Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Research Article

ONLINE SEXUAL VIOLENCE AGAINST WOMEN IN SPAIN: AN ANALYSIS OF THE PSYCHOSOCIAL IMPLICATIONS FROM A GENDER PERSPECTIVE

English translation with AI assistance (DeepL)

María Calvo Lorenzo
University of Granada
mariacalvo1@correo.ugr.es
ORCID: 0009-0001-1078-9557

Received 28/04/2026
Accepted 01/06/ 2026
Published 30/06/ 2026

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.9051

Recommended citation: Calvo, M. (2026). Online sexual violence against women in Spain: An analysis of the psychosocial implications from a gender perspective. *Logos Guardia Civil Journal*, 4(2), pp. 59–84 https://doi.org/10.64217/logosguardiacivil.v4i2.9051

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
Online ISSN: 2952-394X

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.9051

ONLINE SEXUAL VIOLENCE AGAINST WOMEN IN SPAIN: AN ANALYSIS OF THE PSYCHOSOCIAL IMPLICATIONS FROM A GENDER PERSPECTIVE

Abstract: In order to analyse sexual cyberviolence against women in Spain from a psychosocial and gender perspective, a narrative review of the literature was conducted, identifying 438 documents, of which 48 met the inclusion criteria. Sexual cyberviolence is a growing phenomenon that disproportionately affects women, highlighting how digital technologies amplify structural gender inequalities; key aspects include digital sexual harassment, sextortion, image-based sexual abuse or 'revenge porn', as well as emerging phenomena such as the whitewashing of the sex trade on content platforms. Documented mental health consequences include suicidal ideation and attempts, anxiety, depression, trauma, post-traumatic stress, sleep problems, low self-esteem and self-objectification. Artificial intelligence has emerged as a new tool for perpetrating such acts, facilitating the creation of deepfakes and non-consensual nude imagery. In the area of prevention, cybersecurity offers technological tools, although existing applications have significant limitations and reporting rates do not exceed 7.3 per cent. It is concluded that sexual cyberviolence is an amplified expression of gender inequalities, requiring comprehensive interventions that combine gender-sensitive education, platform regulation, professional training and the ethical design of technologies.

Resumen: Con el fin de analizar las ciberviolencias sexuales contra la población femenina en España desde una perspectiva psicosocial y de género, se realizó una revisión narrativa de la literatura identificando 438 documentos de los cuales 48 cumplieron los criterios de inclusión. Las ciberviolencias sexuales constituyen un fenómeno creciente que afecta desproporcionadamente a las mujeres, evidenciando cómo las tecnologías digitales amplifican las desigualdades estructurales de género; entre sus dimensiones destacan el acoso sexual digital, la sextorsión, el abuso sexual basado en imágenes o «porno de venganza», así como fenómenos emergentes como el blanqueamiento del negocio sexual en plataformas de contenido. Las consecuencias en salud mental documentadas incluyen ideación e intentos suicidas, ansiedad, depresión, trauma, estrés postraumático, problemas de sueño, baja autoestima y autoobjetificación. La inteligencia artificial ha emergido como una nueva herramienta de perpetración, facilitando la creación de deepfakes y aplicaciones de desnudo no consensuado. En el ámbito preventivo, la ciberseguridad ofrece herramientas tecnológicas, aunque las aplicaciones existentes presentan limitaciones significativas y las tasas de denuncia no superan el 7,3%. Se concluye que las ciberviolencias sexuales son una expresión amplificada de desigualdades de género, requiriendo intervenciones integrales que combinen educación con perspectiva de género, regulación de plataformas, formación profesional y diseño ético de tecnologías.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.9051

Keywords: cybersecurity, sextortion, digital sexual harassment, digital platforms, gender equality

Palabras clave: ciberseguridad, sextorsión, acoso sexual digital, plataformas digitales, igualdad de género

ABBREVIATIONS

AI: Artificial Intelligence

IBSA: Image-based sexual abuse

NCI: Non-consensual intimate images

NCIID: Non-consensual dissemination of intimate images

OCSEA: Online child sexual exploitation and abuse

TFSV: Technology-facilitated sexual violence

ECHR: European Court of Human Rights

AI Act: European Artificial Intelligence Regulation

DSA: Digital Services Act

1. INTRODUCTION

The digitalisation of human relationships has profoundly transformed spaces for social interaction, creating new contexts in which traditional forms of violence are reproduced, amplified and take on previously unknown forms. Among these, sexual cyberviolence is a growing phenomenon that disproportionately affects women, highlighting how digital technologies are not neutral spaces, but rather a territory where structural gender inequalities are deepened and take on new forms (Mármol et al., 2025). This article analyses sexual cyberviolence against women in Spain from a psychosocial and gender perspective, considering both its scale and its implications for the mental health and well-being of victims.

Technology-facilitated sexual violence (TFSV) is defined as any unwanted sexual behaviour involving the use of digital technologies, encompassing both virtual and in-person sexual harm facilitated by digital means (Champion et al., 2022; Henry and Powell, 2018). This umbrella term encompasses online sexual harassment, harassment based on gender or sexuality, cyberbullying, image-based sexual exploitation, and the use of communication services to coerce a victim into performing unwanted sexual acts (Henry and Powell, 2018). In the Spanish context, the classification used by the Ministry of the Interior includes offences such as sexual abuse, sexual harassment, corruption of minors, grooming, exhibitionism, the dissemination of images of child sexual abuse and sexual provocation, all of which are perpetrated via digital media (Mármol et al., 2025).

Research suggests that TFSV should be understood within conceptual frameworks that draw on gender and actor-network theories to comprehend the causes and consequences of women's experiences of abuse and violence facilitated by digital technologies (Henry et al., 2020). This perspective is essential, as such forms of violence are not isolated incidents, but rather expressions of broader social and structural inequalities that determine who is at risk and how the violence manifests itself (Mármol et al., 2025). Recent studies highlight the role of moral disengagement and sexist ideology—both hostile and benevolent—in perpetuating these behaviours, showing that men, particularly those with more deeply ingrained sexist attitudes and those in positions of power, are more likely to justify sexual cyberviolence (Martínez-Bacaicoa, 2024; Durán and Rodríguez, 2019). Furthermore, it has been documented that men are the main perpetrators, although women and non-binary people may also perpetrate this type of violence, often motivated by self-defence, the management of unpleasant emotions or a lack of reflection (Martínez-Bacaicoa et al., 2023).

The scientific literature reveals significant terminological and conceptual challenges in this field (Henry et al., 2020). The conceptual boundaries of TFSV are broad and dynamic, continually adapting to new emerging technologies and their uses, such as *deepfakes*, generative artificial intelligence systems and encrypted communications, which further complicate detection and the attribution of responsibility (Mármol et al., 2025).

In Spain, the study of online sexual violence has gained increasing prominence, driven by the availability of new, validated measurement tools, such as the Online Sexual Victimisation Scale and the Digital Dating Violence Questionnaire (Martínez-Bacaicoa, 2024), as well as by the development of research agendas that address the relationship

between digital technologies and sexual violence from a comprehensive perspective (García Mingo et al., 2025).

Despite these advances, significant challenges remain: the statistical invisibility of certain forms of violence, the difficulty in capturing the continuity between the *offline* and *online* worlds, the scant attention paid to the experiences of adult women beyond adolescence, and the lack of longitudinal research enabling an understanding of how victimisation evolves according to sex and age.

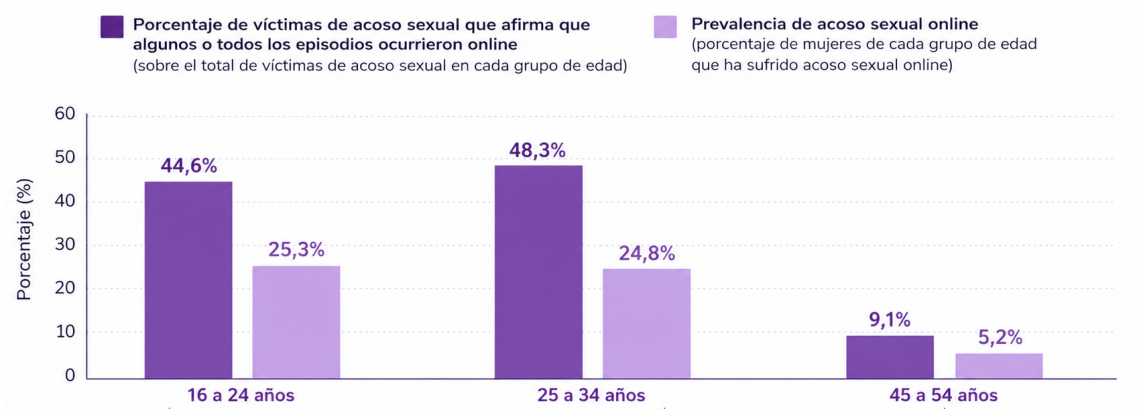
The scale of the phenomenon in Spain is alarming. According to data from the 2019 Macro-survey on Violence against Women, approximately 9.15 per cent of Spanish women have experienced cyber sexual harassment at some point in their lives, with significant impacts on mental health, including high rates of suicidal ideation, depression and anxiety (Benítez-Hidalgo et al., 2024).

The most recent data from the 2024 Macro-survey on Violence against Women provide a more detailed picture of this reality. When considering the location of the incident, 20.7% of women who have experienced sexual harassment at some point state that it occurred *online* (for example, on websites, social media platforms such as Instagram or TikTok, messaging apps such as WhatsApp, dating apps such as Tinder, video conferences, etc.). This means that 7.5% of all women aged 16 or over living in Spain – around 1.6 million – have experienced sexual harassment specifically via digital media (Ministry of Equality, 2025).

However, when asked directly whether any incident of sexual harassment took place via digital technologies – regardless of whether it had also occurred in other settings – the figure rises: 24.8 per cent of victims of sexual harassment, almost one in four, report that all or some of the incidents took place *online*. This represents 9% of Spanish women aged 16 and over, that is, approximately 1.9 million women (Ministry of Equality, 2025).

The problem is particularly serious amongst young women (see *Figure 1*). In the 16–24 age group, 44.6 per cent of victims of sexual harassment state that some or all of the incidents occurred *online*; in the 25–34 age group, the figure is 48.3 per cent. In terms of prevalence relative to the total population in each age group, 25.3 per cent of women aged 16 to 24 and 24.8 per cent of those aged 25 to 34 have experienced *online* sexual harassment. From the age of 45 onwards, these figures drop sharply, to just 5.2% among women aged 45 to 54 (Ministry of Equality, 2025).

Figure 1
Online sexual harassment of women by age group



Note: Prevalence of online sexual harassment among women by age, highlighting that it is much more common amongst younger women (aged 16–34). Taken from the Ministry of Equality. (2025). 2024 Macro-survey on Violence against Women. Government Delegation for Combating Gender-Based Violence.

Another important finding is prior *online* interaction with the perpetrator. Among women who have experienced sexual harassment and state that some (but not all) incidents occurred *online*, 59.4 per cent say that these incidents took place after they had previously met or interacted with the perpetrator via the internet. Even amongst those who said that no incident had taken place *online*, 1.7% admit that the harassment occurred following a previous digital interaction (Ministry of Equality, 2025).

Although these figures are significant, they may underestimate the true scale of the problem, as more recent research indicates that 82.6% of women have experienced at least one form of *online* gender-based violence in the last twelve months, with digital sexual harassment being the most common form (66.7%), followed by violence based on physical appearance (60.7%) (Martínez-Bacaicoa et al., 2024). Along the same lines, a cross-sectional study involving 1,177 Spanish women aged between 18 and 59 found that 68.2% had suffered gender-based violence via social media, whilst 62.7% reported having experienced *online* sexual violence (López-Barranco et al., 2025).

The most recent international evidence puts the global prevalence of this violence at 30.6 per cent of adult women (Benítez-Hidalgo et al., 2025), although these figures vary significantly depending on the definitions and measurement tools used. The European Union Agency for Fundamental Rights' survey on violence against women reveals that sexual harassment remains a widespread experience: between 83 and 102 million women (45%–55%) across the 28 Member States have experienced at least one form of sexual harassment since the age of 15 (Latcheva, 2017). This type of violence disproportionately affects young women and is most commonly perceived and experienced by women with a university degree and those in the highest occupational groups (Latcheva, 2017).

The temporal dimension of this phenomenon is equally significant. During the COVID-19 lockdown, harassment via electronic channels increased significantly (32.6% during the lockdown compared with 16.5% before and 17.8% afterwards) (Casanovas et al., 2022), highlighting how the increased use of digital environments can exacerbate the

risks of victimisation. Furthermore, recent research indicates that daily use of social media and the consumption of pornography are associated with higher rates of victimisation (López-Barranco et al., 2025).

This article aims to address these limitations by analysing the psychosocial implications of sexual cyberviolence against women in Spain from a gender perspective. To this end, existing definitions and typologies will be critically examined; prevalence rates and risk factors will be analysed; and the consequences for victims' mental health and psychosocial well-being will be explored, alongside an analysis of the role played by artificial intelligence and cybersecurity in the perpetration of such violence. Adopting a gender-based approach is essential for uncovering the structural mechanisms that underpin this violence, as well as for guiding the design of prevention, detection and intervention strategies that are effective, contextually relevant and sensitive to the gender inequalities that permeate the digital space.

2. METHODOLOGY

2.1. STUDY DESIGN

The methodology employed in this study is based on a narrative synthesis of recent scientific literature, adopting a gender perspective that guides both the selection and analysis of the evidence. This approach enables us to describe and synthesise the multifactorial impact of sexual cyberviolence, as it allows us to integrate findings from studies with diverse designs (quantitative, qualitative and mixed) and contexts, facilitating a holistic understanding of the phenomenon from a psychosocial perspective.

2.2. SEARCH STRATEGY

To gather the evidence, a systematic search was conducted in academic databases and specialised repositories, including PubMed, Scopus, ProQuest, Web of Science and PsycInfo. The search was carried out between March 2025 and February 2026, covering publications mainly from 2015 to 2026, with the aim of capturing the most recent developments in the phenomenon, although earlier foundational works were considered where they were essential for conceptual definition.

The search strategy combined terms in Spanish and English using Boolean operators. The search terms used were: ciberviolencia sexual, violencia de género en línea, technology-facilitated sexual violence, online sexual harassment, image-based sexual abuse, sextortion, grooming, ciberacoso sexual, digital sexual violence, together with terms referring to the population (mujeres, women, femenino, adolescentes) and the geographical context (España, Spain). The operators AND and OR were used to combine the concepts, and filters were applied for language (Spanish and English) and document type.

Search results: 438 articles were identified. After removing duplicates, 360 titles and abstracts were screened, with 204 excluded for failing to meet the inclusion criteria. 156 full-text articles were assessed, of which 48 met all the inclusion criteria.

2.3. INCLUSION AND EXCLUSION CRITERIA

The following criteria were established for selecting sources:

Inclusion criteria:

a. Empirical articles (quantitative, qualitative or mixed methods), systematic reviews, meta-analyses and institutional reports published by official bodies.
b. Publications in indexed scientific journals or from recognised institutional sources.
c. Studies whose research focus addressed some form of sexual cyberviolence or technology-facilitated sexual violence (TFSV).
d. Samples including a female population (girls, adolescents, adults or both).
e. Studies carried out in Spain or, failing that, international research providing relevant evidence on prevalence, risk factors or psychosocial consequences.
f. Publications in Spanish or English.
g. Publication period between 2015 and 2026 (except for earlier foundational references essential for conceptual definition).

Exclusion criteria:

a. Studies focusing exclusively on male populations without a breakdown by sex.
b. Research addressing only *offline* violence without reference to digital media.
c. Opinion pieces, editorials, letters to the editor or non-peer-reviewed publications (except institutional reports).
d. Documents whose full text is not available in Spanish or English.
e. Studies duplicated across different databases.

2.4. DATA EXTRACTION AND SYNTHESIS

From each selected source, information was extracted on: authorship and year, methodological design, sample characteristics, operational definitions of sexual cyberviolence, main findings and limitations. The synthesis was carried out using a narrative approach, grouping the findings into thematic categories: (a) prevalence and magnitude of the phenomenon; (b) risk factors; (c) consequences for mental health and psychosocial well-being; (d) definitions and conceptual frameworks; (e) gender perspective and structural inequalities; (f) perpetration and prevention strategies.

2.5. METHODOLOGICAL QUALITY AND VALIDITY

The validity of the conclusions is underpinned by the selection of studies of high methodological quality, assessed using explicit criteria: (a) origin from peer-reviewed publications or recognised official bodies; (b) alignment of the objectives with the research question; (c) appropriateness of the methodological design; (d) clarity in the definition of variables; (e) representativeness of the samples in quantitative studies; (f) analytical rigour in qualitative studies; and (g) consistency of the results with the international scientific consensus.

2.6. REPLICABILITY

This approach is replicable by applying the same search and selection criteria as described, enabling other researchers to verify or extend the analysis by following the detailed procedure.

3. RESULTS AND DISCUSSION

3.1. DIMENSIONS OF CYBERVIOLENCE AND TYPOLOGY

Sexual cyberviolence constitutes a heterogeneous network of behaviours which, underpinned by digital technologies, violate women's sexual integrity and freedom from a gender-based perspective (Henry and Powell, 2018; Champion et al., 2022). Analysing it requires moving beyond a simple listing of forms of victimisation to understand how structural inequalities are transferred and amplified in the digital space. To avoid terminological overlap, it is necessary to distinguish between three concepts that are often used synonymously: technology-facilitated sexual violence (TFSV) is the umbrella term encompassing all unwanted sexual behaviour mediated by digital technologies (Henry and Powell, 2018); digital sexual violence refers specifically to behaviours that occur entirely in digital environments (Martínez-Bacaicoa, 2024); and online gender-based violence emphasises the structural component of inequality between men and women as an underlying cause (Mármol et al., 2025).

An international systematic review and meta-analysis identified three main dimensions of TFSV against women (Benítez-Hidalgo et al., 2025). The first and most common is digital sexual harassment, with an estimated global prevalence of 28.54 per cent. This includes inappropriate sexual comments, unwanted advances, unsolicited sexual attention and sexist remarks on online platforms. In Spain, 66.7 per cent of women have experienced this in the last twelve months (Martínez-Bacaicoa et al., 2024), and the unsolicited sending of explicit images ('dick pics') affects 48.1 per cent of women aged 18 to 30 (Durán and Rodríguez-Domínguez, 2023). The second dimension is sextortion (16.93% globally), defined as the threat to share sexual images in order to coerce the victim into paying, sending further material or performing unwanted acts. It occurs in various contexts: intimate partner violence, cyberbullying, online dating, human trafficking and organised crime (Ray and Henry, 2025). The third is image-based sexual abuse (IBSA) or 'revenge porn' (6.48% globally), which includes the non-consensual taking, distribution or threat of distribution of intimate images. Perpetrators are usually current or former partners, and in 29% of incidents, victims report a devastating impact on their lives (Colburn et al., 2025).

A distinguishing feature of these forms of violence is the digital footprint: the permanence, reproducibility and potential for the material to go viral in digital environments. Unlike offline violence, where the harm may be confined to a specific time and place, digital violence creates a continuity of victimisation over time. Once an intimate image is shared without consent, the loss of control over its dissemination is practically irreversible, creating a state of permanent hypervigilance (Lorca, 2024). Furthermore, digital technologies act as facilitators for the recruitment of victims into trafficking networks for the purposes of sexual exploitation, often through promises of legitimate employment (Mayuri-Bocanegra and Aliaga-Pacora, 2023).

An emerging phenomenon that has sparked debate is the 'whitewashing' of the sex trade through platforms such as OnlyFans or Fansly. Various organisations have warned against what they term 'digital pimping', which presents the creation of intimate content as a form of empowerment when, in reality, it reproduces dynamics of objectification and structural inequality (Fuentes and Berger, 2025; Medina-Bravo, 2021). From a critical perspective, this article highlights that the normalisation of offering intimate content as a source of income amongst young people reveals a worrying lack of awareness of the underlying gender-based violence and inequality, whilst acknowledging the complexity of the phenomenon and the diversity of experiences.

From a criminological perspective, applying the theory of routine online activities helps to understand victimisation: it involves a suitable target (young women with an active digital presence), a perpetrator's motivation (facilitated by digital disinhibition and anonymity) and the absence of a competent guardian (insufficient platform moderation, low reporting rates). Digital disinhibition (Suler) explains that perpetrators engage in behaviour they would not display offline due to anonymity and asynchrony. Furthermore, perpetrators of deepfakes use neutralisation techniques (denial of harm, denial of the victim, condemnation of the accusers) to minimise their responsibility (Flynn et al., 2025). These dynamics are part of a culture of digital rape that normalises non-consensual sexualisation, and of algorithmic governance where platforms' recommendation systems and 'dark patterns' favour the viral spread of abusive content at the expense of users' privacy (Fagan, 2024).

At the legal level, European legislation has significant shortcomings. The AI Act does not explicitly regulate sexualised deepfakes as an unacceptable risk category, and the Digital Services Act faces challenges regarding detection and scale. The case law of the European Court of Human Rights (ECHR) (Buturugă v. Romania, 2020, and Volodina v. Russia, 2019 and 2021) has established that states have positive obligations to protect women from digital violence, laying the groundwork for future legal reforms.

Taken together, these findings have significant implications for the design of preventive health policies. It is suggested that mental health services routinely ask whether online interactions are causing harm (Iroegbu et al., 2024). During the COVID-19 pandemic, sexual violence decreased in public spaces but increased in digital spaces, and the silence surrounding violent situations deepened (Castellanos-Torres et al., 2023), underscoring the need to develop action protocols and improve the accessibility of resources in crisis contexts.

3.2. CONSEQUENCES AND RISK FACTORS FOR VICTIMS

The consequences of sexual cyberviolence on mental health are serious and well documented. In Spain, women who were victims of this form of violence reported significantly higher rates of suicidal ideation (20% compared with 9.79% among non-victims) and suicide attempts (7.20% compared with 1.74%), according to Benítez-Hidalgo et al. (2024). Furthermore, digital sexual harassment is an independent predictor of anxiety, depression, trauma and body image dissatisfaction (Iroegbu et al., 2024).

This pattern is not unique to Spain. International research confirms that victims of technology-facilitated sexual violence experience anxiety, stress, depression, a loss of control, mistrust, multiple victimisation, academic or occupational dysfunction,

problematic alcohol use, shame and changes in their online behaviour (Champion et al., 2022). In fact, those who suffer image abuse online have higher rates of depression, anxiety and occupational or academic dysfunction than victims of other types of technology-facilitated sexual violence (Champion et al., 2022).

Delving deeper into the mechanisms underlying these effects, a recent study has shown that women who are more likely to accept myths about online sexual violence[1] and who have experienced greater victimisation report higher levels of anxiety, depression and body shame, as well as lower self-esteem and body appreciation. This effect is mediated by self-objectification, suggesting that such myths exacerbate the emotional impacts on those who have experienced this type of violence more frequently (Vizcaíno-Cuenca et al., 2025). Furthermore, victims suffer from post-traumatic stress symptoms and sleep problems, which mediate the relationship between cyber-sexual victimisation and psychological distress (Morgan et al., 2025).

Beyond the consequences, it is necessary to understand the scale of the problem and the profiles of those most at risk. According to the 2019 Macro Survey, risk factors associated with cyber sexual violence in Spain include being under 25 years of age, having a higher education qualification, not being in a relationship, having no religious beliefs, and having a certified disability (Benítez-Hidalgo et al., 2024). Women who have experienced other forms of gender-based violence are also at greater risk of suffering sexual cyberviolence (Benítez-Hidalgo et al., 2024). This differential vulnerability is particularly pronounced during adolescence: women under the age of 18 have victimisation rates for grooming of 2.55 per 100,000 inhabitants, compared with 0.95 for men of the same age; whilst in young adulthood (18–25 years), women experience higher rates of sexual harassment and sexual abuse. Projections for 2035 indicate that these gender gaps will not only persist but will widen, particularly among girls under 18 and in the 26–40 age group (Mármol et al., 2025).

From a criminological perspective, the theory of routine online activities helps to explain why victimisation occurs: it involves a suitable target (young women with an active digital presence), the perpetrator's motivation (facilitated by digital disinhibition and anonymity) and the absence of a capable guardian (insufficient platform moderation and low reporting rates). Digital disinhibition explains why perpetrators engage in behaviour they would not display in the offline world, owing to anonymity, invisibility and asynchrony. Furthermore, perpetrators of deepfakes use neutralisation techniques, such as denial of harm ('it's just a photo'), denial of the victim ('she asked for it') or condemnation of the critics ('everyone does it'), to minimise their responsibility (Flynn et al., 2025).

The importance of social and temporal context became particularly evident during the pandemic. A 2022 study involving 2,515 young Spaniards aged between 18 and 35 found that women were almost twice as likely as men to experience sexual harassment (49 per cent compared with 22.2 per cent) (Casanovas et al., 2022). During lockdown, harassment via electronic channels increased (32.6%, compared with 16.5% and 17.8% before and after the period), whilst it decreased in public spaces (22.9%, compared with

[1] These include the minimisation or denial of violence, victim-blaming, blaming digital platforms, and exonerating the perpetrator (Vizcaíno-Cuenca et al., 2025)

63.4% and 54.4% before and after). These figures show that, during lockdown, sexual harassment shifted from public spaces to social media (Casanovas et al., 2022).

Finally, in the face of this suffering, survivors employ various coping strategies and seek help. The most common are confiding in trusted individuals, taking legal action and reporting the content. At the other end of the spectrum, avoidance strategies include relocating, isolating oneself or trying to act as if nothing had happened. However, victims face significant barriers to seeking help: stigma, a lack of awareness of available resources and previous negative experiences with the authorities make it difficult for many women to access the support they need (Karasavva, 2025).

3.3. ARTIFICIAL INTELLIGENCE IN PERPETRATION

Artificial intelligence (AI) has emerged as a tool that significantly enhances the capabilities of perpetrators of sexual cyberviolence, representing a profound escalation in image-based sexual abuse (Williams, 2025). Since 2017, the proliferation of open-source technologies has made the creation and dissemination of *deepfakes* easier than ever before. This has been accompanied by a parallel rise in cases of online sexual abuse, particularly against women (Flynn et al., 2025). The vast majority of *deepfakes* circulating online are pornographic in nature, and the people featured in them have rarely given their consent. Anyone with an online presence can become a victim (Karasavva and Noorbhai, 2021), with women being the most vulnerable group. A 2025 study analysing 29 apps dedicated to this practice concluded that these platforms not only facilitate but actively encourage the creation of non-consensual intimate images (NCII). In doing so, they normalise the objectification of women and contribute to a culture where their privacy and autonomy are systematically undermined (Williams, 2025).

Even more worrying is the behaviour of the perpetrators themselves. A qualitative study from 2025, conducted with ten perpetrators and fifteen victims of sexualised *deepfake* abuse, revealed some very serious patterns: the ease of use of these tools, the normalisation of sexualisation without consent, and the constant downplaying of the harm caused to victims. All of this, according to the authors, can negatively impact any prevention and response efforts (Flynn et al., 2025). Perpetrators justify and downplay their actions, and whilst there are similarities with other forms of technology-facilitated sexual violence, the key difference lies in the accessibility and ease with which a *deepfake* can be created (Flynn et al., 2025).

Another aspect of this problem is sextortion, which occurs in a wide variety of contexts: intimate partner violence, cyberbullying, dating apps, sex trafficking and organised crime (Ray and Henry, 2025). Whilst traditional sextortion used to rely on the victim voluntarily sharing their own intimate images, AI has removed that barrier (Lazard et al., 2025). Generative AI tools can create hyper-realistic fake nude images from any photo on social media, such as a profile picture. This enables perpetrators to turn anyone with an online presence – particularly women, girls and adolescents – into a potential victim, blackmailing them with fake images that appear real (Lazard et al., 2025). AI acts as a catalyst: it facilitates the creation of fake images, the automation of blackmail and the personalisation of threats on a large scale. Reporting and seeking help remain very low due to shame, fear and negative perceptions of the police and digital platforms (Lazard et al., 2025; Ray and Henry, 2025).

In this context, online child sexual exploitation and abuse (OCSEA) is regarded as an urgent and escalating problem, facilitated by the so-called 'triple-A engine': accessibility, affordability and anonymity (Fry et al., 2025). Artificial intelligence amplifies each of these three factors: it makes the production of abusive material more accessible, further reduces the costs of production and distribution, and reinforces the anonymity of perpetrators. According to the CyberTipline of the US National Centre for Missing and Exploited Children, over 36.2 million reports of images and videos suspected of containing OCSEA were received in 2023, representing a 13 per cent increase on 2022 and a 23 per cent increase on 2021 (Fry et al., 2025). The rapid development of social media and other virtual environments is enabling new technological methods and types of abuse to emerge, making it extremely difficult to estimate the full extent of these crimes (Fry et al., 2025).

The difficulty in gauging the scale of these offences does not prevent an active conversation from taking place in parallel regarding AI-generated pornography; a quantitative content analysis of 390 Reddit posts on this topic revealed that the experiences discussed range from outrage and concern about its actual and potential harms to curiosity, enjoyment and even economic benefits (Döring et al., 2025). The production (59.5 per cent) and content (60.8 per cent) of AI pornography were the most discussed topics, whilst ethical and legal implications featured in only around a third of the posts (35.1 per cent). This highlights the need for a nuanced response from legislators, technology developers, educators and mental health professionals (Döring et al., 2025). The use of images of people in pornographic contexts without their consent is an increasingly widespread offence, and illegal activities carried out using AI-generated images are a variant of this phenomenon that highlights how ill-suited legal systems are to a changing reality (Mania, 2024).

Online violence against women is a growing global problem, and the use of *deepfakes* in the context of violence against women has attracted considerable attention (Lazard et al., 2025). As the social sciences begin to examine the implications of the creation and dissemination of *deepfakes* in the context of sexual violence, it is also necessary to investigate how these *deepfakes* are used to silence women in digital public spaces; it is essential to empirically recognise the systemic gender discrimination inherent in both *deepfake* technology and its uses (Lazard et al., 2025). Research must go beyond detection techniques and perceived credibility and move towards an analysis of the intersectional power dynamics at play in this form of violence.

3.4. CYBERSECURITY AS A PREVENTION TOOL

Cybersecurity can act as a preventative tool through technological, educational and platform design strategies, although current evidence suggests that technological responses are necessary but not sufficient on their own, requiring them to be complemented by specialised human resources and survivor-centred approaches (Harkin and Merkel, 2023).

A systematic review from 2023 identified 136 apps for the prevention of domestic violence, classified into five categories (Sumra et al., 2023):

Table 1
Categories of apps for the prevention of domestic violence

Category	%	Description and context of use
Emergency assistance	44.9%	Generation of emergency alerts. This is not limited to situations requiring avoidance; it also intervenes in cases of ongoing violence, imminent threats or any high-risk situation requiring immediate intervention (e.g. active assault, harassment, danger to physical safety).
Avoidance	21.3%	Geofences, accelerometer-based alerts, shake-based alerts. Primarily aimed at preventing encounters with the aggressor or detecting sudden movements that may indicate an attack whilst on the move or being stalked.
Informative	21.3%	These provide information on support services, rights, refuges, emergency helplines, etc.
Legal information	7.4%	Basic legal advice, steps to take when reporting an incident, necessary documentation.
Self-assessment	5.1%	Basic legal advice, steps to take when reporting a case, necessary documentation.

Note. Adapted from Sumra, M., Asghar, S., Khan, K. S., Fernández-Luna, J. M., Huete, J. F., and Bueno-Cavanillas, A. (2023). Smartphone Apps for Domestic Violence Prevention: A Systematic Review. International Journal of Environmental Research and Public Health, 20(7), 5246.

Despite their usefulness, cybersecurity apps have significant limitations. More than half of the emergency alerts require manual activation by the potential victim, with no automation whatsoever, and none of the apps reviewed incorporated artificial intelligence to assist people at risk. Future apps should prioritise automation and make better use of AI through multimedia features, voice recognition and tone detection, in order to contribute to real-time situation analysis (Sumra et al., 2023).

Furthermore, integrating online safety into established, evidence-based programmes – those that currently address related harms such as general bullying, abuse in intimate relationships or the prevention of sexual abuse – offers significant advantages (Finkelhor et al., 2021). These advantages stem from four factors: the considerable overlap between online and offline harms; the higher prevalence of harms offline; the same underlying risk factors; and the more robust empirical basis of longer-standing programmes, originally developed for offline settings (Finkelhor et al., 2021). Furthermore, prevention interventions should focus on modifying the opportunities, facilities and infrastructure that enable harm to be perpetrated, as well as on addressing problematic attitudes and social norms (Henry and Beard, 2024). This implies that technology platforms must take active responsibility for the design and regulation of their services.

In this context, so-called ‘dark patterns’ – techniques that manipulate users into making decisions contrary to their own interests – are particularly relevant. They are categorised under the acronym FORCES: Frame, Obstruct, Ruse, Compel, Entangle and Seduce. These techniques exploit psychological principles such as negativity bias, the curiosity gap and cognitive fluency to encourage social content to go viral (Fagan, 2024). Furthermore, digital platforms incorporate elements that may facilitate or exacerbate sexual cyberviolence (Fagan, 2024; Munzer et al., 2026

Furthermore, digital platforms frequently incorporate features that can facilitate or exacerbate sexual cyberviolence (Fagan, 2024; Munzer et al., 2026):

Table 2
Elements that may facilitate or exacerbate sexual cyberviolence

Frequent in-game rewards	Notification and ‘like’ systems that generate compulsive behaviour and increase the time spent exposed to potentially abusive content
Embedded distractions	Excessive adverts or interactive elements that hinder safe browsing and privacy settings
Viralisation algorithms	Systems that prioritise sensationalist or provocative content, potentially amplifying the spread of harmful content
Default privacy settings	Settings that prioritise public visibility over user privacy

Note. Adapted from Fagan, P. (2024). Clicks and tricks: The dark art of online persuasion. Current Opinion in Psychology, 58, 101844 and Munzer, T., Parga-Belinkie, J., Milkovich, L. M., Tomopoulos, S., Ajumobi, T., Cross, C., Gerwin, R., Madigan, S., Psych, R., and Council on Communications and Media. (2026). Digital Ecosystems, Children, and Adolescents: Policy Statement. *Pediatrics*, 157(2), e2025075320.

With the advancement of technologies such as predictive algorithms, generative artificial intelligence and virtual reality, these techniques will become increasingly powerful (Fagan, 2024). It is therefore essential that platforms commit to an ethical design that prioritises user safety, particularly when it comes to vulnerable groups such as women or sexual minorities (Ray and Henry, 2025).

However, the European and Spanish regulatory frameworks have significant shortcomings when it comes to tackling new forms of sexual cyberviolence. The European Artificial Intelligence Regulation (AI Act) classifies AI systems according to their level of risk, but sexualised deepfakes are not explicitly regulated within its categories of unacceptable risk. The Digital Services Act (DSA) imposes content moderation obligations on platforms, but its effective application to non-consensual deepfake pornography faces challenges relating to detection and scale. In Spain, Organic Law 10/2022 on the comprehensive guarantee of sexual freedom (‘the “only yes means yes” law’) incorporates some forms of digital violence, but the regulation of non-consensual deepfakes remains insufficient (Mania, 2024).

The case law of the European Court of Human Rights has established positive obligations on states regarding digital violence. In Buturugă v. Romania (2020), the

ECHR ruled against Romania for failing to protect a woman who was being harassed online, holding that Article 8 (right to private life) and Article 3 (prohibition of inhuman or degrading treatment) impose a duty on States to take reasonable measures to prevent digital violence. In Volodina v. Russia (2019 and 2021), the Court emphasised that state inaction in the face of repeated cyberbullying constitutes a violation of human rights. These judgments are particularly relevant to cases of sextortion and the non-consensual dissemination of intimate images. Furthermore, the CEDAW Committee has issued specific recommendations on digital gender-based violence (General Recommendation No. 35), urging States to criminalise forms of violence against women facilitated by technology. The European Institute for Gender Equality (EIGE) and Europol have published recent reports warning of the rise in sexualised deepfakes and the need for legislative harmonisation, whilst UN Women has developed guidelines for the prevention of online violence against women.

Despite this framework, victims rarely report such incidents. According to Colburn et al. (2023), only 7.3% of incidents of online violence are reported on websites, and of that percentage, the majority are left dissatisfied: less than half (42.2%) feel that the site took useful action, and only 29.8% rate the police response as useful, in cases where a report was actually made. The risk that technology may end up facilitating abuse is real; therefore, as Shirzad et al. (2025) point out, it is essential to ensure that its use in contexts of sexual violence is safe and ethical.

4. LIMITATIONS AND FUTURE DIRECTIONS

Despite the rigour of the search and analysis, this study has a number of limitations that must be borne in mind when interpreting its conclusions.

Firstly, this is a narrative review rather than a systematic review with a meta-analysis. Although the narrative approach allows findings from highly diverse study designs to be integrated and offers a broad view of the phenomenon, it lacks the level of standardisation and reproducibility that a meta-analysis would guarantee.

Secondly, most of the studies included in the review are cross-sectional in nature, which prevents the establishment of robust causal relationships between victimisation and mental health outcomes. It cannot be determined with certainty whether anxiety and depression are consequences of cyberviolence or whether, on the contrary, certain pre-existing vulnerability profiles increase the risk of experiencing it. Nor are there any Spanish longitudinal studies available that would allow for an analysis of the temporal evolution of victimisation.

Thirdly, unequal attention has been paid to the different forms of sexual cyberviolence. The bulk of the evidence focuses on digital sexual harassment (comments, innuendo, sending unsolicited images), whilst phenomena such as sextortion, image-based abuse or grooming appear less frequently in national studies. This may be due both to the lower visibility of these forms of violence and to the absence of specific instruments validated in the Spanish population for all types.

Fourthly, the study has not been able to systematically address the experiences of women with intersectional identities (migrant women, women with disabilities, Roma women, LGBTIQ+ women). Although it is mentioned at times that disability or age are

risk factors, there is insufficient disaggregated evidence to analyse how different axes of inequality interact in victimisation and its consequences.

Fifthly, the study faces the limitations inherent in secondary sources: prevalence data depend on what victims are willing to report, and it is known that reporting and disclosure rates are very low (barely 7.3% on online platforms (Colburn et al., 2023), and 9.2% for non-partner sexual violence (Pastor-Moreno et al., 2022)). This implies that the figures provided likely underestimate the true scale of the problem, particularly in the case of forms of violence that are more stigmatised or less socially recognised as such.

Finally, with regard to the analysis of artificial intelligence and cybersecurity, the review has drawn on a rapidly evolving body of literature. Given that the search cut-off date was February 2026, it is possible that some studies or reports published after that date may not have been included, particularly those assessing the effectiveness of the most recent prevention measures.

In light of these limitations, the following avenues for future research are suggested. It would be necessary to investigate all the issues highlighted by these limitations, placing particular emphasis on three aspects. Firstly, to study intersectional populations and less visible forms of violence in greater depth. Secondly, the effectiveness of current responses should be investigated, including cybersecurity training with a gender perspective, the development of specific protocols, and the integration of digital technologies into sex education. Finally, given the rapid evolution of AI and cybersecurity, it is recommended that the evidence be periodically updated and that longitudinal studies be designed to assess the actual impact of interventions and the effectiveness of legal reforms. Overall, comprehensive responses are needed that combine technological strategies, legal reforms and compulsory gender-sensitive educational programmes to effectively tackle sexual cyberviolence in Spain.

5. CONCLUSIONS

The findings of this review confirm that sexual cyberviolence is a widespread phenomenon in Spain, disproportionately affecting young women: 25.3 per cent of women aged 16 to 24 have experienced online sexual harassment. The high prevalence, particularly among those aged 16 to 34, indicates that digital sexual harassment is not an exceptional experience, but rather the norm within women's everyday interactions in digital environments. This pattern across age groups is consistent with international studies (Latcheva, 2017) and suggests that early digital socialisation and the pressure to maintain an active presence on social media act as specific vulnerability factors. The documented psychological consequences – suicidal ideation, anxiety, depression, trauma, post-traumatic stress, sleep problems, low self-esteem and self-objectification – are serious and consistent with the international literature (Champion et al., 2022; Iroegbu et al., 2024).

The most significant finding from a theoretical perspective is the exacerbating role of myths about sexual cyberviolence. Women who internalise these beliefs exhibit poorer mental health following victimisation, and this effect is mediated by self-objectification (Vizcaíno-Cuenca et al., 2025). This mechanism, which had not previously been explored in the Spanish context, provides empirical evidence for the theory of objectification as

applied to the digital environment and suggests that the culture of digital rape not only justifies violence but also actively amplifies psychological harm.

With regard to artificial intelligence, the results indicate that AI is qualitatively transforming the perpetration of such abuse. The ease with which deepfakes can be created and the automation of sextortion remove barriers that previously limited this type of abuse (Williams, 2025; Lazard et al., 2025). Unlike more traditional forms of online sexual violence, where the victim usually had some degree of prior interaction or voluntarily shared their images, AI makes it possible to turn any woman with an online presence into a potential victim, thereby bypassing current legal and prevention frameworks (Mania, 2024). The novel finding of this review is the observation that public debate on forums such as Reddit continues to prioritise production and content over ethical and legal implications (Döring et al., 2025), indicating a worrying normalisation.

In the field of cybersecurity, the findings confirm that existing applications are insufficient. The lack of automation and the absence of artificial intelligence in current tools (Sumra et al., 2023) contrast with the sophistication of the methods used to commit these offences. Reporting rates do not exceed 7.3 per cent and dissatisfaction with institutional responses is widespread (Colburn et al., 2023), pointing to a structural mistrust that cannot be resolved by technological improvements alone, but requires changes to support protocols and the training of professionals.

When comparing these findings with previous studies, there is continuity with what has been documented regarding offline sexual violence in terms of risk factors and psychological consequences. However, the digital nature of the phenomenon introduces novel elements – the permanence of the digital footprint, instant virality and the ease with which perpetrators can remain anonymous – which explain why offline prevention strategies cannot be directly transferred to the online environment.

The main contribution of this article is to provide an up-to-date synthesis of the evidence available in Spain, integrating, for the first time, a gender perspective, an analysis of myths surrounding cyberviolence, the role of artificial intelligence as a tool for perpetration, criminological approaches (theory of routine online activities, digital disinhibition, neutralisation techniques) and a legal-criminal analysis (case law of the European Court of Human Rights, the AI Act, the DSA, and recommendations from CEDAW, EIGE and UN Women) within a single framework. In contrast to previous literature, which tends to address these forms of violence in a fragmented manner, this review highlights their interconnection and how structural gender inequalities are carried over and amplified in the digital space.

This article has addressed the objectives set out in the introduction. The findings confirm the high prevalence of sexual cyberviolence in Spain, particularly amongst young women; its serious consequences for mental health; the exacerbating role of myths about cyberviolence through self-objectification; the accelerating effect of artificial intelligence in perpetuating such violence; and the shortcomings of current cybersecurity measures, which result in very low reporting rates.

As practical recommendations, we suggest: (a) incorporating questions on sexual cyberviolence into mental health protocols; (b) designing compulsory educational programmes that address myths about cyberviolence and promote a gender-sensitive

approach to digital sexuality; (c) requiring digital platforms to adopt an ethical design that eliminates dark patterns and prioritises women's privacy; (d) training cybersecurity and law enforcement professionals in a gender-sensitive approach and survivor-centred care; and (e) harmonising legislation on non-consensual sexualised deepfakes online with the recommendations of the European Court of Human Rights (ECHR), CEDAW, EIGE and UN Women.

6. REFERENCES

Benítez-Hidalgo, V., Henares-Montiel, J., Ruiz-Pérez, I., and Pastor-Moreno, G. (2024). Cyber sexual harassment against women and its impact on health. A cross-sectional study in a representative population sample. Journal of Public Health, 46(1), 3–11. https://doi.org/10.1093/pubmed/fdad182

Benítez-Hidalgo, V., Henares-Montiel, J., Ruiz-Pérez, I., and Pastor-Moreno, G. (2025). International prevalence of technology-facilitated sexual violence against women: A systematic review and meta-analysis of observational studies. Trauma, Violence and Abuse, 26(4), 668–681. https://doi.org/10.1177/15248380241286813

Casanovas, L. V.-L., Serra, L., Canals, C. S., Sanz-Barbero, B., Vives-Cases, C., López, M. J., Otero-García, L., Pérez, G., and Renart-Vicens, G. (2022). Prevalence of sexual harassment among young Spaniards before, during, and after the COVID-19 lockdown period in Spain. BMC Public Health, 22(1), 1888. https://doi.org/10.1186/s12889-022-14264-9

Castellanos-Torres, E., Sanz-Barbero, B., Vives-Cases, C., and the CIBER Programme on Violence and Young People team. (2023). COVID-19 and sexual violence against women: A qualitative study on the perspectives of young people and professionals in Spain. PloS One, 18(8), e0289402. https://doi.org/10.1371/journal.pone.0289402

Champion, A. R., Oswald, F., Khera, D., and Pedersen, C. L. (2022). Examining the Gendered Impacts of Technology-Facilitated Sexual Violence: A Mixed Methods Approach. Archives of Sexual Behaviour, 51(3), 1607–1624. https://doi.org/10.1007/s10508-021-02226-y

Colburn, D. A., Finkelhor, D., and Turner, H. A. (2023). Help-Seeking From Websites and Police in the Aftermath of Technology-Facilitated Victimisation. Journal of Interpersonal Violence, 38(21–22), 11642–11665. https://doi.org/10.1177/08862605231186156

Colburn, D., Mitchell, K. J., Gewirtz-Meydan, A., Finkelhor, D., Turner, H. A., and O'Brien, J. E. (2025). Life impact following childhood image-based sexual abuse victimisation among a sample of young adults. Child Abuse and Neglect, 167, 107584. https://doi.org/10.1016/j.chiabu.2025.107584

Committee on the Elimination of Discrimination against Women. (26 July 2017). General Recommendation No. 35 on gender-based violence against women, updating General Recommendation No. 19 (CEDAW/C/GC/35). UNHCR. https://www.acnur.org/fileadmin/Documentos/BDL/2017/11405.pd

Cunha-Oliveira, A., Camarneiro, A. P., Gómez-Cantarino, S., Cipriano-Crespo, C., Queirós, P. J. P., Cardoso, D., Santos, D. G., and Ugarte-Gurrutxaga, M. I. (2021). The Integration of a Gender Perspective into Young People's Sexuality Education in Spain and Portugal: Legislation and Educational Models. International Journal of Environmental Research and Public Health, 18(22), 11921. https://doi.org/10.3390/ijerph182211921

Döring, N., Le, T. D., and Miller, D. J. (2025). Experiences with AI-Generated Pornography: A Quantitative Content Analysis of Reddit Posts. Archives of Sexual Behaviour. https://doi.org/10.1007/s10508-025-03227-x

Durán, M., and Rodríguez-Domínguez, C. (2023). Sending of Unwanted Dick Pics as a Form of Sexual Cyber-Violence: An Exploratory Study of Its Emotional Impact and Reactions in Women. Journal of Interpersonal Violence, 38(5-6), 5236–5261. https://doi.org/10.1177/08862605221120906

European Institute for Gender Equality. (2024). Combating cyber violence against women and girls: Developing an EU measurement framework. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/4a0b01fc-e839-11ef-b5e9-01aa75ed71a1/language-en

Europol. (2025). Internet Organised Crime Threat Assessment (IOCTA) 2025: Steal, deal and repeat: How cybercriminals trade and exploit your data. Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

Fagan, P. (2024). Clicks and tricks: The dark art of online persuasion. Current Opinion in Psychology, 58, 101844. https://doi.org/10.1016/j.copsyc.2024.101844

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., and Collier, A. (2021). Youth Internet Safety Education: Aligning Programmes With the Evidence Base. Trauma, Violence and Abuse, 22(5), 1233–1247. https://doi.org/10.1177/1524838020916257

Flynn, A., Powell, A., Eaton, A., and Scott, A. J. (2025). Sexualised Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualised Deepfake Imagery. Journal of Interpersonal Violence, 8862605251368834. https://doi.org/10.1177/08862605251368834

Fry, D., Krzeczkowska, A., Ren, J., Lu, M., Fang, X., and the Into the Light Index Study Group. (2025). Prevalence estimates and nature of online child sexual exploitation and abuse: A systematic review and meta-analysis. The Lancet. Child and Adolescent Health, 9(3), 184–193. https://doi.org/10.1016/S2352-4642 (24) 00329–8

Fuentes, P. A., and Berger, T. C. (2025). Pornography and sexuality on OnlyFans: The role of female subjectivation. Persona y Sociedad, 39(1), 11–25. https://doi.org/10.53689/pys.v39i1.467

García Mingo, E., Lorca, J. G., and Ruíz Repullo, C. (2025). "Technology in the service of equality": A research agenda on digital sexual violence in Spain. https://doi.org/10.5565/rev/athenea.3687

García-Vázquez, J., Ruiz-Azcona, L., Pellico-López, A., and Paz-Zulueta, M. (2024). Characteristics of emotional and sexuality education programmes in the Spanish school population. Heliyon, 10(20), e39368. https://doi.org/10.1016/j.heliyon.2024.e39368

Harkin, D., and Merkel, R. (2023). Technology-Based Responses to Technology-Facilitated Domestic and Family Violence: An Overview of the Limits and Possibilities of Tech-Based 'Solutions'. Violence Against Women, 29(3-4), 648–670. https://doi.org/10.1177/10778012221088310

Hellevik, P. M., Haugen, L.-E. A., and Överlien, C. (2025). Outcomes of image-based sexual abuse among young people: A systematic review. Frontiers in Psychology, 16, 1599087. https://doi.org/10.3389/fpsyg.2025.1599087

Henry, N., and Beard, G. (2024). Image-Based Sexual Abuse Perpetration: A Scoping Review. Trauma, Violence and Abuse, 25(5), 3981–3998. https://doi.org/10.1177/15248380241266137

Henry, N., Flynn, A., and Powell, A. (2020). Technology-Facilitated Domestic and Sexual Violence: A Review. Violence Against Women, 26(15–16), 1828–1854. https://doi.org/10.1177/1077801219875821

Henry, N., and Flynn, A. (2019). Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. Violence Against Women, 25(16), 1932–1955. https://doi.org/10.1177/1077801219863881

Henry, N., and Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. Trauma, Violence and Abuse, 19(2), 195–208. https://doi.org/10.1177/1524838016650189

Iroegbu, M., O'Brien, F., Muñoz, L. C., and Parsons, G. (2024). Investigating the Psychological Impact of Cyber-Sexual Harassment. Journal of Interpersonal Violence, 39(15–16), 3424–3445. https://doi.org/10.1177/08862605241231615

Karasavva, V. (2025). The Frequency, Nature, Impact, and Coping Strategies of Non-consensual Intimate Image Dissemination Victimisation: A Scoping Review. Trauma, Violence and Abuse, 15248380251383940. https://doi.org/10.1177/15248380251383940

Karasavva, V., and Noorbhai, A. (2021). The Real Threat of Deepfake Pornography: A Review of Canadian Policy. Cyberpsychology, Behaviour and Social Networking, 24(3), 203–209. https://doi.org/10.1089/cyber.2020.0272

Latcheva, R. (2017). Sexual Harassment in the European Union: A Pervasive but Still Hidden Form of Gender-Based Violence. Journal of Interpersonal Violence, 32(12), 1821–1852. https://doi.org/10.1177/0886260517698948

Lazard, L., Capdevila, R., Turley, E. L., Gilfoyle, K., and Stavropoulou, N. (2025). Deepfake Technology and Gender-Based Violence: A Scoping Review. Trauma, Violence and Abuse, 15248380251384271. https://doi.org/10.1177/15248380251384271

López-Barranco, P.J.; López-Yepes, S.; Conesa-Ferrer, M.B.; Cayuela-Fuentes, P.S.; Beladiez-Pérez, M.d.M.; Jiménez-Ruiz, I. Violence Against Women on Social Networks: A Descriptive Analysis. Healthcare 2025, 13, 2574. http://hdl.handle.net/10201/170129

Lorca, J. G. (2024). Redress for harm suffered by women affected by image-based sexual abuse in Spain. Tendencias Sociales. Revista de Sociología, 2(10). https://doi.org/10.5944/ts.2023.43124

Mania, K. (2024). Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study. Trauma, Violence and Abuse, 25(1), 117–129. https://doi.org/10.1177/15248380221143772

Mármol, C. J., Luna, A., and Legaz, I. (2025). Disproportionate Cybersexual Victimisation of Women from Adolescence into Midlife in Spain: Implications for Targeted Protection and Prevention. Behavioural Sciences, 15(11), 1571. https://doi.org/10.3390/bs15111571

Martínez Bacaicoa, J. (2024). Technology-facilitated sexual and gender-based violence: Measurement, moral disengagement, and factors related to perpetration and victimisation (p. 1). https://dialnet.unirioja.es/servlet/tesis?codigo=362106

Martínez-Bacaicoa, J., Henry, N., Mateos-Pérez, E., and Gámez-Guadix, M. (2024). Online Gendered Violence Victimisation Among Adults: Prevalence, Predictors and Psychological Outcomes. Psicothema, 36(3), 247–256. https://doi.org/10.7334/psicothema2023.315

Martínez Román, R., Lameiras Fernández, M., Adá Lameiras, A., and Rodríguez Castro, Y. (2026). Analysis of Image-Based Sexual Harassment and Abuse in Adolescents' Socio-Affective Relationships. Journal of Interpersonal Violence, 41(3-4), 816–840. https://doi.org/10.1177/08862605251315767

Mayuri-Bocanegra, E., and Aliaga-Pacora, A. A. (2023). The regulation of human trafficking for the purposes of labour exploitation and the recruitment of victims via social media in Lima. Ciencia Latina Revista Científica Multidisciplinar, 7(3), 452–471. https://doi.org/10.37811/cl_rcm.v7i3.6206

Medina-Bravo, P. (2021). Women's empowerment: The trap of a tamed feminism. Discurso y Sociedad, 15(3), 588–600. https://doi.org/10.14198/dissoc.15.3.4

Ministry of Equality. (2025). 2024 Macro-survey on Violence against Women. Government Delegation against Gender-Based Violence. https://violenciagenero.igualdad.gob.es/violenciaencifras/macroencuesta-de-violencia-contra-la-mujer-2024/

Morgan, C. H., Stager, L. M., Brockdorf, A. N., Salamanca, N. K., Amaya, S., Mujica, C. A., Davis, K. C., Leone, R., Orchowski, L. M., Gilmore, A. K., and López, C. (2025). Sleep-Related Concerns Mediate the Association Between Cyber-Sexual Victimisation and Psychological Distress Among Diverse University Students. Cyberpsychology, Behaviour and Social Networking, 28(10), 689–697. https://doi.org/10.1177/21522715251375417

Munzer, T., Parga-Belinkie, J., Milkovich, L. M., Tomopoulos, S., Ajumobi, T., Cross, C., Gerwin, R., Madigan, S., Psych, R., and Council on Communications and Media. (2026). Digital Ecosystems, Children, and Adolescents: Policy Statement. Pediatrics, 157(2), e2025075320. https://doi.org/10.1542/peds.2025-075320

UN Women. (2024). Technology-facilitated violence against women and girls: a rapidly evolving threat. In Stepping up efforts to eliminate all forms of violence against women and girls: Report of the Secretary-General (A/79/500). UN Women. https://www.unwomen.org/es/digital-library/publications/2024/10/intensificacion-de-los-esfuerzos-para-eliminar-todas-las-formas-de-violencia-contra-las-mujeres-y-las-ninas-informe-del-secretario-general-2024

Pastor-Moreno, G., Ruiz-Pérez, I., Sordo, L., and Henares-Montiel, J. (2022). Frequency, Types, and Manifestations of Partner Sexual Violence, Non-Partner Sexual Violence and Sexual Harassment: A Population Study in Spain. International Journal of Environmental Research and Public Health, 19(13), 8108. https://doi.org/10.3390/ijerph19138108

European Parliament and Council of the European Union. (13 June 2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Regulation). Official Journal of the European Union, L 2024/1689. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689

European Parliament and Council of the European Union. (19 October 2022). Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation). Official Journal of the European Union, L 277, 1–102. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R2065

Ray, A., and Henry, N. (2025). Sextortion: A Scoping Review. Trauma, Violence and Abuse, 26(1), 138–155. https://doi.org/10.1177/15248380241277271

Rodríguez-Castro, Y., Martínez-Román, R., Alonso-Ruido, P., Adá-Lameiras, A., and Carrera-Fernández, M. V. (2021). Intimate Partner Cyberstalking, Sexism,

Pornography, and Sexting in Adolescents: New Challenges for Sex Education. International Journal of Environmental Research and Public Health, 18(4), 2181. https://doi.org/10.3390/ijerph18042181

Salerno-Ferraro, A. C., Erentzen, C., and Schuller, R. A. (2022). Young Women's Experiences With Technology-Facilitated Sexual Violence From Male Strangers. Journal of Interpersonal Violence, 37(19-20), NP17860-NP17885. https://doi.org/10.1177/08862605211030018

Shirzad, M., Ramaiya, A., Edwards, K., Yuan, M., Bhanot, S., and Kaufman, M. R. (2025). Using safe and ethical technology to prevent and respond to sexual and interpersonal violence during adolescence and young adulthood: Identifying evidence, best practices, and pathways forward—A global scoping review protocol. PloS One, 20(8), e0320709. https://doi.org/10.1371/journal.pone.0320709

Sumra, M., Asghar, S., Khan, K. S., Fernández-Luna, J. M., Huete, J. F., and Bueno-Cavanillas, A. (2023). Smartphone Apps for Domestic Violence Prevention: A Systematic Review. International Journal of Environmental Research and Public Health, 20(7), 5246. https://doi.org/10.3390/ijerph20075246

European Court of Human Rights. (11 February 2020). Buturugă v. Romania (Application No. 56867/15). https://hudoc.echr.coe.int/eng?i=001-201342

European Court of Human Rights. (2019). Volodina v. Russia, Application No. 41261/17, judgment of 9 July 2019. Council of Europe. https://www.cepc.gob.es/sites/default/files/2021-12/sentencia-volodina-v-rusia.pdf

Vizcaíno-Cuenca, R., Carretero-Dios, H., and Romero-Sánchez, M. (2026). 'It's Not Violence, It's an Exaggerated Complaint': The Role of Cyber-Rape Culture and Objectification Theory in Understanding the Emotional Impact on Women Who Have Experienced Cyber-Sexual Violence. Journal of Sex Research, 63(2), 270–283. https://doi.org/10.1080/00224499.2025.2592624

Williams, K. (2025). 'There Are No Limits!': AI Undressing Apps and the Normalisation of Non-consensual Intimate Deepfakes. Violence Against Women, 10778012251397966. https://doi.org/10.1177/10778012251397966

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.9051