% degli intervistati afferma di aver stretto amicizie online con persone mai incontrate prima, con una prevalenza tra i 16 e i 18 anni (76%) e una maggiore incidenza tra i ragazzi rispetto alle ragazze (76% contro 70%). Il 64% degli adolescenti ha dichiarato di aver utilizzato i social media per conoscere o avvicinarsi a una persona che gli piace, con i ragazzi (68%) e i giovani tra i 16 e i 18 anni (65%) più inclini a questa pratica. Il 28% dei ragazzi e delle ragazze ha riferito di aver scambiato foto e/o video intimi con persone con cui sono stati o sono attualmente in una relazione, con una percentuale più alta tra i ragazzi (31%) e tra quelli che hanno avuto o sono in una relazione (40%). Inoltre, il 33% degli intervistati ha ricevuto foto o video sessualmente espliciti da amici o conoscenti, con un'incidenza maggiore tra i ragazzi e le ragazze di età compresa tra i 16 e i 18 anni (37%). Infine, circa il 10% degli adolescenti ha condiviso o postato foto intime senza il consenso della persona ritratta, e l'11% ha visto le proprie foto intime condivise senza il proprio permesso.

[12] https://s3-www.savethechildren.it/public/files/uploads/pubblicazioni/le-ragazze-stanno-bene_1.pdf

Anche il report annuale della Polizia Postale del 2024[13] restituisce dei dati allarmanti, soprattutto in termini di età:



Revenge Porn	TOTALE casi trattati	%	Casi trattati vittime 0-9 anni	%	Casi trattati vittime 10-13 anni	%	Casi trattati vittime 14-17 anni	%
Anno 2024	42	+45%	0	+0%	11	+83%	31	+35%
Anno 2023	29		0		6		23	

Fonte: Report annuale 2024 della Polizia Postale e per la Sicurezza Cibernetica

I dati condivisi mostrano chiaramente come anche i minori possono essere esposti a rischi significativi online, spesso sottovalutati. Tra questi, l'adescamento e la *sextortion* rappresentano pericoli reali, soprattutto quando non vi è una piena consapevolezza di ciò che si condivide, con chi e con quali conseguenze. In un contesto digitale sempre più pervasivo, è fondamentale educare i giovani alla cittadinanza digitale, rendendoli consapevoli che il confine tra online e offline è ormai sfumato. In questo senso, il concetto di *onlife*, elaborato dal filosofo Luciano Floridi, ci ricorda quanto la nostra vita digitale sia parte integrante della nostra identità e delle nostre relazioni quotidiane. I linguaggi sessisti e gli stereotipi di genere, inoltre, condizionano profondamente la crescita dei ragazzi, alimentando visioni distorte delle relazioni affettive e sessuali. Questo ambiente culturale può renderli più vulnerabili oppure, al contrario, spingerli verso comportamenti a loro volta dannosi e inconsapevoli. È quindi necessario promuovere percorsi educativi che uniscano l'alfabetizzazione digitale all'educazione affettiva e al rispetto dell'altro, per contrastare la cultura della prevaricazione e costruire spazi digitali più sicuri per tutti.

RISCHI FUTURI: I DEEP NUDE

Negli ultimi anni, la diffusione di immagini false e manipolate attraverso l'**intelligenza artificiale** sta assumendo dimensioni sempre più preoccupanti. L'intelligenza artificiale generativa, in particolare i modelli di *deep learning*, ha reso possibile la creazione di contenuti iperrealistici che, purtroppo, possono essere utilizzati in modi eticamente problematici, come

[13] https://www.poliziadistato.it/statics/40/2024-report-def.-sppsc.pdf

nel caso dei *deep nudes* - immagini o video alterati per mostrare persone in nudità non consensuale.
Un rischio per il futuro, che sta già emergendo con sempre maggiore frequenza, è l'uso di questi contenuti per attirare e manipolare utenti, in particolare attraverso strategie di seduzione e inganno. Le immagini *fake*, utilizzate in contesti di *romance scam* (truffe amorose) o di *sextortion*, rappresentano **uno degli strumenti più efficaci** per manipolare e adescare persone vulnerabili. Tali immagini vengono infatti create ad hoc, prendendo come base di partenza foto di donne molto sensuali o in atteggiamenti provocanti rubate da internet, e vengono abbinate a storie inventate o alterate. L'intento di queste immagini è principalmente quello di costruire una relazione virtuale apparentemente autentica che, attraverso il gioco delle emozioni e della fiducia, porta l'individuo a compiere azioni o rivelare informazioni sensibili. Il processo di adescamento, anche negli adulti, è spesso lungo e articolato, ma il suo obiettivo rimane invariato: **sfruttare la debolezza psicologica o emotiva della persona adescata per ottenere denaro, informazioni personali o altri vantaggi**.
Un aspetto importante di questo fenomeno è la creazione di una **seconda vittima**, ovvero la persona a cui sono state sottratte - solitamente da profili social pubblici - le immagini utilizzate per questi scopi, senza che essa ne sia consapevole. Questi furti d'immagine comportano una **violazione della privacy** e, talvolta, un **danno irreparabile alla reputazione** della persona coinvolta.
Da un punto di vista strettamente normativo, allo stato attuale, non esistono disposizioni del Codice Penale volte a sanzionare la condotta di illecita diffusione di contenuti generati o manipolati artificialmente. Invero, a seconda del contesto entro il quale tali immagini o video sono utilizzati, si potrebbero configurare i reati di diffamazione aggravata, sostituzione di persona, truffa, frode informatica, estorsione, minaccia, atti persecutori, diffusione illecita di immagini o video sessualmente espliciti. Si segnala inoltre che, in ragione del fatto che la creazione di un falso contenuto digitale comporta, in genere, anche il trattamento di dati personali, trovano applicazione le norme del **GDPR** (**Regolamento UE 679/2016**).

Negli ultimi anni, la diffusione di immagini false e manipolate attraverso l'**intelligenza artificiale** sta assumendo dimensioni sempre più preoccupanti. L'intelligenza artificiale generativa, in particolare i modelli di *deep learning*, ha reso possibile la creazione di contenuti iperrealistici che, purtroppo, possono essere utilizzati in modi eticamente problematici, come nel caso dei *deep nudes* - immagini o video alterati per mostrare persone in nudità non consensuale.
Un rischio per il futuro, che sta già emergendo con sempre maggiore frequenza, è l'uso di questi contenuti per attirare e manipolare utenti, in particolare attraverso strategie di seduzione e inganno. Le immagini *fake*, utilizzate in contesti di *romance scam* (truffe amorose) o di *sextortion*, rappresentano **uno degli strumenti più efficaci** per manipolare e adescare persone vulnerabili. Tali immagini vengono infatti create ad hoc, prendendo come base di

partenza foto di donne molto sensuali o in atteggiamenti provocanti rubate da internet, e vengono abbinate a storie inventate o alterate. L'intento di queste immagini è principalmente quello di costruire una relazione virtuale apparentemente autentica che, attraverso il gioco delle emozioni e della fiducia, porta l'individuo a compiere azioni o rivelare informazioni sensibili. Il processo di adescamento, anche negli adulti, è spesso lungo e articolato, ma il suo obiettivo rimane invariato: **sfruttare la debolezza psicologica o emotiva della persona adescata per ottenere denaro, informazioni personali o altri vantaggi**.

Un aspetto importante di questo fenomeno è la creazione di una **seconda vittima**, ovvero la persona a cui sono state sottratte - solitamente da profili social pubblici - le immagini utilizzate per questi scopi, senza che essa ne sia consapevole. Questi furti d'immagine comportano una **violazione della privacy** e, talvolta, un **danno irreparabile alla reputazione** della persona coinvolta.

Da un punto di vista strettamente normativo, allo stato attuale, non esistono disposizioni del Codice Penale volte a sanzionare la condotta di illecita diffusione di contenuti generati o manipolati artificialmente. Invero, a seconda del contesto entro il quale tali immagini o video sono utilizzati, si potrebbero configurare i reati di diffamazione aggravata, sostituzione di persona, truffa, frode informatica, estorsione, minaccia, atti persecutori, diffusione illecita di immagini o video sessualmente espliciti. Si segnala inoltre che, in ragione del fatto che la creazione di un falso contenuto digitale comporta, in genere, anche il trattamento di dati personali, trovano applicazione le norme del **GDPR** (**Regolamento UE 679/2016**).

TESTIMONIANZE

Davide – 26 febbraio 2024

Buonasera,
Mi chiamo Davide e vi ho trovati cercando su Internet. Ho deciso di contattarvi per chiedervi aiuto. Il 5 febbraio sono stato contattato su Instagram da una ragazza di nome Julie, che affermava di avermi visto su un una app di incontri e di voler fare la mia conoscenza. Io in effetti sporadicamente le ho utilizzate e quindi non mi sono insospettivo. Per un paio di giorni ci siamo scritti, sempre in inglese perché lei non è italiana, ma mi ha detto che per Pasqua sarebbe venuta in Italia in vacanza, fatalità a Roma dove risiedo.
Dopo un paio di sere Julie mi ha chiesto se volevamo "divertirci". Le ho chiesto se prima potevamo sentirci in videochiamata per conoscerci meglio, visto che non ci eravamo mai parlati ma solo scritti. Lei ha effettuato una breve videochiamata su Instagram, parlando con me per pochi secondi, dicendomi che non era a casa da sola e si vergognava. Successivamente, mi ha chiesto di continuare su Telegram e io ho accettato senza pormi grossi problemi. Una volta aggiunta su Telegram mi spiegato che sarebbe rimasta in muto perché i genitori stavamo dormendo nella stanza affianco. Durante la videochiamata, ho visto questa ragazza spogliarsi e assumere atteggiamenti intimi, incoraggiandomi a fare altrettanto: io l'ho fatto, inquadrandomi solo dal petto in giù. Ad un certo punto mi sono accorto che il suo video si era interrotto, pensavo ad un problema di connessione sul più bello. E invece sullo schermo è apparso un video che ritraeva me pochi secondi prima mentre mi stavo masturbando. Li ho capito di essere stato registrato e preso dal panico mi sono inquadrato in faccia chiedendole cose stesse facendo. A quel punto ha interrotto la videochiamata e ha iniziato a scrivermi dicendomi che se non volevo che tutti i miei contatti ricevessero in DM il mio video dovevo pagarla 3.000 euro, aggiungendo anche di avere una sorella malata di cancro. Istintivamente, ho eliminato i miei profili Instagram e Telegram per evitare che potesse ottenere altre mie foto e contatti e che continuasse a scrivermi (mi scriveva a raffica). Il giorno dopo mi sono recato dai Carabinieri per sporgere denuncia. Da un altro profilo IG ho controllato ed il suo profilo Instagram risulta cancellato, quello di Telegram invece è ancora attivo. Specifico infine che in data odierna (26-02-2024) non ho ricevuto segnalazioni dai miei amici riguardo alla diffusione del mio video in rete, ma sono comunque ansioso per la situazione e non riesco a dormire la notte.

Giorgia – 7 Ottobre 2023

Ho bisogno di aiuto urgente. Una persona che non conosco sta minacciando di diffondere un mio video intimo. Questa persona è entrata in possesso della registrazione di una videochiamata erotica che ho fatto circa un anno fa con il mio ex. Si è trattato di un episodio isolato: è stata l'unica volta in cui mi sono esposta in questo modo e, proprio per questo, non riesco a spiegarmi come qualcuno possa avere accesso a quel materiale oggi.
Quando ha iniziato a contattarmi, ho cercato di negare che fossi io nel video, ma la situazione è peggiorata rapidamente. Ha cominciato a ricattarmi, minacciando di inviare il video ai miei amici e conoscenti se non gli avessi inviato altro materiale intimo. Mi ha scritto chiaramente che, se avessi raccontato a qualcuno di queste minacce, avrebbe pubblicato il video. Da allora continua a contattarmi, anche se non gli rispondo, insistendo perché gli invii nuove foto intime e ripetendo le minacce. Io sto cercando di prendere tempo con scuse e pretesti, ma la verità è che non so più come gestire la situazione. Mi sento sotto pressione, spaventata e disperata.
Non ho mai pensato che qualcosa del genere potesse succedermi e ora mi sento completamente sola. Ho davvero bisogno di aiuto e non so a chi rivolgermi.

Giulio – 24 Dicembre 2021

Sono stato contattato da una ragazza su Instagram, sembrava avere poco più di vent'anni. Abbiamo iniziato a scriverci per qualche giorno e poi ci siamo spostati su Telegram.
Una notte le ho inviato un selfie dove, seppur con casco e occhiali, ero riconoscibile. Successivamente ho inviato due brevi video intimi, pensando che si sarebbero autodistrutti. Poco dopo, quella stessa persona ha fatto degli screenshot e ha inviato il materiale a tre dei miei contatti su Instagram. Subito dopo è iniziato il ricatto: mi hanno chiesto dei soldi per non diffondere ulteriormente le immagini.
Preso dal panico, ho ceduto e inviato 780 euro, sperando che finisse tutto.
Dopo il pagamento mi hanno mandato delle prove (screenshot) in cui sembrava avessero cancellato i messaggi mandati ai miei amici. Per fortuna era notte, penso che nessuno li abbia visti. Quando hanno continuato a chiedere altri soldi, ho finto di essere al verde per cercare di fargli pena. Mi hanno detto di restare calmo e di trovare altri 100 euro, lasciandomi tempo fino al mattino. Al mattino, ho inviato un ultimo messaggio in cui dicevo che la banca non mi aveva bloccato la carta. Ho poi cambiato nickname su Telegram e ho bloccato i contatti. Da quel giorno non ho più ricevuto nulla. Ho ancora il mio profilo Instagram e Facebook attivi, ma non accetto nuove richieste né seguo più nessuno.

COSA POSSO FARE SE SONO VITTIMA DI CONDIVISIONE NON CONSENSUALE DI MATERIALE INTIMO?

Come abbiamo visto, durante le relazioni virtuali, si potrebbe incappare nella diffusione di contenuti che appartengono alla propria sfera personale. La natura di questi contenuti potrebbe essere varia: da immagini riprese volontariamente nel corso di un atto sessuale ma destinate a rimanere private o ad essere condivise solamente all'interno di un legame di relazione, ad immagini carpite da telecamere nascoste o, talvolta, immagini sottratte da dispositivi elettronici vittime di effrazioni digitali - spesso appositamente congegnate - fino ad immagini riprese nel corso di una violenza sessuale.

Il "mondo virtuale" è caratterizzato dalla **viralità**, vale a dire che i contenuti possono diffondersi molto rapidamente attraverso la condivisione spontanea degli utenti, spesso raggiungendo milioni di persone in breve tempo. È pertanto fondamentale **segnalare tempestivamente i contenuti alle piattaforme**, quando se ne viene a conoscenza. I motori di ricerca, i social media, i siti di incontri ed i siti porno riconoscono che la condivisione non consensuale di materiale intimo è dannosa e sbagliata e mettono a disposizione specifiche procedure di segnalazione. Qualora non sia disponibile, è comunque possibile contattare il proprietario del sito, cioè il *webmaster*, attraverso il modulo "Contattaci" o l'indirizzo email messo a disposizione. Queste informazioni sono spesso riportate in calce nella home page del sito o all'interno della Privacy Policy.

Prima di procedere con la segnalazione è importante acquisire sempre **una evidenza dei contenuti pubblicati** *(screenshot)* prima che questi vengano rimossi, al fine di poter successivamente procedere con un'eventuale azione legale. Potrebbe essere inoltre utile conservare evidenza anche di eventuali minacce ricevute e qualsiasi riferimento inerente all'account della persona "attaccante".

Infine, consigliamo di rivolgersi all'Autorità Giudiziaria per **sporgere una denuncia o una querela**, sia al fine di vedersi riconosciuta l'ingiustizia subita, sia per portare alla luce un reato che è ancora troppo sottostimato.

RACCOMANDAZIONI FINALI

Alla luce della crescente diffusione del fenomeno della sextortion e più in generale della condivisione non consensuale di materiale intimo, risulta imprescindibile l'adozione di misure sistemiche e coordinate, che affianchino all'educazione digitale e culturale un intervento normativo e istituzionale deciso. Affrontare seriamente la diffusione non consensuale di contenuti intimi richiede un cambio di prospettiva: non si tratta di episodi privati, ma di un problema sociale e culturale che riguarda tutti. Una risposta efficace nasce dal coordinamento tra norme aggiornate, tecnologie responsabili e servizi vicini alle persone. Non è un obiettivo irraggiungibile: è una direzione necessaria.

Le seguenti proposte operative sono rivolte a tre attori fondamentali nel contrasto a questo fenomeno: **il legislatore**, **le piattaforme digitali** e gli **enti pubblici**.

Per il legislatore: aggiornare il quadro normativo alla realtà digitale

L'attuale impianto giuridico spesso fatica a inquadrare con precisione e tempestività le dinamiche legate alla diffusione non consensuale di contenuti intimi, fenomeno che assume forme diverse: *sextortion, revenge porn*, ricatti affettivi, diffusione accidentale o intenzionale. Adeguare il sistema normativo alle esigenze attuali, è il primo passo per affrontare in maniera compiuta i nuovi fenomeni criminosi di cui si è trattato.
Si raccomanda pertanto di:

- **introdurre una fattispecie autonoma di reato** che includa gli elementi principali di questi comportamenti (estorsione, violazione della riservatezza, abuso digitale), in modo da garantire un'applicazione uniforme e una tutela rafforzata per le vittime;
- **prevedere aggravanti specifiche**, ad esempio quando la vittima è minorenne, appartiene a categorie particolarmente esposte (come le persone LGBTQ+) o si trova in una condizione di vulnerabilità psichica;
- e**stendere il diritto al patrocinio gratuito**, senza necessità di ulteriori requisiti, alle vittime di questi reati, al pari di quanto già previsto per altri crimini a sfondo sessuale.

Per le piattaforme digitali: favorire prevenzione, reattività e collaborazione

Le piattaforme digitali hanno un ruolo cruciale nella prevenzione e nella gestione dei contenuti abusivi. Non si tratta solo di reagire quando il danno è fatto, ma di mettere in atto misure tecniche e organizzative che lo rendano meno probabile. La fiducia degli utenti passa anche dalla capacità delle piattaforme di proteggere la loro integrità.
Si raccomanda pertanto di:

- **Rispondere entro 24 ore alle segnalazioni di condivisione non consensuale di materiale intimo**, garantendo tempi certi e canali di contatto diretti;

- **Integrare sistemi automatici di rilevamento** delle immagini tramite *hash* già identificati da ONG certificate (come StopNCII e TakeitDown), prevenendo la ripubblicazione dei contenuti;
- **Stabilire partnership operative con organizzazioni non profit** e professionisti del settore, per rafforzare la moderazione proattiva, soprattutto nei casi di segnalazione multipla o vulnerabilità delle vittime.

Per gli enti pubblici: offrire risposte concrete, accessibili e integrate

In Italia, la condivisione non consensuale di materiale intimo non è ancora riconosciuta dal Servizio Sanitario Nazionale come evento traumatico paragonabile a una violenza sessuale. Questo limita l'accesso diretto, immediato e gratuito a un supporto psicologico specifico per le vittime, salvo rientrino in percorsi già esistenti per altre forme di violenza.
Esistono servizi pubblici e convenzionati – come consultori, centri antiviolenza, CPS o neuropsichiatria infantile – ma non sempre sono formati o attrezzati per affrontare le conseguenze di questo tipo di esperienza. L'accesso, inoltre, può essere ostacolato da burocrazia, attese lunghe e risorse limitate, come nel caso del bonus psicologo.
Un ulteriore limite riguarda la formazione del personale sanitario, scolastico ed educativo, che non è sistematica né obbligatoria. Questo fa sì che segnali come isolamento, ansia, autolesionismo o calo del rendimento scolastico possano passare inosservati. Alcuni progetti educativi locali in collaborazione con il terzo settore esistono, ma restano iniziative sporadiche e non uniformi sul territorio nazionale.

Si raccomanda pertanto di:

- **Riconoscere la diffusione non consensuale di materiale intimo come esperienza potenzialmente traumatica**, prevedendo **accesso gratuito e diretto a percorsi di supporto psicologico**, senza vincoli burocratici;
- **Educazione digitale ed emotiva obbligatoria nelle scuole:** La prevenzione deve partire dall'educazione, e soprattutto i minori e gli adulti devono essere consapevoli dei rischi online, inclusi quelli legati alla sextortion. **Per migliorare la consapevolezza e la preparazione sui pericoli della rete, si raccomanda di rendere obbligatori i corsi di educazione digitale, sessuale ed affettiva nelle scuole**, focalizzandosi su come riconoscere i pericoli, adottare comportamenti sicuri in Internet e come questi debbano sempre essere basati sul consenso;
- **Formare il personale scolastico, sanitario e dei servizi sociali** al riconoscimento dei segnali indiretti (ritiro sociale, disagio emotivo improvviso, calo nel rendimento scolastico), in modo da poter intervenire in fase precoce e indirizzare le persone verso i servizi competenti;
- **Sensibilizzazione e formazione delle forze dell'ordine:** Le forze dell'ordine devono essere adeguatamente formate per affrontare i crimini a sfondo sessuale online, che

richiedono un approccio specifico e sensibile. **Per garantire un intervento tempestivo ed efficace, si raccomanda di avviare programmi di sensibilizzazione e formazione specifici per le forze dell'ordine**, affinché possano gestire in modo competente e empatico le denunce di reati a sfondo sessuale, offrendo supporto alle vittime e raccogliendo evidenze in modo appropriato.

- **Promuovere campagne pubbliche continuative** per informare i cittadini sui rischi e sui canali di aiuto, normalizzando la richiesta di supporto e contrastando lo stigma.

Si raccomanda infine:

- **La creazione di una banca dati centralizzata per la raccolta dei casi di *sextortion:*** La mancanza di dati sistematici rende difficile analizzare e rispondere efficacemente al fenomeno. **Per migliorare la comprensione e il monitoraggio della *sextortion*, cosìì come della condivisione non consensuale di materiale intimo, si raccomanda di creare una piattaforma centralizzata per la raccolta, analisi e condivisione di dati anonimi sui casi**, in collaborazione con forze di polizia, organizzazioni non profit e istituzioni.

CONCLUSIONE

L'analisi di oltre 1.000 casi di *sextortion* ci restituisce un quadro complesso e allarmante: chiunque può essere un bersaglio. Le vittime sono uomini e donne di ogni età ed estrazione sociale, segno che non esiste un profilo unico, né una categoria intrinsecamente "più debole". Gli uomini, spesso invisibili nella narrazione pubblica di questi reati, possono trovarsi in situazioni di estrema vulnerabilità, acuite dal silenzio e dal peso delle aspettative sociali legate alla mascolinità. Essere esposti, umiliati, ricattati, non rientra nell'immaginario dell'uomo forte e invulnerabile, e proprio questa distanza tra esperienza vissuta e stereotipi culturali rende ancora più difficile chiedere aiuto. Parallelamente, non si può ignorare che la maggior parte delle vittime di diffusione non consensuale di materiale intimo continua a essere composta da donne, le quali devono spesso affrontare anche un giudizio sociale impregnato di *victim blaming* e sessismo. Questo doppio standard, che colpisce in modo differente ma trasversale, evidenzia l'urgenza di decostruire modelli tossici di genere e promuovere una cultura del rispetto e del consenso.

Dal punto di vista psicologico, i reati sessuali digitali si rivelano particolarmente insidiosi: colpiscono la sfera più intima della persona, generando traumi profondi, spesso invisibili ma duraturi. La violenza non si esaurisce nel momento dell'abuso, ma si annida nella memoria, nella percezione di sé, nei rapporti interpersonali. La risposta psicologica deve quindi andare oltre l'assistenza clinica: deve offrire strumenti per la ricostruzione dell'identità e per la riconnessione con gli altri, aiutando le vittime a riappropriarsi della propria storia.

Sul piano giuridico e investigativo, la *sextortion* rappresenta una sfida crescente. Nonostante l'elevata diffusione del fenomeno, i riferimenti giurisprudenziali restano limitati, anche a causa della reticenza delle vittime nel denunciare. Tuttavia, la segnalazione è un passaggio fondamentale per avviare le indagini e smantellare le reti criminali – talvolta internazionali, talvolta composte da singoli soggetti – che sfruttano questi reati per ottenere guadagni rapidi e con rischi contenuti.

È evidente, dunque, che il primo e più efficace strumento di contrasto sia la prevenzione: un'educazione digitale diffusa, consapevole, trasversale. Un'educazione che inizi dalle scuole, con un approccio multidisciplinare capace di parlare ai giovani di consenso, empatia, rispetto reciproco, e di offrire gli strumenti per difendersi, ma anche per non diventare – magari inconsapevolmente – carnefici. Uscire da una cultura che normalizza la violenza e il ricatto, che impone ruoli di genere rigidi e penalizzanti, è possibile ma richiede un impegno condiviso: parlare, educare, ascoltare. Solo mediante un simile impegno collettivo potremo edificare una comunità in cui nessuna vittima venga lasciata sola.

GLOSSARIO

La condivisione non consensuale di materiale intimo, nelle sue diverse manifestazioni, come la *sextortion*, il *revenge porn* o la diffusione di *deepfake* pornografici, rappresenta un fenomeno complesso e in rapida evoluzione. Comprendere le differenze tra questi comportamenti è fondamentale non solo per riconoscere con precisione i reati, ma anche per attribuire loro la giusta gravità, sostenere adeguatamente le vittime e non perpetuare dinamiche di colpevolizzazione o confusione.
L'utilizzo di un linguaggio corretto e aggiornato è un elemento centrale nella lotta contro questi fenomeni: nominare correttamente un abuso significa vederlo, riconoscerlo e contrastarlo più efficacemente. Siamo consapevoli che le definizioni di questi concetti sono in continua evoluzione, seguendo i cambiamenti sociali, culturali e tecnologici. Per questo motivo ci impegniamo a mantenere una terminologia il più possibile aggiornata, affinché la nostra azione di sensibilizzazione, prevenzione e supporto alle vittime sia sempre rispettosa e fondata.
Di seguito proponiamo un glossario essenziale dei principali termini utilizzati all'interno di questo report.

Condivisione non consensuale di materiale intimo

La condivisione non consensuale di materiale intimo consiste nella diffusione, pubblicazione, cessione o invio a terzi di immagini o video sessualmente espliciti, destinati a rimanere privati, senza il consenso della persona rappresentata. In Italia è riconosciuta come reato ai sensi dell'art. 612-*ter* del Codice Penale (recante *Diffusione illecita di immagini o video sessualmente espliciti*). In inglese si utilizza la definizione *Image-Based Sexual Abuse*.

Sextortion

La sextortion è una forma di estorsione basata sulla minaccia di diffondere materiale intimo reale o creato artificialmente, se la vittima non fornisce ulteriori contenuti, prestazioni sessuali o denaro. Il fenomeno, che rientra nella più ampia categoria della condivisione non consensuale di materiale intimo, può essere opera sia di singoli individui che di gruppi criminali organizzati. Come la condivisione non consensuale di materiale intimo, anche nel caso della sextortion le conseguenze sono spesso gravissime: senso di impotenza, paura, isolamento sociale e rischio di vittimizzazione secondaria. Un esempio frequente è il ricatto ricevuto dopo uno scambio online apparentemente innocuo.

Revenge Porn

Il *revenge porn* è una sottocategoria della condivisione non consensuale di materiale intimo e si riferisce specificamente alla diffusione di contenuti sessuali, solitamente da parte di un ex partner, con finalità di vendetta. La differenza principale rispetto ad altre forme di diffusione non consensuale è la motivazione ritorsiva, legata spesso alla fine di una relazione. È importante sottolineare che il termine *revenge porn* viene spesso abusato o usato impropriamente: per questo motivo è preferibile utilizzare la locuzione più ampia e corretta condivisione non consensuale di materiale intimo, che copre tutti i casi, indipendentemente dalla motivazione.

Victim blaming

Il *victim blaming* è l'atteggiamento per cui la responsabilità di un reato viene, anche solo parzialmente, attribuita alla vittima, giustificando o minimizzando l'azione del colpevole. Non si tratta di un reato ma di una dinamica sociale tossica che aggrava il trauma della vittima, scoraggiando la denuncia e rafforzando specifici stereotipi. Frasi come "*se l'è cercata*" o "*non avrebbe dovuto inviare quelle foto*" sono esempi di *victim blaming*.

Cyber-bullismo

Il cyber-bullismo comprende atti di aggressione, molestia, intimidazione o umiliazione reiterati nel tempo attraverso strumenti digitali come social media, messaggistica o email. È regolamentato in Italia dalla legge n. 71/2017, con particolare attenzione alla tutela dei minori. A differenza del bullismo tradizionale, il cyber-bullismo si distingue per la velocità e l'ampiezza della diffusione del danno. Gli effetti possono includere depressione, ritiro scolastico, ansia e, nei casi estremi, pensieri suicidari. Un esempio è la creazione di profili falsi per ridicolizzare o denigrare una persona online.

Deepfake / Deepfake porn

Il *deepfake* si riferisce alla creazione di immagini o video manipolati tramite intelligenza artificiale per sovrapporre il volto di una persona su corpi o scene che non la coinvolgono realmente. Il *deepfake porn* riguarda specificamente la creazione di materiale sessualmente esplicito falso, in cui il volto della vittima viene inserito senza consenso. Negli ultimi anni sono emerse anche applicazioni e strumenti digitali accessibili a chiunque che consentono di "spogliare" artificialmente una persona a partire da una semplice fotografia, aumentando in modo esponenziale il rischio di abuso. Rispetto alla diffusione di materiale reale, il *deepfake porn* produce contenuti fittizi ma con effetti reali devastanti: violazione della reputazione,

trauma psicologico, perdita del controllo sulla propria immagine e difficoltà nel dimostrare la falsità del materiale.

Vittimizzazione secondaria

La vittimizzazione secondaria si verifica quando una vittima, dopo aver subito un reato, sperimenta ulteriori danni emotivi, psicologici o sociali a causa delle reazioni inadeguate di autorità, media, contesto sociale o istituzioni. Nello specifico deriva dal modo in cui la vittima viene trattata successivamente: ad esempio, attraverso giudizi, colpevolizzazione, mancato riconoscimento del danno subito o una gestione insensibile della denuncia.

Adescamento online

L'adescamento online consiste nell'attività di contattare e manipolare una persona tramite internet, con l'obiettivo di guadagnarne la fiducia per sfruttarla sessualmente, estorcerle materiale intimo o ottenere altri vantaggi. Quando la vittima è minorenne, l'adescamento assume un rilievo penale ancora più grave ed è specificamente normato (ad esempio, dall'art. 609-*undecies* del Codice Penale). Nel caso di maggiorenni, l'adescamento non configura un reato autonomo, ma può essere parte integrante di altri crimini come *sextortion* o truffe romantiche. Un esempio è il caso di un minore convinto da un adulto, attraverso false identità online, a inviare fotografie intime; oppure di un adulto persuaso a condividere materiale privato da una persona che si rivela poi un truffatore.

Digital trauma

Il Digital Trauma è una forma di trauma psicologico che deriva dall'esposizione diretta o indiretta a esperienze traumatiche mediate da tecnologie digitali, caratterizzata da una risposta emotiva intensa, persistente e disfunzionale a contenuti o interazioni online disturbanti, che può includere sintomi tipici del disturbo post-traumatico da stress (PTSD) e altre condizioni psicopatologiche correlate.

BIOGRAFIA

- **Bandura, A.** (1997). *Self-efficacy: The exercise of control*. W. H. Freeman.
- **Beck, J. S.** (2011). *Cognitive behavior therapy: Basics and beyond* (2ª ed.). Guilford Press.
- **Berne, E.** (1949). Transactional analysis: A new and effective method of group therapy.
- *American Journal of Psychotherapy, 3*(4), 546–556. https://doi.org/10.1176/appi.psychotherapy.1949.3.4.546
- **Carletto, S., Oliva, F., & Borgogno, F.** (2016). EMDR e interventi psicologici nel trattamento del trauma relazionale e online. *Psicoterapia Cognitiva e Comportamentale, 22*(3), 411–425.
- **Cass. pen. n.** 491954/2019.
- **Cass. pen. n.** 14075/2025.
- **Cass. pen. n.** 44408/2016.
- **Cass. pen. n.** 6017/2016.
- **Chatzittofis, A., et al.** (2020). Cyber sexual exploitation: Victimization and clinical implications. *International Journal of Environmental Research and Public Health, 17*(19), 7235. https://doi.org/10.3390/ijerph17197235
- **Cohen, S., & Wills, T. A.** (1985). Stress, social support, and the buffering hypothesis. *Psychological Bulletin, 98*(2), 310–357. https://doi.org/10.1037/0033-2909.98.2.310
- **Courtois, C. A., & Ford, J. D.** (2020). *Treating complex traumatic stress disorders: An evidence-based guide* (2ª ed.). Guilford Press.
- **Del Pizzo. Corona, A.** (2021). I sex crimes nell'era digitale. In *Reati informatici e investigazioni digitali*. Pacini Giuridica, Pisa.
- **De Santisteban, P., Gámez-Guadix, M., & Almendros, C.** (2020). Perpetual trauma loop: Understanding the long-term impact of online sexual coercion. *Child Abuse & Neglect, 108*, 104636. https://doi.org/10.1016/j.chiabu.2020.104636
- **Feinstein, B. A., et al.** (2014). Self-perceived barriers to seeking mental health services among victims of online sexual coercion. *Psychological Services, 11*(4), 390–397. https://doi.org/10.1037/a0037360
- **Hayes, S. C., Strosahl, K. D., & Wilson, K. G.** (2016). *Acceptance and commitment therapy: The process and practice of mindful change* (2ª ed.). Guilford Press.
- **Kabat-Zinn, J.** (1990). *Full catastrophe living: Using the wisdom of your body and mind to face stress, pain, and illness*. Delacorte.
- **Karpman, S. B.** (1968). Fairy tales and script drama analysis. *Transactional Analysis Bulletin, 7*(26), 39–43.

- **Levin, M. E., et al.** (2022). Shame, social connectedness, and distress among victims of sextortion: A clinical perspective. *Journal of Contextual Behavioral Science, 24*, 64–72. https://doi.org/10.1016/j.jcbs.2021.12.002
- **Luberto, M.** (s.d.). "Sex-torsion" via web e minaccia a mezzo ransomware: la nuova frontiera del delitto di estorsione. In *Cybercrime II edizione*, collana *Omnia Trattati giuridici* (A. Cadoppi, S. Canestrari, A. Manna, M. Papa, dir.). UTET Giuridica, Milano.
- **Minuchin, S.** (1974). *Families and family therapy*. Harvard University Press.
- **Notté, R. J.** (2024). Exploring the impact of sextortion on adult males: A narrative approach. *Technology in Society, 78*.
- **PermessoNegato – Sidoti, C., Beckman, E. M., et al.** (2023). *IBSA 2023 Report: Image-Based Sexual Abuse all'interno dei Gruppi Telegram* https://www.permessonegato.it/wp-content/uploads/2024/09/PermessoNegato_IBSA2023_Report_ITA.pdf
- **Polizia Postale e per la Sicurezza Cibernetica** (2024). *Report annuale 2024* https://www.poliziadistato.it/statics/40/2024-report-def.-sppsc.pdf
- **Rapkoch, M.** (2024). The perpetual trauma loop: Understanding chronic threat exposure in sextortion cases. *Journal of Traumatic Stress Studies, 37*(1), 12–25.
- **Save the Children** (2024). *Le ragazze stanno bene? Indagine sulla violenza di genere onlife in adolescenza* https://s3-www.savethechildren.it/public/files/uploads/pubblicazioni/le-ragazze-stanno-bene_1.pdf
- **Segal, Z. V., Williams, J. M. G., & Teasdale, J. D.** (2018). *Mindfulness-based cognitive therapy for depression* (2ª ed.). Guilford Press.
- **Shapiro, F.** (2018). *Eye movement desensitization and reprocessing (EMDR) therapy: Basic principles, protocols, and procedures* (3ª ed.). Guilford Press.
- **Southwick, S. M., & Charney, D. S.** (2012). *Resilience: The science of mastering life's greatest challenges*. Cambridge University Press.
- **Tribunale di Perugia**, sez. penale, sent. 26 giugno 2017, Pres. est. Loschi.
- **Wang, F.** (2024). Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. *Sexual Abuse*. https://journals.sagepub.com/doi/10.1177/02697580241234331#tab-contributors