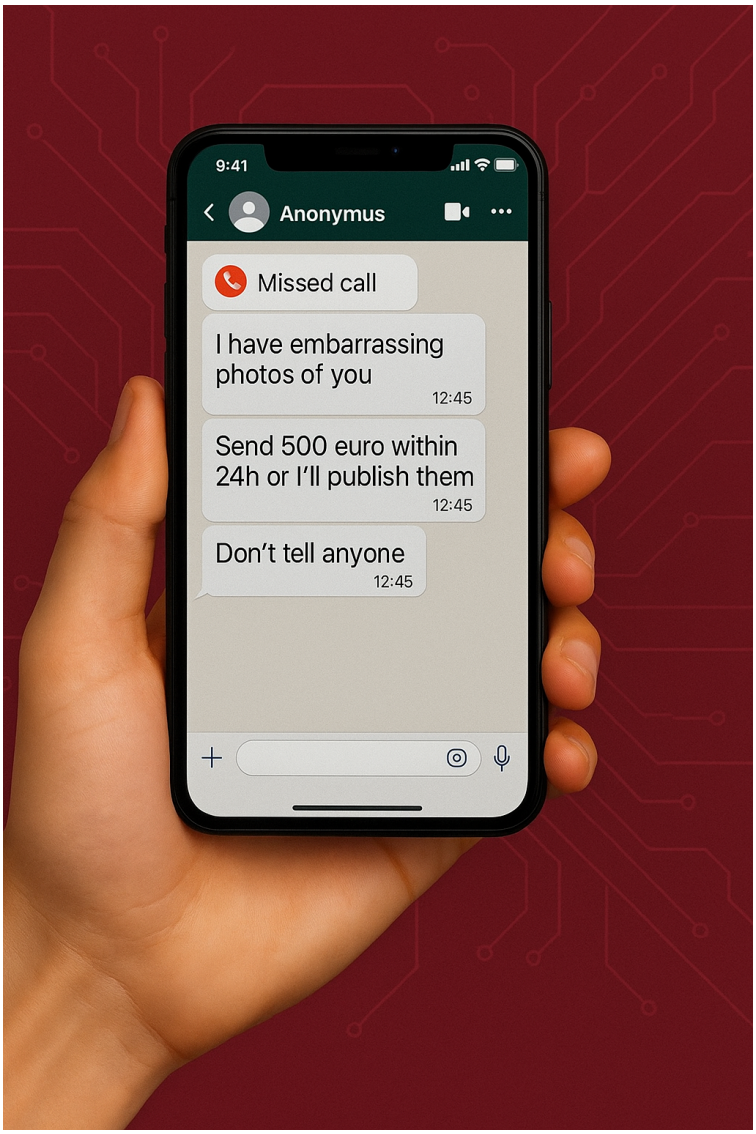
"ANSWER ME QUICKLY"

A MULTIDISCIPLINARY ANALYSIS OF MALE SEXTORTION IN ITALY



REPORT 2025

PERMESSONEGATO ASSOCIATION

Edited by:

Edel Margherita Beckman, with a degree in Law and a specialization in Clinical Criminology and Victimology, focuses on gender-based violence and digital criminology, with particular attention to the non-consensual sharing of intimate material and cyberbullying. Her work examines the intersection between technology and human relationships, analyzing how digital tools can amplify dynamics of control and abuse. She conducts training and prevention activities in schools, promoting a culture of consent and dismantling gender stereotypes. Since 2020, she has been part of the PermessoNegato team, and since 2024 she has served as Training Program Director.

Ilaria Lavarini holds a Master's degree in Clinical and Dynamic Psychology, with several years of experience in the field of socio-economic and psychological distress. She has collaborated with organizations such as Caritas Italiana, the International House of Women in Rome, and anti-violence centers (CAV), working to protect the most vulnerable individuals. Since 2022, she has been a volunteer with PermessoNegato. She is currently completing a Master's program in Business Innovation Coaching for Executives, as well as training as a Safety Instructor with a focus on psychosocial risks (stress, burnout, workplace harassment).

Matilde Bellingeri, criminal lawyer at the Milan Bar. From 2021 to 2025, she was part of the legal team at PermessoNegato. Alongside her legal work, she is involved in legal education in secondary schools, helping to promote a culture of legality among young people. She is currently a PhD student in Criminal Law at the University of Verona.

Noemi Tentori holds a degree in "Sicurezza dei Sistemi e delle Reti Informatiche" and specializes in cybersecurity, antifraud measures, and business continuity management within the corporate sector. Since 2021, she has volunteered with PermessoNegato. Deeply interested in Open Source Intelligence, her personal research also encompasses topics such as online individual reputation, the processing of sensitive data through the Internet, and hate speech.

Suggested citation: *Beckman E. M., Lavarini I., Bellingeri M., & Tentori N. (2025, May) "Answer me quickly": A Multidisciplinary Analysis of Male Sextortion in Italy.*

INDEX

PERMESSONEGATO

PermessoNegato *(literally "Permission Denied")* is an Italian non-profit organization founded in Milan in late 2019 that works to support victims of the non-consensual sharing of intimate material (also known as IBSA – Image-Based Sexual Abuse), a crime that in recent years has gained both visibility and severity. Since it was founded, *PermessoNegato* has emerged as one of the leading national and international organizations in this field, responding to victims' needs through a multidisciplinary approach that combines technological, legal, and psychological support.

To date, the organization has assisted over **4,000 victims**, building a network of qualified professionals to help individuals remove intimate content shared without their consent, protect their online reputation, and provide free and immediate assistance. Victims contact *PermessoNegato* from all over the world, and in response to this global demand, the organization offers support in multiple languages, ensuring accessible help for anyone in need, regardless of their location.

The non-consensual sharing of intimate material is a complex crime that requires an integrated response to be addressed effectively. For this reason, the *PermessoNegato* team includes professionals from diverse backgrounds, such as lawyers, psychologists, criminologists, online reputation specialists, and cybersecurity experts.

1. **Preventive removal –** *PermessoNegato* was the first association in Europe to activate a preventive removal service, an initiative that allowed victims and potential victims to upload their intimate content through a link provided to the association by Facebook, which was then shared with the person concerned. If these contents were uploaded to Facebook or Instagram, they would be automatically removed and could not be uploaded again. Since 2023, victims and potential victims have been redirected to the *StopNCII* platform for adults and *Take It Down* for minors; both portals allow users to independently initiate the preventive removal process. One of the most significant advancements has been the involvement of multiple platforms, which ensures far wider coverage in cases of non-consensual sharing of intimate content. The process, which follows the same model previously adopted, begins with selecting intimate images or videos on one's device to generate a unique digital fingerprint ("hash"). Only the hash is sent to the platform, while the original content remains private and is never uploaded online. Once the case is successfully registered, the user receives a reference number to monitor the request's status. Participating companies compare the hash against their systems and, if matches are found, proceed with the removal of the content.

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?jid=90000262000695&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: Procedure used until 2022

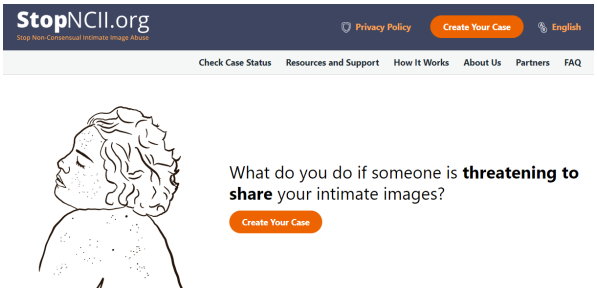


Fig. 2: Platform StopNCII.org for adults

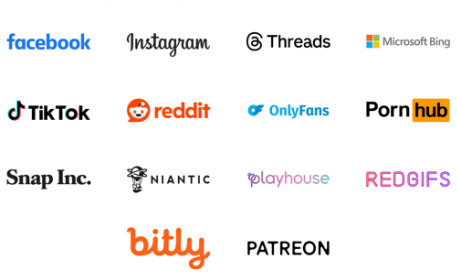


Fig.3: Partner participating in StopNCII.org

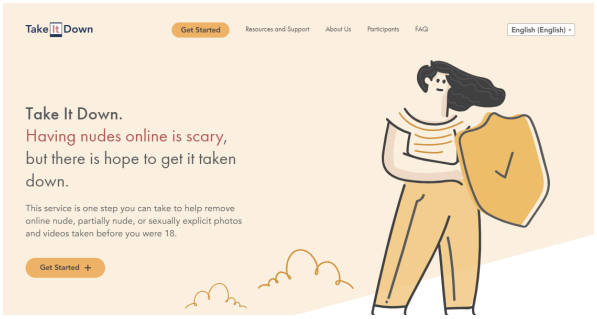


Fig. 4: PlatformTake it Down for minors

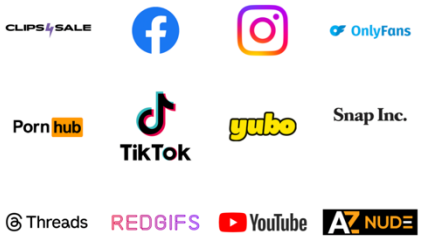


Fig. 5: Partner participating in Take it Down

2. **Removal of Published Content and Reporting of Accounts:** In combating the unlawful dissemination of intimate content already published online, the organization actively reports such material to digital platforms, requesting the immediate removal of links provided by victims. Over time, *PermessoNegato* has built an effective network of collaboration with numerous adult content platforms, achieving significant results especially through its partnership with Aylo, one of the industry's leading actors.

Unfortunately, many pornographic websites (particularly those that are unmoderated or poorly regulated) can become fertile ground for the spread of this type of material, fueling dynamics of violence, blackmail, and public humiliation. For this reason, it is considered essential not only to act after the fact through removal, but also to work in synergy with platforms to promote greater responsibility in the management and moderation of user-uploaded material. A key component of the organization's activities is actively identifying and reporting accounts (primarily on Meta platforms) involved in the distribution or threatened distribution of unlawful content, seeking their prompt removal.

3. **Legal Guidance and Forensic Preservation:** The association offers each victim a free legal consultation with one of the lawyers on its team, who cannot represent the individual in court but will guide them through an initial orientation (a step that has often proved essential for those who turn to *PermessoNegato)*. This consultation helps victims clarify their rights, understand the next legal steps, and overcome the fear of possible secondary victimization, an unfortunately common experience for those affected by digital violence. Should the person decide to pursue legal action, *PermessoNegato* also supports the activation of forensic preservation, a service that legally certifies the online presence of unlawful or defamatory content through a procedure recognized at the judicial level. This process is vital for safeguarding oneself and collecting admissible evidence in court. The service is made possible through collaboration with specialized external partners.

4. **Psychological Support:** Through its network of partners, the association also provides free psychological assistance to anyone seeking professional help in managing the emotional consequences of their experience.

PermessoNegato collaborates with leading global companies and platforms to deliver concrete support to victims of the non-consensual sharing of intimate material. Key partners include Meta (owner of Facebook, Instagram, and WhatsApp), Aylo (owner of adult platforms such as Pornhub), TikTok, and Google. These partnerships allow the organization to obtain swift, direct action for the removal of harmful content, while also fostering public awareness of the need to safeguard individuals' privacy and dignity online.

IMAGE-BASED SEXUAL ABUSE

Non-Consensual Sharing of Intimate Material

The non-consensual sharing of intimate material (often mistakenly referred to as "Revenge Porn") refers to the distribution of intimate images or videos, intended to remain private, without the consent of the people represented. In Italy, this offence is criminalised under Article 612-*ter* of the Penal Code.

It is important to note that the term *"revenge porn"* is both limiting and inaccurate, as it suggests that the phenomenon is always linked to some form of revenge, whereas in reality it can stem from multiple motivations, including coercion, psychological manipulation, extortion, or the simple desire to humiliate or harm someone. Not all victims are involved in dynamics of revenge, and often the offence is unrelated to intimate relationships or the breakdown of a romantic partnership.

Using accurate terms like "Non-Consensual Sharing of Intimate Material" or "Image-Based Sexual Abuse, ensures that the gravity of the offence is properly acknowledged, while avoiding any minimisation of the victim's experience. Such terminology more effectively conveys the violent and damaging nature of this conduct, which can have devastating consequences for individuals involved.

Another phenomenon that falls within the scope of non-consensual sharing of intimate material is sextortion, which involves the threat of disseminating intimate content to extort money, goods, or other favours (often of a sexual nature) from victims. Sextortion is typically perpetrated via the internet and social media, where offenders obtain compromising material (e.g., intimate photos or videos) and threaten to publish it online and/or send it to family and friends if their demands are not met.

In recent years, *PermessoNegato* has observed a significant increase in the number of male victims involved in sextortion cases. This trend has highlighted the need for further research and analysis on the phenomenon, not only from a statistical perspective but also from legal, psychological, and criminological standpoints.

RESEARCH LIMITATIONS

This report focuses primarily on male victims of sextortion, a group that, as will be shown, has traditionally been under-researched both in Italy and abroad.

To protect the privacy and safety of victims, *PermessoNegato* collects only the information strictly necessary to provide immediate and targeted support when individuals seek assistance. Consequently, many potentially valuable details for research purposes, such as specific elements of the offenders' *modus operandi*, the psychological profiles of victims, or

the precise characteristics of the contexts in which these crimes occur, remain unknown as of today.
The decision to limit data collection stems from the need to shield victims from potential further psychological harm and from risks linked to the unnecessary disclosure of personal information. Indeed, many of those who contacted *PermessoNegato* do it in a state of panic, shame, and vulnerability, making it essential to respect their desire for anonymity and confidentiality.
As a result, several variables that would be crucial for a deeper and more comprehensive understanding of the phenomenon remain only partially explored. At present, there is no significant research on this topic in Italy, and international investigations are limited too. The less availability of specific data and studies makes it particularly difficult to draw an accurate picture of the extent and characteristics of this phenomenon in the global context. This lack of literature can hinder both the understanding of the scale of the problem and the development of effective preventive and support policies.
Another significant limitation lies in the general underreporting of sexual offences. The number of reported cases is consistently lower than the actual incidence of such crimes, largely due to victims' reluctance to come forward because of fear, shame, or concerns about not being believed. This underreporting makes analysing the phenomenon more complex, as the available data do not reflect the full scope of victims affected by this type of offence.

Data Anonymization

The data analysed in this report originate solely from cases reported to PermessoNegato. The sample is self-selected, composed of victims who voluntarily reached out to the association seeking support. As such, the findings cannot be considered representative of the broader male population affected by the phenomenon. They do, however, offer a valuable insight into emerging patterns, recurrent issues, and unmet needs.
From the outset, all information was anonymized, and no personally identifiable data were ever collected. The entire process was conducted with the utmost respect for the confidentiality of victims and in full compliance with the General Data Protection Regulation (GDPR – EU Regulation 2016/679). The objective has never been to trace individual profiles, but rather to gain an understanding of the phenomenon in its complexity, while consistently placing the protection and dignity of those involved at the centre.
This research also includes anonymized screenshots, directly provided by victims at the time of reporting. All identifying elements were meticulously removed, and the materials are used solely for study and analytical purposes, ensuring full respect for the privacy and safety of the individuals represented.
While the protection of victims remains the foremost priority, PermessoNegato recognizes the need to expand data collection in a more systematic way in the future. Strengthening support

practices and fostering an environment that is both safe and reassuring could facilitate the gathering of broader and more detailed information. Such an approach would enable more effective monitoring of the phenomenon's progression, a deeper understanding of its underlying dynamics, and the design of increasingly targeted intervention strategies. Any future expansion of data collection will, however, remain firmly anchored in the strictest respect for privacy and the well-being of victims, who continue to represent the central focus of every initiative.

LEGAL PROFILES

From a legal perspective, sextortion refers to conduct in which the perpetrator threatens to disclose information or distribute sexually explicit images that could harm the victim's dignity, reputation, or right to privacy, in order to coerce them into performing or refraining from a certain act.

This conduct can take various forms. Generally, we can distinguish between cases where images are obtained through hacking — when the cybercriminal gains unauthorized access to the victim's computer systems or cloud storage and retrieves sexually explicit content — and cases where the victim is directly involved from the outset.

In the former scenario, the victim is contacted solely for the purpose of blackmail, typically through emails or messages containing threats and demands for payment in exchange for not uploading the material online. In the latter, the cybercriminal builds a relationship of trust with the victim with the aim of obtaining explicit content, luring them into virtual environments such as social networks, chat rooms, or dating platforms using a fake profile created ad hoc.

As will be discussed later, the sexual theme is often introduced gradually to desensitize the victim and encourage them to share intimate information or images, which are later used for extortion.

The crime of sextortion in Italy

Sextortion is not specifically recognized as a distinct criminal offense under Italian law. Depending on how the conduct is carried out, it may fall under several provisions of the Italian Criminal Code, including:

- Extortion (Article 629)
- Defamation (Article 595)
- Unlawful interference with private life (Article 615-bis)
- Private violence (Article 610)
- Threats (Article 612)

In most cases, sextortion is prosecuted under the crime of extortion, which generally involves coercing someone — through violence or threats — into doing or refraining from doing something. This crime protects both the victim's property and their moral freedom.
When extortion is committed through sextortion, the victim's rights to personal identity, privacy, and protection of personal data are also violated, in addition to their property and moral freedom.

Elements of the crime: objective component

To qualify as extortion, the conduct must involve violence or threats. The crime consists of four key elements:

1. Psychological coercion of the victim;
2. The victim's compelled action or omission;
3. Resulting harm to the victim;
4. Unjust profit for the perpetrator or others.

Based on available case law and data from PermessoNegato, sextortion typically involves:

- threats to disseminate intimate images or videos;
- the creation of a credible fear of future harm;
- use of remote communication tools (e.g., messaging apps, email).

The threat must be capable of coercing the victim into taking a specific action or omitting one. In sextortion cases, the psychological pressure is often severe and difficult to dismiss. The fear of social exposure and reputational damage—especially due to the viral and irreversible nature of online content—makes the coercion particularly effective.
Once uploaded online, explicit material is extremely difficult, if not impossible, to remove completely. Content may be duplicated across platforms, stored in cache memory, or downloaded and redistributed, making permanent deletion practically unachievable. To establish the crime, the coercion must cause the victim to act or refrain from acting. This must result in:

- unjust profit for the offender (not necessarily monetary);
- economic damage to the victim (either direct or indirect).

Unjust profit can include any benefit or advantage not protected by law. For example, in Criminal Cassation No. 44408/2016, a defendant threatened to disclose an explicit video unless the victim resigned as a municipal councilor, hoping to replace her on the council as the first unelected candidate. The court considered this indirect economic damage, as it involved loss of public compensation and allowances.

In Criminal Cassation No. 14075/2025, the Court reaffirmed that unjust profit includes any advantage sought by the perpetrator that is not legally grounded, even if not economic in nature.

Subjective element and timing of the offence

Extortion is a general intent crime. To convict, it must be proven that the perpetrator intended to coerce the victim into causing harm to themselves or others, for the purpose of obtaining unjust profit.
The offense is considered committed at the time and place where both the unjust profit and the damage occur. However, in cases involving online sexual extortion and electronic payments (e.g., via bank transfer, prepaid cards, or e-money), the temporal and geographical disconnection between the perpetrator and the victim creates jurisdictional complexities.
This issue is debated. According to a ruling by the Court of Perugia[1] (26 June 2017), jurisdiction lies where the offender receives the profit (i.e., where the money is collected or used). However, this view is not universally accepted.
Later decisions (e.g., Criminal Cassation No. 491954/2019)[2] have held that when fraud involves rechargeable payment cards (such as Postepay), the crime occurs where the victim makes the payment, and this determines territorial jurisdiction.
Furthermore, if payment is made by standard bank transfer (less common in PermessoNegato cases), jurisdiction would lie with the court in the district where the funds are credited, due to the non-simultaneity of transfer and receipt.

International regulations

In Italy, as noted, sextortion is not defined as a standalone offense. Instead, it is prosecuted under existing laws relating to extortion, privacy violations, and the unlawful dissemination of intimate content. This fragmented regulatory framework can make it more difficult to report and legally classify such offenses.
By contrast, some countries have taken more targeted approaches:

- **Philippines:** the Cybercrime Prevention Act (Republic Act No. 10175 of 2012) addresses cybercrimes, including those of a sexual nature. While it does not explicitly use the term "sextortion," it criminalizes related behaviors, such as online extortion and the non-consensual dissemination of intimate material.
- **United States:** there is no federal law specifically addressing sextortion, but many U.S. states have enacted relevant legislation. For example:

[1] For further information: https://archiviodpc.dirittopenaleuomo.org/upload/1486-sentenzaperugiapostepay.pdf
[2] For further information: https://www.giurisprudenzapenale.com/wp-content/uploads/2019/07/cass-pen-ssuu-2019-28911.pdf

    - California: Criminal Code § 647j(4) criminalizes the non-consensual dissemination of intimate images ("revenge porn"), which may encompass cases of sextortion.
    - Texas: Criminal Code § 16.05 punishes the unlawful disclosure of electronic communications, applicable to sextortion scenarios.
- **Canada:** the Criminal Code has been amended to criminalize the non-consensual distribution of intimate images. In a recent case, a man was convicted for extorting sexually explicit images from a minor, demonstrating the law's effectiveness in prosecuting sextortion-related offenses[3].

The case for a specific sextortion offense in Italy

Introducing a dedicated offense for sextortion into the Italian legal system could provide several key benefits:

- **Legal Clarity:** a precise definition would help victims better understand their rights and the appropriate procedures for reporting offenses.
- **Data Collection:** a specific offense would enable more accurate statistical tracking, which is essential for designing effective prevention policies and building consistent case law.
- **Public awareness:** recognizing sextortion as a standalone crime would help raise awareness and reduce the stigma often experienced by victims, who may otherwise hesitate to come forward.
- **Victim Protection:** dedicated legal tools would strengthen the ability of law enforcement and the judiciary to protect victims and prosecute offenders more effectively.

MEANS OF OBTAINING EVIDENCE

Before filing the criminal complaint, it is crucial to collect evidence that proves the offense while the material is still available online, even though this process may be emotionally difficult for the victim.

[3] https://www.sfchronicle.com/crime/article/sextortion-sentence-contra-costa-20055506.php

Forensic Acquisition

The entry into force of Law No. 48/2008[4] marked a fundamental step in aligning the Italian criminal procedural system with European standards on the collection, preservation, and use of digital evidence. In particular, Article 8 of the aforementioned law provides that the judicial authority may order the acquisition of information contained within an IT or telematic system by *"adopting technical measures aimed at ensuring the preservation of the original data and preventing its alteration"*. The underlying principle is that when the acquisition and preservation phases are carried out in accordance with **uniform and rigorous standards**, the evidence thus collected can subsequently be deemed **admissible and reliable by the judge in establishing the facts of the case**. The copy produced under these specific protocols is referred to as a forensic copy and is typically carried out by digital forensic experts or accredited professionals. However, in some cases, legal entities or other professional figures may also be involved, depending on the jurisdiction and the nature of the investigation.

The Evidentiary Value of Screenshots

The most immediate and accessible method for the average user of an electronic device remains taking a screenshot on a computer or smartphone. The Italian Supreme Court of Cassation, in its recent decision No. 34212/2024, reaffirmed the established case law holding that screenshots have full evidentiary value in judicial proceedings. This is because a screenshot is capable of capturing the exact moment a message is received or an image is sent, thereby ensuring proof of its existence and content. It should be noted that, in cases where the authenticity of a screenshot is questioned, the Judge may order the seizure of the mobile device (either of the defendant or the injured party) to allow for the necessary technical examinations. It is therefore essential to preserve chat histories on the device's memory and, for long-term secure storage, to also save them on an external medium. By retaining the original file, the risk of easy challenges during trial is significantly reduced.

[4] https://www.parlamento.it/parlam/leggi/08048l.htm

DATA

The present study relies on data collected by the association between **January 2020 and December 2024,** concerning individuals (both Italian and non-Italian) who reported being victims of sextortion and sought assistance from *PermessoNegato*. The dataset comprises **1,086 documented cases**, increasing from **41 in 2020 to 392 in 2024.** Overall, the data reveal a consistent upward trend across the observation period, with the sole exception of 2023, which registered a minor decline. These figures underscore the sustained growth of the phenomenon over time.

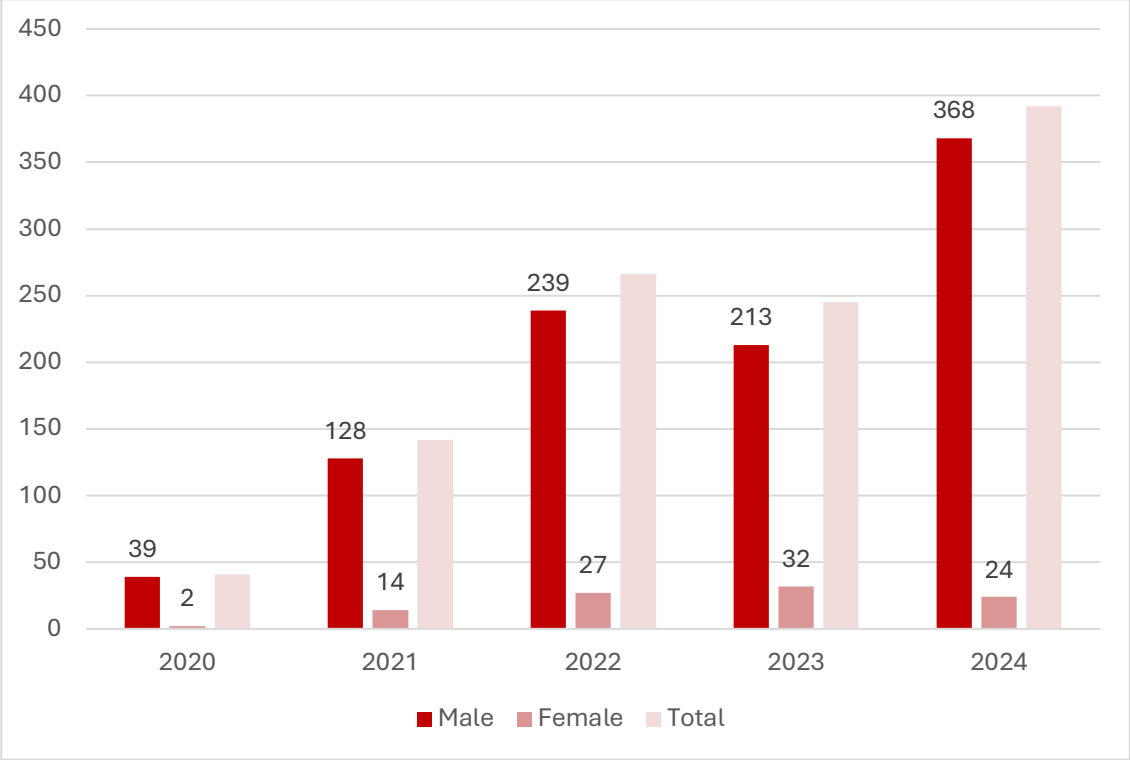


Fig.6: Victims of sextortion who contacted PermessoNegato over the four-year period

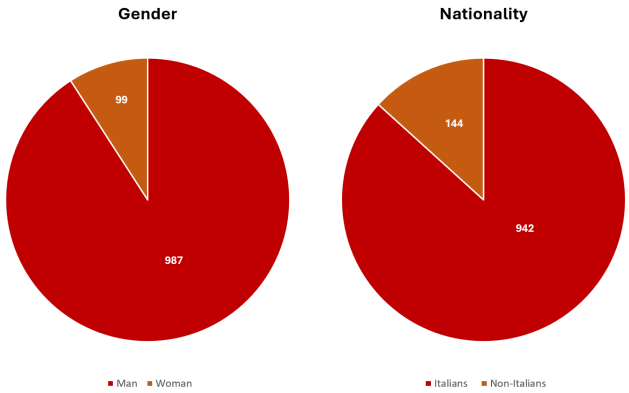


Fig.7: Gender and Nationality

One of the primary objectives of this research is to **raise public awareness** about the increasing number of male victims of sextortion, as well as about the crime more broadly. Although the phenomenon of non-consensual sharing of intimate material has historically been predominantly associated with women, the data collected indicate a significant rise among men in cases specifically involving sextortion.

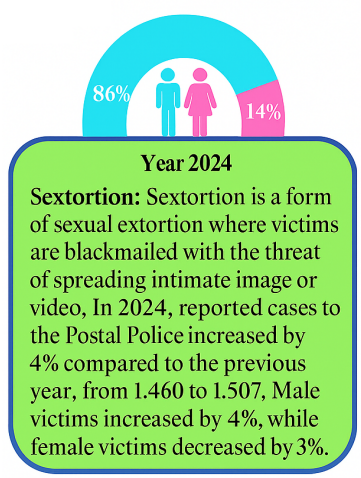
In the case of online sextortion, the traditional pattern **undergoes a significant shift.** Evidence collected by PermessoNegato, together with sources such as reports from the Postal Police, points to a clear reversal compared to more "classic" forms of non-consensual image distribution: the overwhelming majority of sextortion victims are men. This is a pronounced and meaningful difference that calls for a re-evaluation of current approaches and intervention strategies. At the same time, it must be acknowledged that, across the broader spectrum of crimes involving the non-consensual dissemination of intimate material, women continue to account for the vast majority of victims.

A substantial body of research[5] confirms that women remain, in most cases, the primary targets of these forms of violence, and that this trend, regrettably, shows no indication of reversing. Gender therefore continues to be a critical variable, carrying significant implications for prevention policies, awareness-raising efforts, and victim support mechanisms.
The research further underscores the urgent need to reinforce prevention strategies, particularly in light of the growing use of social media among increasingly younger age groups - an issue that will be examined in greater detail in the following sections.

One of the most striking aspects emerging from the analysis of sextortion cases is the difficulty of identifying **a specific target group of victims**, alongside the increasing number of male victims. Experience accumulated over the years clearly shows that there is no single recognizable profile: *PermessoNegato* has been contacted by individuals of widely varying ages (excluding minors, ranging from **18 to 75**), with no strong prevalence in any particular age group. Victims come from diverse social, cultural, and geographical backgrounds; they identify with different sexual orientations; and they include both Italian and foreign nationals, as well as individuals who are married, cohabiting, single, or in complex relational circumstances. Some had extensive familiarity with social media and digital technologies, while others had little to none. This variety of profiles presents an extremely **heterogeneous picture**, underscoring the cross-cutting nature of the phenomenon.

[5] For further information:
1. European Institute for Gender Equality: https://eige.europa.eu/mk
2. Revenge Porn Helpline: https://revengepornhelpline.org.uk
3. Report on non-consensual sharing of intimate material: https://www.permessonegato.com/doc/PermessoNegato_IBSA2023_Report_ENG.pdf

Sextortion thus emerges as a crime that **transcends narrowly defined victim categories,** representing instead a potential threat to anyone engaging - even sporadically - with digital technologies. This breadth of exposure presents a major challenge, not only for prevention efforts but also for the design of effective support systems able to respond to the diverse needs of victims, who vary significantly in age, background, experience, and personal resources.



	Cases handled	Male victims	Female victims	People under investigation
Year 2024	1.507	1.295	212	130
Year 2023	1.460	1.241	219	165
Var. %	+3%	+4%	-3%	-21%

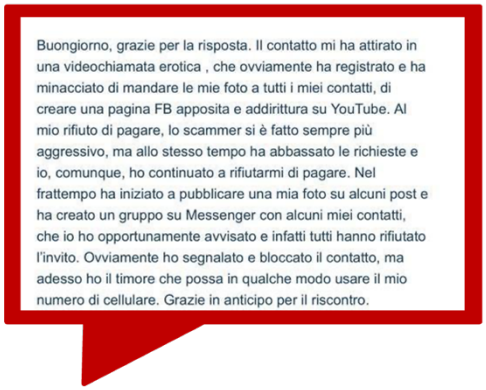
Fonte: 2024 Annual Report of the Italian Postal and Communications Police[6]

THE STAGES OF GROOMING

Over the years, recurring patterns have emerged that can be interpreted as a sequential model of manipulative strategies employed by offenders. This process unfolds through a series of structured phases, each designed to gradually condition the victim by fostering a deceptive sense of trust and emotional intimacy within a virtual relationship. Such dynamics of victim–offender interaction ultimately facilitate the perpetrator's ability to achieve the intended outcome: **coercion through blackmail.**

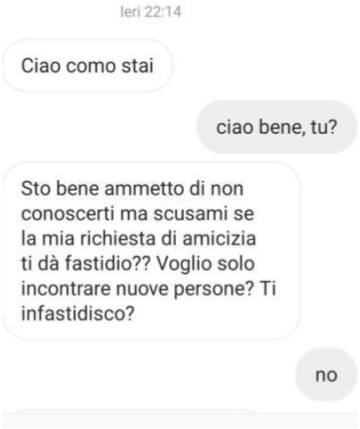
Drawing on the narratives of individuals who contacted *PermessoNegato* over the years, it has been possible to identify distinct stages typically observed during the grooming process:

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



Translation of the original request in Italian: *Hi, thanks for your reply. The contact lured me into an erotic video call, which he obviously recorded, and then threatened to send the video and my photos to all my contacts, even saying he would create a Facebook page or upload them on YouTube. When I refused to pay, the scammer got more aggressive, but at the same time lowered his demands. Still, I kept refusing to pay. In the meantime, he started posting one of my photos to some people and even created a Messenger group with some of my contacts, which I quickly reported and made sure not to join. Of course, I reported and blocked him, but now I'm worried he might somehow use my phone number. Thanks in advance for your feedback.*

1. **Initiating Contact and Constructing False Intimacy:** The first stage typically occurs through social media platforms, online chatrooms, or dating applications. This phase primarily revolves around the construction of an **apparently genuine relationship,** intended to establish an initial connection between the perpetrator and the victim. The approach generally involves presenting oneself as trustworthy, empathetic, and genuinely interested in the victim's life. Initial exchanges typically revolve around some **generic personal topics:** however, they are strategically structured to extract sensitive information from the victim, including details about habits, social networks, and personal interests. Such information is gathered not only through the ongoing interaction, but also by exploiting the victim's profile on social media, where elements of private life) such as friends lists, photographs, or daily routines (are often publicly accessible. The **appropriation of personal data** constitutes a crucial mechanism in the construction of a "false intimacy," which can subsequently be leveraged for further fraudulent purposes (Spender, 2012). In almost all documented cases, victims are approached by accounts that appear to belong to women, often characterized by images of highly attractive or sexually provocative females. The deployment of the female body as a manipulative tool is not merely an act of deception but constitutes a form of exploitation that reinforces dynamics of domination and control. The deliberate use of such images for manipulative purposes not only reduces women to objects of desire, but also perpetuates a **distorted and stereotypical representation of femininity.** Within a broader social context in which the female body is constantly exposed and instrumentalized to attract attention and generate approval, the use of fabricated images in grooming schemes contributes to a degrading narrative and reality.



Translation of the original request in Italian:
A: *Hi, how are you?*
B: *Hi, I'm good, you?*
A: *I'm fine. I admit I don't know you, but sorry if my friend request bothers you?? I just want to meet new people. Am I bothering you?*
B: *No*

This phenomenon extends beyond a simple breach of privacy; it reflects a broader process of commodification of the female body, in which women are reduced to aestheticized and sexualized constructs, deprived of their humanity, and transformed into instruments of manipulation. The dissemination of such imagery further distorts interpersonal relationships, reinforcing a dangerous perception of women as objects of male gratification. In doing so, this dynamic not only perpetuates the objectification of the female body but also consolidates cultural frameworks that legitimize and normalize its utilitarian exploitation.

2. **Shifting toward sexual topics:** Once the initial connection has been established and sufficient personal information has been gathered, the perpetrator gradually shifts the dialogue toward increasingly intimate themes, with the strategic aim of weakening the victim's psychological defenses. This progression can be explained through the notion of *desensitization*, a process by which the offender attempts to render the sexualization of the exchange seemingly natural and unproblematic. Psychological manipulation intensifies as the offender capitalizes on the emotional tone of an ostensibly "intimate" conversation to redirect it toward sexual content. This stage may also be interpreted through the lens of *gaslighting* (Schechter, 2002), a psychological tactic that induces individuals to doubt their own perception of reality. Within this dynamic, the victim is gradually led to believe that the sexualized nature of the interaction is both legitimate and desirable, even as it entails a progressive erosion of personal boundaries.

Translation of the original request in Italian:
A: *Please don't disappoint me, send me a video showing your face while [redacted].*
B:*Uuuuu me too!*
I'll try later, right now I can't.
A: *Just a short video, please.*
B: *I'll send it to you as soon as I can.*
Don't disappoint me, we're so close to meeting.

3. Recording and Blackmail. Once the victim has become involved in an intimate conversation, this interaction is often **secretly recorded**, taking advantage of the individual's vulnerability and lowered inhibitions. After obtaining compromising material (typically photos sent by the victim, or audio and video recordings of a sexual nature) the perpetrator threatens to disclose this information in order to coerce the victim into complying with their demands. This dynamic illustrates how the relationship between offender and victim becomes a **game of power**, in which the perpetrator exercises direct control over the victim's life by threatening to expose their intimacy if their requests are not fulfilled. Within this context, the victim's social isolation (often exacerbated by online vulnerability and the absence of immediate support) further strengthens the effectiveness of the blackmail. The selection of victims through social media and other online platforms is intrinsically tied to the virtual character of the relationships offender construct. Scholarship in the sociology of information technologies (Turkle, 2011) demonstrates that physical distance and technological mediation can reduce both the perception of "danger" and the sense of social oversight, thereby heightening individuals' susceptibility. Within anonymous online environments, victims frequently lower their guard and act more spontaneously or disinhibitedly, conditions that perpetrators deliberately exploit to manipulate and gain leverage. **A marked gendered asymmetry also emerges in the treatment of victims.** Men are more commonly pressured to provide money in exchange for silence or the non-disclosure of compromising material, whereas women are almost invariably coerced into producing and sharing further intimate images. This pattern underscores a deeply entrenched practice of female body exploitation and sexual objectification (Fredrickson & Roberts, 1997), wherein a woman's value is reduced to her sexual availability and her body becomes a transactional commodity. Such differentiation reflects structural sexism: while men are targeted primarily through their economic capacity, women's vulnerability is reinforced by their persistent framing as bodies to be consumed rather than as autonomous subjects. This constitutes a double violence: both digital and sexual, but also cultural, as it reflects and amplifies pre-existing gender inequalities within society.

PLATFORM USAGE AND FINANCIAL EXPLOITATION

The analysis of sextortion cases presented in this report suggests a troubling hypothesis: many of these offences may be linked to a highly organized criminal structure. The techniques used to lure victims display remarkable consistency across cases involving both Italian and non-Italian individuals, indicating the presence of a deliberate and coordinated operational strategy on the part of the perpetrators. A common feature in numerous sextortion cases is the use of multiple platforms to achieve the ultimate objective: obtaining money. The analysis of the

phenomenon highlights a recurring pattern that has evolved in recent years. Victims are initially approached through a social network where personal information is easily accessible, such as Instagram or Facebook, enabling the offender to build a relationship of trust. Following an apparently innocent initial conversation, the perpetrator then pressures the victim to move to another platform, such as Telegram.

This platform shift is crucial: unlike platforms belonging to the Meta group (Facebook, Instagram, WhatsApp), Telegram is not regulated in terms of preventing non-consensual sharing of intimate material and provides no meaningful response to requests for assistance. In practice, offenders exploit one platform to gather personal information, but commit the offence on another, where they know there will be no interventions. The use of multiple platforms in this type of crime is relatively recent and can be interpreted as an adaptive strategy by perpetrators seeking to circumvent monitoring and safety measures. Nevertheless, it should be noted that the use of a single platform remains the predominant method, as it is faster and more effective for offenders.

Based on available data, in **501 cases** a single platform was used, while in **290 cases** two platforms were involved, in **53 cases** three platforms, and in **242 cases** victims did not provide information regarding the number of platforms involved. The most frequently exploited platforms are those belonging to the Meta group (in more than half of cases), followed by Telegram and dating applications. Furthermore, during 2021–2022, other messaging applications such as Google Hangouts were also reported. An emerging trend documented in 2024 concerns the adoption of Discord, with **10 cases**, suggesting that video games and related chat platforms are becoming fertile ground for the spread of these crimes.

Another significant aspect concerns the financial gains obtained by perpetrators. It must be emphasized that available information is scarce and relies exclusively on victims' testimonies, many of whom are reluctant to disclose details of the payments made. To date, it is confirmed that **133 victims** paid money to perpetrators, amounting to approximately **€45,453**, transferred through various online payment methods including **PayPal, Western Union, MoneyGram, and Tip Tap**. Notably, these payment methods are often instantaneous, thereby facilitating the offenders' operations.

However, according to the information collected, perpetrators demanded a total of **€392,482** from victims. This discrepancy suggests that there may be a substantial number of additional victims who gave in to blackmail but chose not to disclose this information.

A recurring element in sextortion dynamics is the perpetrator's initial demand for large sums of money (often exceeding **€1,000**), followed by a negotiation in which the requested amount is gradually reduced. This tactic is intended to give the victim the illusion of exerting some control over the situation, while in reality it constitutes a process of extortion.

It is important to note that during the blackmail phase, offenders typically adopt an extremely aggressive strategy of threats. They repeatedly send screenshots containing collages of the victim's friends and family members, accompanied by threats to publicly disseminate these

images if payment is not made immediately. In many instances, perpetrators impose a countdown to heighten the sense of urgency.

Moreover, linguistic patterns have been observed in these threats: while the messages are often written in Italian, they appear to be the result of poor translations, suggesting that many offenders are not native speakers and may operate from outside the country. Victims are also bombarded with calls and messages from multiple phone numbers, creating an intense psychological pressure that frequently drives them to comply.

However, it is crucial to emphasize that paying does not represent a solution. Evidence shows that in cases where victims have submitted payments, the threats did not cease; instead, perpetrators quickly resumed their demands, often requesting even larger sums.

Translation of the original request in Italian:
A: *Stop, please.*
B: *Now, if you want this to be deleted, I want you to do what I ask.*
A: *No, please, I've already done enough.*
B: *I want you to send another payment.*

The Role of Platforms

The **principle of conditional immunity** for intermediaries, introduced by the 2000 e-Commerce Directive, establishes that online service providers **are not legally liable** for user-generated content, provided that they have no actual knowledge of unlawful activity, promptly remove illegal content once notified, and maintain a neutral role without exercising active control over such content.

The *Digital Services Act* (DSA)[7], which came into force in 2023, retained this principle but - unlike the e-Commerce Directive, which focused primarily on reactive immunity (after notification) - introduced certain **proactive obligations** for platforms with more than 45 million monthly users in the EU (*VLOPs – Very Large Online Platforms*). These platforms are now required to **play a central role in combating illegal content**, striking a balance between freedom of expression and user protection. Violations of the DSA may result in penalties of up to 6% of the platform's annual global turnover.

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

INTERPERSONAL DYNAMICS BETWEEN THE MALE VICTIM AND THE PERPETRATOR

The dynamics of sextortion are grounded in a process of escalating control. After initially obtaining consent - often within intimate or manipulative relational contexts—the perpetrator exploits the victim's trust to establish a recurring cycle of threats and demands.

The sample examined was analyzed with the purpose of exploring the relational dynamics between victim and perpetrator. The study adopted a **transactional analytic approach**, drawing on the model proposed by Eric Berne (1949). In particular, **Karpman's Drama Triangle**[8] (1968) was applied, which outlines dysfunctional interpersonal dynamics emerging in social conflicts. This model demonstrates how individuals unconsciously adopt **complementary roles** within interactions, thereby reinforcing **maladaptive** relational patterns.

The three fundamental roles identified by Karpman—the Victim, the Persecutor, and the Rescuer—interact with one another in a repetitive cycle. The **Victim** perceives themself as powerless, unable to cope with difficulties independently, and tends to seek external intervention to resolve their problems. This role is marked by passive attitudes and may involve feelings of injustice or resentment, often resulting in blaming the Persecutor or expecting rescue from the Rescuer. The **Persecutor**, by contrast, adopts a critical, aggressive, or authoritarian stance toward the Victim, exerting pressure or assigning blame. This role may manifest actively through threats, reproaches, or coercive behaviorsor passively, through demeaning or manipulative attitudes.
The **Rescuer,** finally, intervenes to help the Victim, often without being asked, thereby reinforcing the Victim's dependency. In some cases, the Rescuer may derive gratification from their role as helper but risks depriving the Victim of the opportunity to develop self-determination. When help is not accepted or does not produce the desired results, the Rescuer may shift into the role of Victim (if they feel misunderstood) or into that of Persecutor, if they begin to experience frustration or criticism.

The Application of Karpman's Drama Triangle to *Sextortion*

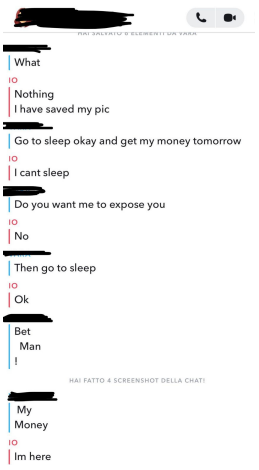
In the context of *sextortion*, the victim assumes the role of the individual directly subjected to threats or blackmail. They experience a profound sense of powerlessness and feel trapped in a situation where the perpetrator holds control. In many cases, the **victim** comes to internalize blame, perceiving themselves as responsible for what has happened and thereby developing a form of **self-persecution**. This psychological state is often marked by shame, guilt, and fear - emotions fueled both by the manipulative strategies of the perpetrator and by the victim's own

[8] For further reading: https://karpmandramatriangle.com

tendency to remain ensnared in recurrent negative emotional states.
The **perpetrator**, in turn, adopts behaviors aimed at exerting psychological pressure through threats, such as the dissemination of intimate images, with the goal of obtaining personal gains - whether financial, sexual, or otherwise. Psychologically, the perpetrator justifies their actions through a mindset of superiority or a need for control, displaying little to no empathy toward the victim's suffering.
In certain circumstances, the perpetrator may also take on the role of **Rescue**r. This occurs when, by further manipulating the victim, they offer a so-called "way out" - for example, by promising not to release the compromising material in exchange for compliance with their demands. Such behavior, although seemingly framed as assistance, in reality constitutes a sophisticated **strategy of control**, as it sustains the illusion of possible relief while never restoring the victim's genuine freedom.

Coping Strategies Employed by Victims

The application of the theoretical model developed by Lazarus and Folkman (1984) makes it possible to understand the psychological reactions enacted by victims of *sextortion*. According to these authors, **stress** results from a perceived relationship between the individual and the environment in which the person evaluates their resources as insufficient to cope with the situation. *Sextortion* constitutes a highly stressful and emotionally impactful event, and victims' responses may vary significantly. Some individuals adopt **problem**-focused coping, seeking to address the **threat** directly. This may take the form of reporting the blackmailer to the authorities, blocking channels of communication, or seeking technical and legal support. Other victims, by contrast, engage in **emotion**-focused coping strategies. Here, the emphasis is placed on managing the emotional burden, which may include anxiety, fear, guilt, and shame. Such strategies involve seeking social support, employing cognitive restructuring, or engaging in activities that help contain **emotional distress**. Finally, there are cases in which **avoidant** coping predominates, whereby the individual refuses to confront reality, withdraws, or—in more severe instances—may engage in self-harming behaviors. While this type of response can be understood as an initial defensive reaction, it risks exacerbating distress and prolonging the state of psychological vulnerability.



THE SHORT- AND LONG-TERM PSYCHOLOGICAL EFFECTS OF SEXTORTION

Sextortion has significant psychological consequences, which manifest both in the short and the long term. The psychological harm suffered by victims often takes the form of **complex trauma**, as the experience encompasses elements of relational abuse, violation of intimacy, and loss of control over one's bodily and identity-related self-image (Courtois & Ford, 2020).

Short-term effects

In the short term, victims may develop acute symptomatology, with clinical presentations dominated by severe anxiety, panic attacks, insomnia, irritability, and intrusive thoughts related to the traumatic event. The fear of sexually explicit material being disclosed functions as a constant stressor, producing a state of **hypervigilance** and **helplessness** (Chatzittofis et al., 2020). Dissociative reactions, psychosomatic manifestations, and mood disturbances are also frequent. In many cases, feelings of shame, guilt, and internalized blame emerge, which may hinder help-seeking and lead to social withdrawal (Feinstein et al., 2014). At this stage, psychological distress is often exacerbated by the perception of **judgmen**t from the social or family environment and by the difficulty of disclosing the event for fear of further **stigmatization**.

Long-Term Effects

One of the distinctive features of sextortion lies in its nature of **permanent exposure**. The fear that compromising material can never be definitively erased—or even the mere threat of its reemergence - acts as a constant trigger for trauma reactivation (Shapiro, 2018; Carletto et al., 2016). For this reason, in the long term, victims often develop **Post-Traumatic Stress Disorder** (PTSD), which, due to its recursive nature, has recently been described in the literature as a ***perpetual trauma loop*.** This concept captures the **traumatic experience** associated with *sextortion*: it is not the single event (the dissemination or the threat of dissemination) that causes the primary harm, but rather the chronic persistence of the threat, which keeps the individual in a state of ongoing hyperarousal (De Santisteban et al., 2020). This condition translates into a **cyclical reactivation** of trauma at the cognitive level (intrusive thoughts and hypervigilance), emotional level (anxiety, shame, helplessness), and somatic level (neurophysiological stress activation). The mere possibility that the material may resurface—even years later—is enough to sustain the post-traumatic stress response (Rapkoch, 2024).
For this reason, *sextortion* cannot be considered an **isolated event** but must be understood as a form of continuous traumatic exposure, in which the boundaries between past, present, and future remain constantly blurred. This perpetual state of vulnerability, in the absence of adequate psychological support, makes it extremely difficult for victims to regain a sense of control and safety in their lives.

POTENTIAL THERAPEUTIC INTERVENTIONS

Recognizing the psychological consequences of *sextortion* is essential for designing t**argeted therapeutic interventions**. An integrated approach is required, encompassing **emotional stabilization**, **cognitive restructuring**, **work on shame**, and the strengthening of **self-efficacy**.

Cognitive-Behavioral Therapy (CBT)

Cognitive-Behavioral Therapy (CBT) is widely used in the treatment of psychological trauma and anxiety resulting from forms of **sexual coercion**. It is grounded in the restructuring of **dysfunctional thoughts** and the reduction of emotional symptoms through techniques such as graduated exposure and cognitive reframing (Beck, 2011). In the context of *sextortion*, CBT seeks to deconstruct the **shame** and **guilt** that victims may experience (Feinstein et al., 2014), replacing negative thought patterns with more adaptive beliefs and thereby reducing self-blame. Furthermore, the approach incorporates *problem-solving* techniques, which are useful in enhancing the perceived sense of control over the situation.

Eye Movement Desensitization and Reprocessing (EMDR) and Treatment of Post-Traumatic Symptoms

Eye Movement Desensitization and Reprocessing (EMDR) has proven effective in the treatment of Post-Traumatic Stress Disorder (PTSD) and in cases of relational trauma (Shapiro, 2018). This therapeutic approach enables victims of *sextortion* to reprocess traumatic memories in a less distressing way, thereby reducing symptoms of emotional hyperarousal and flashbacks. Recent studies (Carletto et al., 2016) have shown that EMDR can significantly decrease levels of **anxiety** and **depression** in individuals who have experienced **psychological abuse** and **online threats**.

Mindfulness-Based Interventions (MBIs)

Mindfulness-Based Stress Reduction (MBSR) and *Mindfulness-Based Cognitive Therapy* (MBCT) represent valuable tools for helping victims manage **emotional stress** and improve **emotion regulation** (Kabat-Zinn, 1990). Both approaches focus on cultivating present-moment awareness and reducing negative rumination. This proves particularly effective for victims of *sextortion*, who, due to the constant threat of intimate content being disclosed, frequently develop **anticipatory anxiety** and **intrusive thoughts** (Segal, Williams & Teasdale, 2018).

Interventions Targeting Emotion Regulation and Self-Efficacy

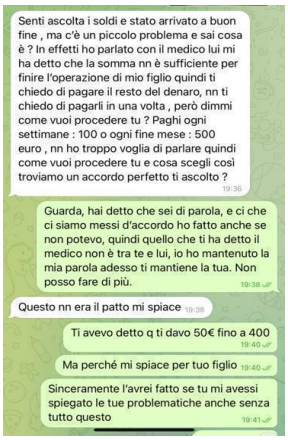
Many victims of *sextortion* experience intense levels of shame and fear of social judgment, which often result in **isolation** and a worsening of psychological distress (Levin et al., 2022). In such cases, therapeutic interventions based on *Acceptance and Commitment Therapy* (ACT) have proven effective in helping patients accept their emotions without attempting to avoid or amplify them, thereby fostering the development of **self-acceptance** (Hayes, Strosahl & Wilson, 2016).

The process of psychological recovery also requires the strengthening of personal **self-efficacy**. According to Bandura (1997), the sense of self-efficacy is a key factor in overcoming stressful events and reducing the risk of developing *PTSD*. To this end, resilience-focused therapeutic programs, such as *Resilience Training Therapy*, can provide valuable support in helping victims rebuild self-confidence and develop strategies aimed at preventing future vulnerabilities (Southwick & Charney, 2012).

Integrated Approach and Social Support

To effectively address the psychological consequences of *sextortion*, an **integrated therapeutic approach** is often required, combining multiple clinical models. Social support plays a crucial role as a **protective factor**: the involvement of family networks or support groups can facilitate recovery processes and counteract the risk of **social withdrawal** (Cohen & Wills, 1985). Moreover, **Systemic Therapy** can be valuable in analyzing and reorganizing relational dynamics, thereby helping to prevent further episodes of victimization (Minuchin, 1974).

CAN YOU HELP MY CHILD?



Translation of the original request in Italian:

A: *Listen, the money arrived safely, but there's a small problem, you know what it is?*

Actually, I spoke with the doctor and he told me that the amount isn't enough to finish my son's surgery, so I'm asking you to pay the rest of the money in one go. To make it easier for you, tell me how you want to proceed. Here are the options: €100 each month, €500 in one go. I don't want to keep arguing, so let me know how you prefer to handle this and we'll find a perfect solution.

B: *Look, you said you'd keep your word, and since we agreed I kept my side even though I couldn't. So since the doctor said it's up to you, I kept my promise, now you need to keep yours. I can't do more than this.*

A: *That wasn't the deal, I'm sorry.*

B; *I told you I'd give you €50 up to €400. But I'm sorry for your son. Honestly, I would have helped you if you had explained your situation, even without all this.*

One of the most insidious schemes in online financial extortion exploits alleged medical emergencies involving vulnerable family members, particularly very young children or gravely ill mothers. The extortionist's goal is to obtain money by constructing a fictitious, often detailed narrative capable of manipulating the victim's emotions. Although the sick relative does not exist, the use of illness as justification is deliberate, reflecting specific psychological, social, and criminological dynamics. During the monitoring period, Permesso Negato identified **45 cases** in which money was requested for the supposed medical care of children or other relatives.

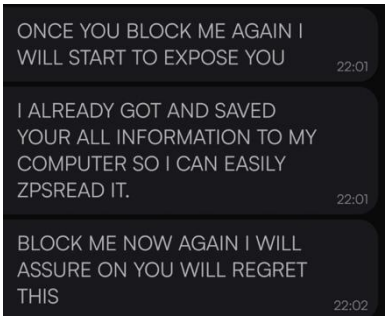
At the psychological level, this scheme activates what is known as a primary empathic trigger, an automatic mechanism prompting individuals to respond with compassion and solidarity when faced with suffering, particularly when embodied by socially "sacred" or "protected" categories such as children and mothers. The sense of urgency and moral responsibility is amplified by the narrative, which often employs dramatic details, photographs, names, medical appointment times, and countdowns linked to life-saving surgeries, thereby generating a false sense of immediacy and inevitability. In such conditions, the victim's behavior can be understood as a response to induced moral shock—an impulsive action driven by sudden emotional and social pressure.

Sociologically, the fabricated narrative exploits **deeply ingrained cultural stereotypes and archetypes**: the sick child symbolizes violated innocence, while the sick mother embodies sacrifice and silent suffering. These figures evoke an immediate sense of collective responsibility, enabling the extortionist to bypass rational defenses. What emerges is a distorted application of the principle of moral suasion, leveraging shared values to induce altruistic behavior even in the absence of fact-checking.

Within criminological frameworks, the phenomenon can be situated in multiple theoretical perspectives. **The Routine Activity Theory** (Cohen & Felson, 1979), which conceptualizes crime as the convergence of a motivated offender, a suitable target, and the absence of a capable guardian, is fully applicable in the digital context: online platforms provide an environment where offenders encounter exposed victims, often lacking the tools to recognize deception. In parallel, the **Neutralization Theory** (Sykes & Matza, 1957) explains how offenders justify their actions through cognitive mechanisms of neutralization, for example by convincing themselves that "they are not truly harming anyone" or that "people are wealthy enough to donate something."

The structure of these extortion attempts typically follows a predictable pattern: an initially neutral approach, followed by the construction of a fabricated medical narrative, the introduction of a financial request, and ultimately an escalation of **psychological pressure.** This pressure is frequently intensified through manipulative messages (e.g., *"you are the only person who can save my daughter"*) or guilt-inducing statements (e.g., *"if you do not help me, she will die and it will be your fault")*. In several documented cases, perpetrators inundated victims with distressing messages, images, and voice recordings, overwhelming them until their resistance collapsed.

This dynamic is consistent with what criminological literature defines as **affective leverage scams**, a subcategory of relational fraud in which the ultimate goal is financial gain, while the means employed is the construction of a fabricated empathic and relational bond. In such instances, offenders not only obtain monetary benefits but also exercise psychological control over victims, often leaving them in states of guilt or shame that inhibit formal reporting.



Moreover, the deployment of the figure of the sick mother or child may be interpreted as part of a broader strategy of manipulation. By projecting the vulnerability of "the other" (mother or child) onto the victim, the extortionist seeks to elicit identification with the depicted suffering. This mechanism is particularly effective when victims have themselves experienced situations of familial fragility, bereavement, or illness.

MINORS

Over the four-year period under review, **fewer than 100 minors** contacted *PermessoNegato* to seek assistance. This surprisingly low figure may be attributed to several factors: feelings of shame, attempts to handle the situation independently, fear of parental reactions, or, in some cases, the concern that disclosing their status as minors might preclude access to support without direct adult involvement. When compared to findings from other studies on the subject, it is reasonable to assume that these numbers do not fully capture the scope of the phenomenon among young people. On the contrary, the actual prevalence is likely to be significantly higher than the cases formally recorded.

In 2024, Save the Children published the report *"Le ragazze stanno bene? Indagine sulla violenza di genere onlife in adolescenza"* (*"Are the Girls Doing Well? Survey on Gender-Based Violence Onlife in Adolescence"*). Based on an IPSOS survey conducted in January 2024 on a sample of **800 adolescents** aged **14 to 18**, stratified by gender, age, and geographical area, several significant findings emerged. A majority of respondents (**54%**) believed that those who send intimate photos are aware of the risks involved, including the possibility that such images may be shared with third parties. **27%** of participants did not perceive anything wrong with repeatedly requesting intimate images from a partner, while **34%** considered the receipt of unsolicited intimate images as a sign of interest from the sender. Nearly half of adolescents (**49%**) disagreed with this interpretation; however, the belief that unsolicited intimate images may indicate interest remains widespread, particularly among boys in relationships (**48%**) compared to girls with the same experience (**29%**).

Adolescents also demonstrated partial awareness of the risks associated with sharing intimate images: **54%** at least partially agreed that those who send such content accept the risks, including the possibility of redistribution. This finding suggests that although awareness campaigns on the dangers of sharing intimate material online have been relatively effective, they are still insufficient to dissuade young people from engaging in these practices.

With regard to new forms of intimate and social relationships, building friendships through social media is a highly widespread phenomenon. **73%** of respondents reported having formed online friendships with individuals they had never met in person, with higher prevalence among those aged **16–18** (**76%**) and among boys (**76%**) compared to girls (**70%**). Similarly, **64%** of adolescents stated that they had used social media to connect with someone they were romantically or sexually interested in, with boys (**68%**) and those aged **16–18** (**65%**) again reporting higher levels of engagement.

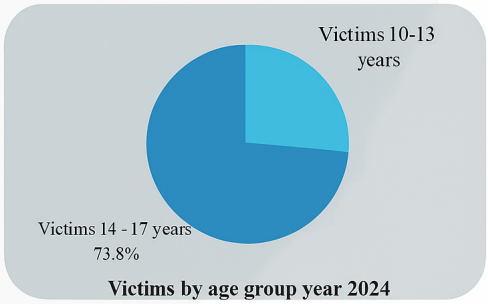
Furthermore, **28%** of respondents reported exchanging intimate photos and/or videos with partners (past or current), with the proportion higher among boys (**31%**) and among those who had been or were currently in a relationship (**40%**). Additionally, **33%** had received sexually

explicit photos or videos from friends or acquaintances, with higher incidence among those aged **16–18** (**37%**). Finally, approximately **10%** admitted to having shared or posted intimate images without the subject's consent, while **11%** reported that their own intimate images had been shared without their permission.

The **2024 annual report of the Italian Postal Police (Polizia Postale)** likewise highlights alarming figures, particularly concerning the age of victims.

Revenge Porn	TOTAL CASES TREATED	%	CASES treated victims 0-9 years	%	CASES treated victims 10-13 years	%	CASES trealed victims 14-17 years	
Year 2024	42	+45%	0	+0%	11	+83%	31	+35%
Year 2023	29		0		6		23	

The data analysis shows an overall increase ot 45% in revenge porn cases from 2023 to 2024. The 10-13 age group recorded the most significant increase (+83%). while the 14-17 age group remains the most affected with 31 cases in 2024.



Source: 2024 Annual Report of the Italian Postal and Communications Police

The data clearly indicate that **minors are also exposed to significant online risks**, which are frequently underestimated. Among these, grooming and sextortion constitute particularly concrete threats, especially in situations where there is limited awareness of what is being shared, with whom, and with what consequences. In today's increasingly pervasive digital environment, it is crucial to equip young people with the skills of digital citizenship, helping them to recognize that the boundary between online and offline has become blurred. In this context, Luciano Floridi's concept of *onlife* serves as a reminder that our digital presence is not separate from, but rather an integral component of, our identity and everyday relationships.

At the same time, **sexist language and gender stereotypes** exert a powerful influence on young people's development, shaping distorted perceptions of affective and sexual relationships. Such a cultural climate can heighten vulnerability or, conversely, encourage adolescents to engage in harmful and unreflective behaviors. For this reason, it is essential to promote educational strategies that integrate digital literacy with affective education and the

cultivation of mutual respect. Only by doing so can we effectively counter cultures of domination and foster safer, more inclusive digital spaces for all.

FUTURE RISKS: DEEP NUDE

In recent years, the spread of fake and manipulated images through **artificial intelligence** has reached increasingly concerning levels. Generative artificial intelligence, particularly deep learning models, has made it possible to create hyper-realistic content that, unfortunately, can be used in ethically problematic ways, such as in the case of deep nudes - altered images or videos showing people in non-consensual nudity.

A risk for the future, which is already emerging with increasing frequency, is the use of such content to lure and manipulate users, particularly through strategies of seduction and deception. Fake images, used in the context of romance scams or sextortion, represent **one of the most effective tools** for manipulating and entrapping vulnerable individuals. These images are often created ad hoc, using stolen photos of very sensual or provocatively posed women from the internet as a base, then paired with fabricated or altered stories. The primary aim of these images is to build an apparently authentic virtual relationship that, through the play of emotions and trust, leads the victim to take actions or disclose sensitive information. The grooming process, even with adults, is often long and complex, but its objective remains unchanged: **exploiting the psychological or emotional weakness of the targeted person to obtain money, personal data, or other benefits.**

An important aspect of this phenomenon is the creation of a **second victim**: the individual whose images - usually taken from public social media profiles - are used for these purposes without their knowledge. Such image theft entails a **violation of privacy** and, in some cases, **irreparable damage to the person's reputation**.

From a strictly legal perspective, as of now, there are no specific provisions in the Penal Code addressing the unlawful dissemination of artificially generated or manipulated content. However, depending on the context in which such images or videos are used, offenses such as aggravated defamation, identity theft, fraud, cyber fraud, extortion, threats, stalking, or the unlawful distribution of sexually explicit images or videos could be applicable. It should also be noted that, since the creation of false digital content generally involves the processing of personal data, the provisions of the **GDPR (EU Regulation 679/2016)** also apply.

TESTIMONIES

Davide - February 26, 2024

Good evening,
My name is Davide and I found you while searching online. I decided to reach out because I need help.
On February 5th, I was contacted on Instagram by a girl named Julie, who said she had seen me on a dating app and wanted to get to know me. Since I had occasionally used those apps, I didn't find it suspicious. For a couple of days, we chatted (always in English since she wasn't Italian) and she told me she was coming to Italy for Easter, to Rome, where I live.
After a few evenings, Julie asked if I wanted to "have some fun." I told her I'd prefer to video call first, since until then we had only exchanged messages. She agreed to a very short call on Instagram, spoke to me for a few seconds, and said she wasn't alone at home and felt embarrassed. Later, she asked me to continue on Telegram, and I accepted without thinking too much about it.
On Telegram, she explained she would stay muted because her parents were sleeping in the next room. During the video call, I saw her undress and act intimately, encouraging me to do the same. I did, showing myself only from the chest down. Suddenly, her video froze (I thought it was just a bad connection), but then a clip appeared on the screen showing me from just moments earlier, while I was masturbating. That's when I realized I had been recorded. Panicking, I showed my face on camera and asked what was going on. She immediately ended the call and started messaging me, saying that if I didn't want all my contacts to receive the video, I had to pay her €3,000. She also added that she had a sister with cancer. Instinctively, I deleted my Instagram and Telegram accounts so she couldn't access more of my photos or contacts, and so she would stop spamming me (she was sending nonstop messages). The next day, I went to the Carabinieri to file a report. From another IG profile, I checked and saw that her Instagram account was deleted, but her Telegram account is still active. As of today (February 26,2024), none of my friends have told me they received the video, but I'm still extremely anxious and unable to sleep at night.

Giorgia - October 7, 2023

I urgently need help. A person I don't know is threatening to spread an intimate video of me. This person has come into possession of a recording of an erotic video call I had about a year ago with my ex. It was a one-time episode: it was the only occasion in which I exposed myself in this way and, for this very reason, I can't understand how someone could have access to that material today.
When they first contacted me, I tried to deny that it was me in the video, but the situation quickly worsened. They began to blackmail me, threatening to send the video to my friends and acquaintances if I didn't send them more intimate material. They wrote to me clearly that, if I told anyone about these threats, they would publish the video. Since then, they keep contacting me, even though I don't reply, insisting that I send new intimate photos and repeating their threats. I've been trying to buy time with excuses and pretexts, but the truth is I no longer know how to handle the situation. I feel under pressure, scared, and desperate.
I never thought something like this could happen to me and now I feel completely alone. I really need help and I don't know who to turn to.

Giulio - December 24, 2021

I was contacted by a girl on Instagram who appeared to be just over twenty years old. We started chatting for a few days and then moved our conversations to Telegram.
One night, I sent her a selfie in which, despite wearing a helmet and glasses, I was still recognizable. Later, I shared two short intimate videos, believing they would self-destruct. Shortly afterward, that same person took screenshots and sent the material to three of my contacts on Instagram. Immediately after, the blackmail began: they demanded money in exchange for not spreading the images further.
Panicked, I gave in and sent €780, hoping it would all end there.
After the payment, they sent me screenshots as “proof” that they had deleted the messages sent to my friends. Fortunately, it was late at night, so I believe no one saw them. When they continued to demand more money, I pretended to be broke in an attempt to gain their sympathy. They told me to stay calm and find another €100, giving me time until the morning. The next morning, I sent a final message saying that the bank had blocked my card. I then changed my nickname on Telegram and blocked the contacts. Since that day, I have not received anything further. My Instagram and Facebook accounts are still active, but I no longer accept new requests or follow anyone.

WHAT CAN I DO IF I AM A VICTIM OF NON-CONSENSUAL SHARING OF INTIMATE MATERIAL?

As we have seen, digital relationships may expose individuals to the risk of intimate content being shared without consent. The nature of such material may vary: from images voluntarily taken during a sexual act but intended to remain private or shared only within a relationship, to images captured through hidden cameras, stolen from electronic devices following digital breaches—often deliberately engineered—or even recorded in the course of a sexual assault. The "virtual world" is characterized by virality, meaning that content can spread extremely quickly through spontaneous user sharing, often reaching millions in a short time. For this reason, it is crucial to **report non-consensual material to online platforms as soon as it is identified**. Search engines, social media platforms, dating apps, and pornographic websites increasingly acknowledge that the non-consensual sharing of intimate images is harmful and wrongful, and many provide specific reporting mechanisms. Where such procedures are not available, it is still possible to contact the site owner (the webmaster), usually via a "Contact Us" form or an email address listed at the bottom of the homepage or within the Privacy Policy. Before filing a report, it is essential to **collect evidence** of the published content (e.g., screenshots) before removal, in order to preserve the possibility of pursuing legal action later. Victims are also encouraged to document any threats received and retain information linked to the perpetrator's account. On a legal level, whether this conduct constitutes a criminal offence and how it is regulated depends on the **national legislation of each country**. For example, in Italy, the offence is criminalized under Article 612-*ter* of the Penal Code. Alongside institutional responses, it is also important to highlight the role of **support organizations**. In Italy for example, *Permesso Negato* provides legal, technical, and psychological support to victims worldwide, but other countries may have different structures, services, or reporting mechanisms available. Ultimately, victims are strongly encouraged to reach out to the competent **judicial or law enforcement authorities** in their own jurisdiction, not only to seek justice for the harm suffered, but also to contribute to exposing and prosecuting a crime that remains largely underreported.

FINAL RECOMMENDATIONS

These recommendations were developed primarily with reference to the Italian context; however, many of them are of broader relevance and may be applied at a supranational level, given the transnational nature of online sexual violence and the global reach of digital platforms.

In light of the growing spread of sextortion and, more generally, the non-consensual sharing of intimate material, it is essential to adopt systemic and coordinated measures that combine digital and cultural education with decisive legislative and institutional action. Addressing the non-consensual dissemination of intimate content requires a shift in perspective: these are not private incidents, but rather a social and cultural issue that concerns everyone. An effective response stems from the alignment of updated legislation, responsible technologies, and services that remain close to people's needs. This is not an unattainable goal; it is a necessary direction.
The following operational proposals are addressed to three key stakeholders in combating this phenomenon: **lawmakers, digital platforms, and public institutions.**

For Lawmakers: updating the legal framework to the Digital Reality

The current legal system often struggles to address promptly and precisely the dynamics associated with the non-consensual dissemination of intimate content, which may take different forms: sextortion, image-based abuse, emotional blackmail, accidental or intentional sharing. Updating the legal framework to the needs of today is the first step toward effectively addressing these emerging criminal phenomena.
It is therefore recommended to:

- **Introduce an autonomous criminal offence that incorporates the main elements of these behaviours** (extortion, violation of privacy, digital abuse), thereby ensuring consistent enforcement and stronger protection for victims;
- **Provide for specific aggravating circumstances**, such as when the victim is a minor, belongs to particularly exposed groups (e.g. LGBTQ+ individuals), or is in a condition of psychological vulnerability;
- **Extend the right to free legal aid**, without additional requirements, to victims of these offences, in line with what is already foreseen for other sexual crimes.

For Digital Platforms: Promoting Prevention, Responsiveness, and Collaboration

Digital platforms play a crucial role in both preventing and managing abusive content. Their responsibility goes beyond reacting once harm has occurred: they must implement technical and organizational measures that reduce the likelihood of such harm in the first place. User

trust depends significantly on the platforms' ability to safeguard integrity and security. These measures, by their very nature, are applicable across jurisdictions and should be pursued through international cooperation.
It is therefore recommended to:

- **Respond within 24 hours** to reports of non-consensual sharing of intimate material, ensuring reliable timelines and direct communication channels;
- **Integrate automated detection systems** based on hash-matching of images already identified by certified NGOs (such as StopNCII and TakeItDown), in order to prevent re-uploads of harmful content;
- **Establish operational partnerships** with non-profit organizations and sector professionals to strengthen proactive moderation, particularly in cases involving multiple reports or vulnerable victims.

For Public Institutions: Providing Concrete, Accessible and Integrated Responses

In Italy, the non-consensual sharing of intimate material is not yet recognized by the National Health Service as a traumatic event equivalent to sexual violence. This limits direct, immediate, and free access to specialized psychological support for victims, unless they fall within pre-existing frameworks for other forms of violence.
Although public and affiliated services exist—such as counselling centres, anti-violence centres, psychiatric or child neuropsychiatric services—they are not always trained or equipped to address the consequences of such experiences. Access may further be hindered by bureaucracy, long waiting times, and limited resources, as in the case of the psychologist bonus. Another limitation concerns the training of healthcare, educational, and school personnel, which is neither systematic nor mandatory. This often leads to indirect signs—such as social withdrawal, sudden emotional distress, self-harm, or a decline in school performance—going unnoticed. While some local educational projects exist in collaboration with the third sector, they remain sporadic and unevenly distributed across the country.
It is therefore recommended to:

- Recognize the non-consensual sharing of intimate material as a **potentially traumatic experience,** guaranteeing direct and free access to psychological support pathways, without bureaucratic obstacles;
- **Make digital and emotional education mandatory in schools:** prevention must start with education. Both minors and adults must become aware of online risks, including those linked to sextortion. To improve awareness and preparedness regarding online dangers, it is recommended to introduce compulsory digital, sexual, and affective education, focusing on how to identify risks, adopt safe online behaviours, and ensure that these are always grounded in the principle of consent;

- **Train school, healthcare, and social service staff to recognize indirect warning signs** (social withdrawal, sudden emotional distress, decline in academic performance), so that early intervention can be provided and victims directed to the appropriate services;
- **Raise awareness and provide training for law enforcement:** police forces must be adequately prepared to address online sexual crimes, which require a specific and sensitive approach. To ensure prompt and effective intervention, it is recommended to implement targeted training and awareness programmes for law enforcement officers, enabling them to handle reports competently and empathetically, support victims, and collect evidence appropriately;
- **Promote continuous public awareness campaigns** to inform citizens about risks and available support channels, normalize help-seeking, and counter stigma.

Cross-Cutting Recommendation: Centralized Data Collection

The lack of systematic data makes it difficult to analyse and effectively respond to sextortion and other forms of image-based abuse. To improve understanding and monitoring of these phenomena, it is recommended to establish a centralized database for the collection, analysis, and sharing of anonymized case data, in collaboration with law enforcement, non-profit organizations, and institutions. Such an initiative would have clear benefits beyond national borders and could provide a solid basis for comparative research and coordinated interventions at the European and international level.

CONCLUSION

The analysis of over 1,000 cases of sextortion reveals a complex and alarming picture: anyone can become a target. Victims include men and women of all ages and social backgrounds, demonstrating that there is no single profile or inherently "weaker" category. Men, often invisible in the public discourse surrounding these crimes, may find themselves in situations of acute vulnerability, further compounded by silence and the weight of social expectations tied to masculinity. Being exposed, humiliated, and blackmailed does not fit the cultural imaginary of the strong, invulnerable man. This gap between lived experience and cultural stereotypes makes seeking help even more difficult. At the same time, it cannot be ignored that the majority of victims of non-consensual intimate image dissemination continue to be women, who must often contend not only with the abuse itself but also with pervasive social judgment rooted in victim blaming and sexism. This double standard, affecting individuals differently yet across the spectrum, underscores the urgency of dismantling toxic gender norms and fostering a culture of respect and consent.

From a psychological perspective, digital sexual crimes are particularly insidious: they strike at the most intimate sphere of the individual, producing profound trauma that is often invisible yet long-lasting. The violence does not end with the initial abuse but lingers in memory, self-perception, and interpersonal relationships. Psychological support must therefore go beyond clinical assistance, offering tools to rebuild identity and reestablish meaningful connections with others, enabling victims to reclaim their own narrative.

From a legal and investigative standpoint, sextortion represents an increasingly complex challenge. Although the phenomenon is widespread, jurisprudential references remain scarce, partly due to victims' reluctance to come forward. Nevertheless, reporting is essential: it is the entry point for investigations and a prerequisite for dismantling the criminal structures, whether transnational networks or individual offenders—that exploit this crime to secure rapid gains with relatively low risks.

Against this backdrop, prevention emerges as the most effective strategy. What is required is a broad, conscious, and cross-cutting form of digital education. Such education must start in schools and adopt a multidisciplinary approach, capable of engaging young people on key issues such as consent, empathy, and mutual respect. It should equip them not only with the means to protect themselves but also with the awareness needed to avoid becoming (sometimes unknowingly) perpetrators. Overcoming a culture that normalizes coercion and violence, and that perpetuates rigid and harmful gender roles, is possible, but it demands a collective effort: to speak openly, to educate responsibly, and to listen attentively. Only through such shared commitment can we foster a community in which no victim is ever left alone.

GLOSSARY

The non-consensual sharing of intimate material, in its different forms such as sextortion, revenge porn, or the spread of pornographic deepfakes, represents a complex and rapidly evolving phenomenon. Understanding the differences between these behaviors is essential not only to properly identify crimes, but also to assign them the appropriate level of seriousness, provide adequate support to victims, and avoid perpetuating dynamics of blame or confusion.

Using precise and up-to-date language is essential when addressing these issues: naming an abuse correctly means acknowledging it, recognizing its impact, and responding more effectively. We are aware that these definitions continue to evolve alongside social, cultural, and technological changes. For this reason, we strive to keep our terminology as current as possible, ensuring that our work in awareness, prevention, and victim support is always respectful and well-grounded.

Non-Consensual Sharing of Intimate Material

This term refers to the distribution, publication, transfer, or sharing of sexually explicit images or videos intended to remain private, without the consent of the person depicted. In Italy, it is classified as a criminal offense under Article 612-ter of the Penal Code (*unlawful dissemination of sexually explicit images or videos*). In English, the phenomenon is commonly referred to as *Image-Based Sexual Abuse*. Since there is no harmonized legal framework across jurisdictions, however, the legal classification and regulation of this conduct may differ from country to country, and reference should therefore be made to the relevant national legislation.

Sextortion

Sextortion is a form of extortion in which the perpetrator threatens to disclose intimate material (whether authentic or artificially generated) unless the victim complies with specific demands, such as providing additional explicit content, engaging in sexual acts, or paying money. This phenomenon, which is generally understood as part of the broader category of non-consensual sharing of intimate material, may be perpetrated by individual offenders or by organized criminal groups. As with other forms of image-based abuse, the consequences for victims are often severe, including feelings of helplessness, fear, social isolation, and exposure to secondary victimization. A common example is blackmail that follows what initially appears to be an innocuous online interaction.

While sextortion is widely recognized as a form of abuse, the specific legal provisions that criminalize it, and the way in which it may be integrated into national penal frameworks, vary across jurisdictions. For this reason, reference must always be made to the applicable legislation of each country.

Revenge Porn

Revenge porn falls under the non-consensual sharing of intimate material and refers specifically to the distribution of sexual content (usually by a former partner or ex partner) with the aim of revenge. The main difference compared to other forms lies in the motive, often linked to the end of a relationship. It is important to note that the term *revenge porn* is often misused or overextended; for this reason, the broader and more accurate definition (non-consensual sharing of intimate material or image-basex sexual abuse) is preferable, as it covers all cases regardless of the reason.

Victim Blaming

Victim blaming refers to the tendency to assign responsibility for a crime (wholly or in part) to the victim, while downplaying or excusing the actions of the perpetrator. Although not a criminal act in itself, it is a harmful social mechanism that deepens victims' trauma, discourages them from reporting, and perpetuates damaging stereotypes. Common expressions such as "they were asking for it" or "they shouldn't have sent those photos" exemplify this phenomenon.

Cyberbullying

Cyberbullying refers to repeated acts of aggression, harassment, intimidation, or humiliation carried out over time through digital means such as social media, messaging apps, or email. Whether and how it constitutes a criminal offence depends on national jurisdictions, which define and regulate the phenomenon within their own legal frameworks. In Italy, for example, it is specifically addressed by Law No. 71/2017, which focuses on the protection of minors. Unlike traditional bullying, cyberbullying is marked by the speed and potentially limitless reach of harmful content. Its consequences can be severe, including anxiety, depression, school withdrawal, and, in the most serious cases, suicidal ideation. A common example is the creation of fake online profiles aimed at ridiculing or defaming an individual.

Deepfake / Deepfake Porn

Deepfake refers to images or videos digitally manipulated through artificial intelligence to insert a person's face into contexts or bodies in which they were never originally present. When applied to sexually explicit content, this practice is known as deepfake pornography and involves the non-consensual creation of fabricated intimate material featuring the victim. In recent years, the spread of easily accessible apps and tools capable of "undressing" a person from a single photo has significantly heightened the risk of abuse. Unlike the sharing of real intimate material, deepfake pornography produces entirely fabricated content, yet it generates equally devastating real-world consequences: reputational harm, psychological trauma, loss of control over one's image, and the additional difficulty of proving the inauthenticity of the material.

Secondary Victimization

Secondary victimization refers to the additional harm that a victim may suffer after the primary experience of a crime, not because of the offender's actions, but as a consequence of the responses or lack of response by authorities, institutions, the media, or the surrounding social environment. This form of victimization is rooted in the way the victim is treated once they seek help, report the crime, or attempt to reintegrate into their community. It can manifest through judgmental attitudes, explicit or implicit blame, minimization or denial of the harm endured, excessive bureaucratic obstacles, or insensitive and intrusive handling of investigations and legal proceedings.

The effects of secondary victimization can be profound. Instead of finding protection and support, victims may feel further isolated, stigmatized, and silenced. This dynamic not only exacerbates the psychological and emotional trauma already caused by the crime, but also discourages others from reporting similar experiences, reinforcing a cycle of underreporting and invisibility. In this sense, secondary victimization does not simply add to the harm, it represents a failure of the very systems that should ensure recognition, protection, and justice.

Online Grooming

Online grooming refers to the process of contacting, engaging, and manipulating a person through the internet with the aim of gaining their trust and exploiting them, whether sexually, by extorting intimate material, or for other forms of personal advantage. When the victim is a minor, grooming assumes particular legal seriousness and is explicitly criminalized in many jurisdictions; in Italy, for instance, it is regulated under Article 609-undecies of the Penal Code. In the case of adults, grooming is not classified as an autonomous offence, but the conduct may constitute part of other crimes, such as sextortion, sexual exploitation, or romance scams.

Examples include a minor persuaded by an adult (often hiding behind a fake online identity) to send intimate images, or an adult deceived into sharing private content with someone who later reveals themselves to be a fraudster. In both scenarios, the manipulative dynamics of trust-building, deception, and eventual exploitation are central, highlighting the dangerous potential of grooming as a digital strategy of abuse.

Digital Trauma

Digital trauma is a form of psychological trauma that arises from direct or indirect exposure to traumatic experiences mediated by digital technologies. It is characterized by an intense, persistent, and dysfunctional emotional response to disturbing digital content or online interactions, and may include symptoms typical of post-traumatic stress disorder (PTSD) as well as those associated with other related psychopathological conditions.

BIBLIOGRAPHY AND ONLINE RESOURCES

- **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