



Artículo de Investigación

# CIBERVIOLENCIAS SEXUALES CONTRA LA POBLACIÓN FEMENINA EN ESPAÑA: UN ANÁLISIS DE LAS IMPLICACIONES PSICOSOCIALES DESDE LA PERSPECTIVA DE GÉNERO

**María Calvo Lorenzo**  
Universidad de Granada  
mariacalvo1@correo.ugr.es  
ORCID: 0009-0001-1078-9557

Recibido 28/04/2026  
Aceptado 01/06/2026  
Publicado 30/06/2026

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

Cita recomendada: Calvo, M. (2026). Ciberviolencias sexuales contra la población femenina en España: un análisis de las implicaciones psicosociales desde la perspectiva de género. *Revista Logos Guardia Civil*, 4(2), pp. 59-84  
<https://doi.org/10.64217/logosguardiacivil.v4i2.9051>

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)  
Depósito Legal: M-3619-2023  
NIPO en línea: 126-23-019-8  
ISSN en línea: 2952-394X



## **CIBERVIOLENCIAS SEXUALES CONTRA LA POBLACIÓN FEMENINA EN ESPAÑA: UN ANÁLISIS DE LAS IMPLICACIONES PSICOSOCIALES DESDE LA PERSPECTIVA DE GÉNERO**

**Sumario:** 1. INTRODUCCIÓN. 2. METODOLOGÍA. 2.1. Diseño del estudio. 2.2. Estrategia de búsqueda. 2.3. Criterios de inclusión y exclusión. 2.4. Extracción y síntesis de datos. 2.5. Calidad metodológica y validez. 2.6. Replicabilidad. 3. RESULTADOS Y DISCUSIÓN. 3.1. Dimensiones de las ciberviolencias y tipología. 3.2. Consecuencias y factores de riesgo en las víctimas. 3.3. Inteligencia artificial en la perpetración. 3.4. Ciberseguridad como herramienta de prevención. 4. LIMITACIONES Y LÍNEAS FUTURAS. 5. CONCLUSIONES. 6. REFERENCIAS BIBLIOGRÁFICAS.

**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.

**Abstract:** In order to analyze technology-facilitated sexual violence 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. Technology-facilitated sexual violence is a growing phenomenon that disproportionately affects women, demonstrating how digital technologies amplify structural gender inequalities. Its main dimensions include digital sexual harassment, sextortion, image-based sexual abuse or "revenge porn", as well as emerging phenomena such as the whitewashing of the sex business on content platforms. Documented mental health consequences include suicidal ideation and attempts, anxiety, depression, trauma, post-traumatic stress disorder, sleep problems, low self-esteem, and self-objectification. Artificial intelligence has emerged as a new tool for perpetration, facilitating the creation of deepfakes and non-consensual nudity applications. In the field of prevention, cybersecurity offers technological tools, although existing applications have significant limitations and reporting rates remain below 7.3%. It is concluded that technology-facilitated sexual violence is an amplified expression of gender inequalities, requiring comprehensive interventions that combine gender-sensitive education, platform regulation, professional training, and ethical technology design.

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

**Keywords:** cybersecurity, sextortion, digital sexual harassment, digital platforms, gender equity

## **ABREVIATURAS**

IA: Inteligencia Artificial

IBSA: Abuso sexual basado en imágenes

NCI: Imágenes íntimas no consentidas

NCIID: Difusión no consensuada de imágenes íntimas

OCSEA: Explotación y abuso sexual infantil en línea

TFSV: Violencia sexual facilitada por la tecnología

TEDH: Tribunal Europeo de Derechos Humanos

AI Act: Reglamento Europeo de Inteligencia Artificial

DSA: Digital Services Act

## 1. INTRODUCCIÓN

La digitalización de las relaciones humanas ha transformado profundamente los espacios de interacción social, creando nuevos escenarios donde las violencias tradicionales se reproducen, amplifican y adquieren formas hasta el momento desconocidas. Entre ellas, las ciberviolencias sexuales constituyen un fenómeno creciente que afecta de manera desproporcionada a las mujeres, evidenciando cómo las tecnologías digitales no son espacios neutrales, sino un territorio donde las desigualdades estructurales de género se profundizan y adquieren nuevas expresiones (Mármol et al., 2025). Este artículo hace un análisis de las ciberviolencias sexuales contra la población femenina en España desde una perspectiva psicosocial y de género, considerando tanto su magnitud como sus implicaciones en la salud mental y el bienestar de las víctimas.

La violencia sexual facilitada por la tecnología (TFSV) se define como cualquier comportamiento sexual no deseado que incluye el uso de tecnologías digitales, abarcando tanto daños sexuales virtuales como presenciales facilitados por medios digitales (Champion et al., 2022; Henry y Powell, 2018). Bajo este paraguas entran el acoso sexual en línea, el acoso basado en género o sexualidad, el ciberacoso, la explotación sexual basada en imágenes y el uso de servicios de comunicación para coaccionar a una víctima a realizar actos sexuales no deseados (Henry y Powell, 2018). En el contexto español, la tipología empleada por el Ministerio del Interior incluye delitos como el abuso sexual, acoso sexual, corrupción de menores, grooming, exhibicionismo, difusión de imágenes de abuso sexual infantil y provocación sexual, todos ellos perpetrados a través de medios digitales (Mármol et al., 2025).

La investigación sugiere que la TFSV se entienda dentro de marcos conceptuales que utilizan teorías de género y de redes de actores para comprender las causas y consecuencias de las experiencias de abuso y violencia de las mujeres, facilitadas por tecnologías digitales (Henry et al., 2020). Esta perspectiva es esencial, ya que estas violencias no constituyen incidentes aislados, sino expresiones de desigualdades sociales y estructurales más amplias que determinan quién está en riesgo y cómo se manifiesta la violencia (Mármol et al., 2025). Estudios recientes subrayan el papel de la desconexión moral y la ideología sexista, tanto hostil como benévola, en la perpetuación de estas conductas, mostrando que los hombres, aquellos con actitudes sexistas más arraigadas y quienes se sitúan en posiciones de poder tienen mayores niveles de justificación de la ciberviolencia sexual (Martínez-Bacaicoa, 2024; Durán y Rodríguez, 2019). Asimismo, se ha documentado que los varones son los principales perpetradores, aunque las mujeres y personas no binarias también pueden ejercer este tipo de violencia, a menudo motivados por la defensa propia, el manejo de emociones desagradables o la falta de reflexión (Martínez-Bacaicoa et al., 2023).

La literatura científica revela importantes desafíos terminológicos y conceptuales en este campo (Henry et al., 2020). Los límites conceptuales de la TFSV son amplios y dinámicos, adaptándose continuamente a las nuevas tecnologías emergentes y a los usos de estas, como los *deepfake*, los sistemas de inteligencia artificial generativa y las comunicaciones encriptadas, que complican aún más la detección y la asunción de responsabilidades (Mármol et al., 2025).

En España, el estudio de la ciberviolencia sexual ha adquirido una relevancia creciente, impulsado por la disponibilidad de nuevos instrumentos de medición validados,

como la Escala de Victimización Sexual Online y el Cuestionario de Violencia en el Noviazgo Digital (Martínez-Bacaicoa, 2024), así como por el desarrollo de agendas de investigación que abordan la relación entre tecnologías digitales y violencia sexual desde una perspectiva integral (García Mingo et al., 2025).

A pesar de estos avances, persisten importantes desafíos: la invisibilidad estadística de ciertas formas de violencia, la dificultad para capturar la continuidad entre el mundo *offline* y *online*, la escasa atención a las experiencias de mujeres adultas más allá de la juventud y la falta de investigaciones longitudinales que permitan comprender la evolución de la victimización en función del sexo y la edad.

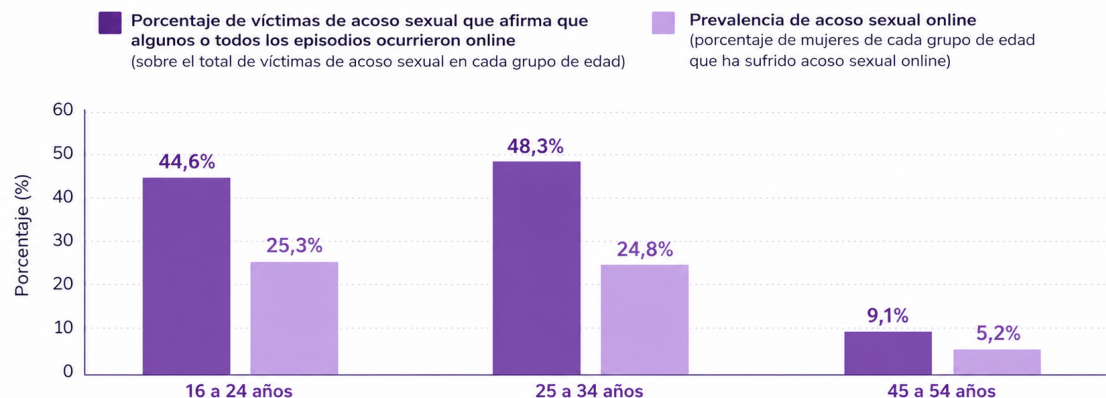
La magnitud del fenómeno en España alcanza cifras preocupantes. Según los datos de la Macroencuesta de Violencia contra la Mujer de 2019, aproximadamente el 9,15% de las mujeres españolas ha experimentado acoso sexual cibernético en algún momento de su vida, con impactos significativos en la salud mental que incluyen tasas elevadas de ideación suicida, depresión y ansiedad (Benítez-Hidalgo et al., 2024).

Los datos más recientes de la Macroencuesta de Violencia contra la Mujer de 2024 permiten afinar esta realidad. Atendiendo al lugar de la agresión, el 20,7% de las mujeres que han sufrido acoso sexual en algún momento señalan que ocurrió *online* (por ejemplo, en páginas web, redes sociales como Instagram o TikTok, aplicaciones de mensajería como WhatsApp, aplicaciones de citas como Tinder, videoconferencias, etc.). Eso supone que el 7,5% de todas las mujeres de 16 o más años residentes en España, alrededor de 1,6 millones, han padecido acoso sexual específicamente a través de medios digitales (Ministerio de Igualdad, 2025).

Sin embargo, cuando se pregunta directamente si algún episodio de acoso sexual tuvo lugar mediante tecnologías digitales, con independencia de que también hubiera ocurrido en otros espacios, la cifra asciende: el 24,8% de las víctimas de acoso sexual, casi una de cada cuatro, responde que todos o algunos de los episodios sucedieron *online*. Esto representa el 9% de las mujeres españolas mayores de 16 años, es decir, aproximadamente 1,9 millones de mujeres (Ministerio de Igualdad, 2025).

El problema es especialmente grave entre las jóvenes (ver *Figura 1*). En el grupo de 16 a 24 años, el 44,6% de las víctimas de acoso sexual afirma que algunos o todos los episodios ocurrieron *online*; en las de 25 a 34 años, el 48,3%. En términos de prevalencia sobre el total de cada grupo de edad, el 25,3% de las mujeres de 16 a 24 años y el 24,8% de las de 25 a 34 años han sufrido acoso sexual *online*. A partir de los 45 años, estas cifras se desploman, solo el 5,2% en mujeres de 45 a 54 años (Ministerio de Igualdad, 2025).

**Figura 1**  
Acoso sexual online a mujeres por grupo de edad



Nota. Prevalencia del acoso sexual online en mujeres según la edad, destacando que es mucho más frecuente entre las más jóvenes (16–34 años). Tomado de Ministerio de Igualdad. (2025).

Macroencuesta de Violencia contra la Mujer 2024.  
Delegación del Gobierno contra la Violencia de Género.

Otro dato importante es la interacción *online* previa con el agresor. Entre las mujeres que han sufrido acoso sexual y declaran que algunos (pero no todos) los episodios ocurrieron *online*, el 59,4% afirma que esos episodios sucedieron tras haber conocido o interactuado previamente con el agresor a través de Internet. Incluso entre las que dijeron que ningún episodio había sido *online*, un 1,7% admite que el acoso se produjo después de una interacción digital previa (Ministerio de Igualdad, 2025).

Estos datos, si bien relevantes, pueden subestimar la magnitud real del problema, ya que investigaciones más recientes indican que el 82,6% de las mujeres ha experimentado al menos una forma de violencia *online* basada en el género en los últimos doce meses, siendo el acoso sexual digital la forma más frecuente (66,7%), seguido de la violencia basada en la apariencia física (60,7%) (Martínez-Bacaicoa et al., 2024). En esta misma línea, un estudio transversal con 1.177 mujeres españolas de entre 18 y 59 años encontró que el 68,2% había sufrido violencia de género a través de redes sociales, mientras que el 62,7% reportó haber experimentado violencia sexual *online* (López-Barranco et al., 2025).

La evidencia internacional más reciente sitúa la prevalencia global de esta violencia en el 30,6% de las mujeres adultas (Benítez-Hidalgo et al., 2025), si bien estas cifras varían significativamente en función de las definiciones empleadas y los instrumentos de medición utilizados. La encuesta de la Agencia de Derechos Fundamentales de la Unión Europea sobre violencia contra las mujeres revela que el acoso sexual sigue siendo una experiencia generalizada: entre 83 y 102 millones de mujeres (45%-55%) en los 28 Estados miembros han experimentado al menos una forma de acoso sexual desde los 15 años (Latcheva, 2017). Este tipo de violencia afecta desproporcionadamente a mujeres jóvenes y es más comúnmente percibido y experimentado por mujeres con título universitario y en los grupos ocupacionales más altos (Latcheva, 2017).

La dimensión temporal de este fenómeno resulta igualmente relevante. Durante el confinamiento por COVID-19, el acoso a través de canales electrónicos aumentó significativamente (32,6% durante el confinamiento frente a 16,5% antes y 17,8%

después) (Casanovas et al., 2022), evidenciando cómo la intensificación del uso de entornos digitales puede exacerbar los riesgos de victimización. Asimismo, investigaciones recientes señalan que el uso diario de redes sociales y el consumo de pornografía se asocian con mayores tasas de victimización (López-Barranco et al., 2025).

El presente artículo se propone abordar estas limitaciones mediante un análisis de las implicaciones psicosociales de las ciberviolencias sexuales contra la población femenina en España desde una perspectiva de género. Para ello, se examinarán críticamente las definiciones y tipologías existentes, se analizarán las tasas de prevalencia y los factores de riesgo y se explorarán las consecuencias en la salud mental y el bienestar psicosocial de las víctimas, así como el análisis de la función que cumplen la inteligencia artificial y la ciberseguridad en la perpetración de estas violencias. La adopción de un enfoque de género resulta fundamental para desvelar los mecanismos estructurales que sostienen estas violencias, así como para orientar el diseño de estrategias de prevención, detección e intervención que resulten efectivas, contextualmente pertinentes y sensibles a las desigualdades de género que atraviesan el espacio digital.

## 2. METODOLOGÍA

### 2.1. DISEÑO DEL ESTUDIO

La metodología empleada en este trabajo se fundamenta en una síntesis narrativa de la literatura científica reciente, adoptando una perspectiva de género que guía tanto la selección como el análisis de la evidencia. Este enfoque permite describir y sintetizar el impacto multifactorial de la ciberviolencia sexual, ya que permite integrar hallazgos de estudios con diversos diseños (cuantitativos, cualitativos y mixtos) y contextos, facilitando una comprensión holística del fenómeno desde una aproximación psicosocial.

### 2.2. ESTRATEGIA DE BÚSQUEDA

Para recopilar la evidencia, se realizó una búsqueda sistemática en bases de datos académicas y repositorios especializados, incluyendo PubMed, Scopus, ProQuest, Web of Science y PsycInfo. La búsqueda se llevó a cabo entre marzo de 2025 y febrero de 2026, abarcando publicaciones comprendidas principalmente entre 2015 y 2026, con el fin de recoger la evolución más reciente del fenómeno, si bien se consideraron trabajos fundacionales previos cuando resultaron esenciales para la definición conceptual.

La estrategia de búsqueda combinó términos en español e inglés utilizando operadores booleanos. Los descriptores empleados fueron: 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, junto con los términos referidos a la población (mujeres, women, femenino, adolescentes) y al contexto geográfico (España, Spain). Se utilizaron los operadores AND y OR para combinar los conceptos, y se aplicaron filtros de idioma (español e inglés) y tipo de documento.

Resultados de la búsqueda: Se identificaron 438 artículos. Tras eliminar duplicados, se cribaron 360 títulos y resúmenes, excluyendo 204 por no cumplir los criterios de inclusión. Se evaluaron 156 artículos a texto completo, de los cuales 48 cumplieron todos los criterios de inclusión.

### 2.3. CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Se establecieron los siguientes criterios para seleccionar las fuentes:

Criterios de inclusión:

- a. Artículos empíricos (cuantitativos, cualitativos o mixtos), revisiones sistemáticas, meta-análisis e informes institucionales publicados por organismos oficiales.
- b. Publicaciones en revistas científicas indexadas o procedentes de fuentes institucionales reconocidas.
- c. Estudios cuyo objeto de investigación abordara alguna forma de ciberviolencia sexual o violencia sexual facilitada por tecnología (TFSV).
- d. Muestras que incluyeran población femenina (niñas, adolescentes, adultas o ambas).
- e. Estudios realizados en España o, en su defecto, investigaciones internacionales que aportarán evidencia relevante sobre prevalencia, factores de riesgo o consecuencias psicosociales.
- f. Publicaciones en español o inglés.
- g. Período de publicación comprendido entre 2015 y 2026 (excepto referencias fundacionales previas imprescindibles para la definición conceptual).

Criterios de exclusión:

- a. Estudios centrados exclusivamente en poblaciones masculinas sin separación por sexo.
- b. Investigaciones que abordaran únicamente violencia *offline* sin referencia a medios digitales.
- c. Artículos de opinión, editoriales, cartas al director o publicaciones sin revisión por pares (excepto informes institucionales).
- d. Documentos cuyo texto completo no estuviera disponible en español o inglés.
- e. Estudios duplicados en las diferentes bases de datos.

### 2.4. EXTRACCIÓN Y SÍNTESIS DE DATOS

De cada fuente seleccionada se extrajo información sobre: autoría y año, diseño metodológico, características de la muestra, definiciones operativas de ciberviolencia sexual, principales resultados y limitaciones. La síntesis se realizó mediante un enfoque narrativo, agrupando los hallazgos en categorías temáticas: (a) prevalencia y magnitud del fenómeno; (b) factores de riesgo; (c) consecuencias en la salud mental y bienestar psicosocial; (d) definiciones y marcos conceptuales; (e) perspectiva de género y desigualdades estructurales; (f) estrategias de perpetración y prevención.

### 2.5. CALIDAD METODOLÓGICA Y VALIDEZ

La validez de las conclusiones se sustenta en la selección de investigaciones de alta calidad metodológica, evaluada mediante criterios explícitos: (a) procedencia de publicaciones con revisión por pares o de organismos oficiales reconocidos; (b) congruencia de los objetivos con la pregunta de investigación; (c) adecuación del diseño metodológico; (d) claridad en la definición de las variables; (e) representatividad de las

muestras en estudios cuantitativos; (f) rigor analítico en estudios cualitativos; y (g) concordancia de los resultados con el consenso científico internacional.

## 2.6. REPLICABILIDAD

Este enfoque es replicable mediante la aplicación de los mismos criterios de búsqueda y selección descritos, lo que permite a otros investigadores verificar o ampliar el análisis siguiendo el procedimiento detallado.

## 3. RESULTADOS Y DISCUSIÓN

### 3.1. DIMENSIONES DE LAS CIBERVIOLENCIAS Y TIPOLOGÍA

Las ciberviolencias sexuales constituyen una red heterogénea de conductas que, apoyadas en las tecnologías digitales, vulneran la integridad y la libertad sexual de las mujeres desde una lógica de género (Henry y Powell, 2018; Champion et al., 2022). Su análisis requiere superar la simple enumeración de formas de victimización para comprender cómo las desigualdades estructurales se trasladan y amplifican en el espacio digital. Para evitar solapamientos terminológicos, es preciso delimitar tres conceptos que a menudo se usan como sinónimos: violencia sexual facilitada por tecnología (TFSV) es el concepto paraguas que incluye todo comportamiento sexual no deseado mediado por tecnologías digitales (Henry y Powell, 2018); ciberviolencia sexual se refiere específicamente a las conductas que ocurren íntegramente en entornos digitales (Martínez-Bacaicoa, 2024); y violencia de género online enfatiza el componente estructural de desigualdad entre hombres y mujeres como causa subyacente (Mármol et al., 2025).

Una revisión sistemática y metaanálisis internacional identificó tres dimensiones principales de TFSV contra mujeres (Benítez-Hidalgo et al., 2025). La primera y más frecuente es el acoso sexual digital, con una prevalencia global estimada del 28,54%. Incluye comentarios sexuales inapropiados, insinuaciones no deseadas, atención sexual no solicitada y observaciones sexistas en plataformas online. En España, el 66,7% de las mujeres lo ha experimentado en los últimos doce meses (Martínez-Bacaicoa et al., 2024), y el envío no solicitado de imágenes explícitas ("dick pics") afecta al 48,1% de las mujeres de 18 a 30 años (Durán y Rodríguez-Domínguez, 2023). La segunda dimensión es la sextorsión (16,93% global), definida como la amenaza de compartir imágenes sexuales para coaccionar a la víctima a pagar, enviar más material o realizar actos no deseados. Ocurre en contextos diversos: violencia de pareja, ciberacoso, citas online, trata y crimen organizado (Ray y Henry, 2025). La tercera es el abuso sexual basado en imágenes (IBSA) o "porno de venganza" (6,48% global), que incluye la toma, distribución o amenaza de distribución no consensuada de imágenes íntimas. Los perpetradores suelen ser parejas actuales o anteriores, y en el 29% de los incidentes las víctimas reportan un impacto vital devastador (Colburn et al., 2025).

Una característica diferencial de estas violencias es la huella digital: la permanencia, reproducibilidad y potencial viralización del material en entornos digitales. A diferencia de las violencias offline, donde el daño puede circunscribirse a un momento y lugar, las digitales generan una continuidad de la victimización en el tiempo. Una vez que una imagen íntima es compartida sin consentimiento, la pérdida de control sobre su difusión es prácticamente irreversible, generando un estado de hiperalerta permanente (Lorca, 2024). Además, las tecnologías digitales operan como facilitadoras del

reclutamiento de víctimas para redes de trata con fines de explotación sexual, frecuentemente mediante promesas de empleo legítimo (Mayuri-Bocanegra y Aliaga-Pacora, 2023).

Un fenómeno emergente que ha suscitado debate es el blanqueamiento del negocio sexual a través de plataformas como OnlyFans o Fansly. Diversas organizaciones han alertado sobre lo que denominan "proxenetismo digital", que presenta la creación de contenido íntimo como una forma de empoderamiento cuando, en realidad, reproduce dinámicas de cosificación y desigualdad estructural (Fuentes y Berger, 2025; Medina-Bravo, 2021). Desde una perspectiva crítica, este artículo subraya que la normalización de ofrecer contenido íntimo como fuente de ingresos entre la población joven evidencia una preocupante falta de conciencia sobre la violencia y la desigualdad de género subyacente, sin desconocer la complejidad del fenómeno ni la diversidad de experiencias.

Desde una óptica criminológica, la aplicación de la teoría de las actividades rutinarias online ayuda a comprender la victimización: convergen un objetivo adecuado (mujeres jóvenes con presencia digital activa), una motivación del agresor (favorecida por la desinhibición digital y el anonimato) y la ausencia de un guardián capacitado (moderación insuficiente de plataformas, baja denuncia). La desinhibición digital (Suler) explica que los agresores expresan conductas que no manifestarían offline debido al anonimato y la asincronía. Además, los perpetradores de deepfakes utilizan técnicas de neutralización (negación del daño, negación de la víctima, condena de los condenadores) para minimizar su responsabilidad (Flynn et al., 2025). Estas dinámicas se inscriben en una cultura de la violación digital que normaliza la sexualización no consentida, y en una gobernanza algorítmica donde los sistemas de recomendación y los patrones de diseño oscuro (dark patterns) de las plataformas favorecen la viralización de contenido abusivo frente a la privacidad de las usuarias (Fagan, 2024).

En el plano jurídico, el ordenamiento europeo presenta insuficiencias significativas. El AI Act no regula explícitamente los deepfakes sexualizados como categoría de riesgo inaceptable, y el Digital Services Act enfrenta desafíos de detección y escala. La jurisprudencia del TEDH (Asuntos Buturugă v. Rumania, 2020, y Volodina v. Russia, 2019 y 2021) ha establecido que los Estados tienen obligaciones positivas de proteger a las mujeres de la violencia digital, sentando bases para futuras reformas legales.

En conjunto, estos hallazgos tienen implicaciones significativas para el diseño de políticas preventivas de salud. Se sugiere preguntar rutinariamente en los servicios de salud mental si las interacciones en línea causan daño (Iroegbu et al., 2024). Durante la pandemia de COVID-19, la violencia sexual disminuyó en espacios públicos pero aumentó en digitales, y el silencio en torno a las situaciones violentas se profundizó (Castellanos-Torres et al., 2023), lo que subraya la necesidad de desarrollar protocolos de acción y mejorar la accesibilidad de recursos en contextos de crisis.

### 3.2. CONSECUENCIAS Y FACTORES DE RIESGO EN LAS VÍCTIMAS

Las consecuencias de las ciberviolencias sexuales sobre la salud mental son graves y están documentadas. En España, las mujeres víctimas de esta forma de violencia reportaron tasas significativamente más altas de ideación suicida (20% frente al 9,79% de las no víctimas) y de intentos de suicidio (7,20% frente al 1,74%), según Benítez-Hidalgo et al.

(2024). A ello se suma que el acoso sexual digital predice de manera independiente ansiedad, depresión, trauma e insatisfacción con la imagen corporal (Iroegbu et al., 2024).

Este patrón no es exclusivo de España. La investigación internacional confirma que las víctimas de violencia sexual facilitada por tecnología experimentan ansiedad, estrés, depresión, pérdida de control, desconfianza, múltiples victimizaciones, disfunción académica o laboral, consumo problemático de alcohol, vergüenza y cambios en su comportamiento en línea (Champion et al., 2022). De hecho, quienes sufren abuso de imágenes en línea presentan índices más elevados de depresión, ansiedad y malfuncionamiento ocupacional o académico que las víctimas de otros tipos de violencia sexual facilitada por tecnología (Champion et al., 2022).

Profundizando en los mecanismos que explican estos efectos, un estudio reciente ha demostrado que las mujeres con una mayor aceptación de los mitos de la ciberviolencia sexual<sup>1</sup> y una mayor victimización reportan niveles más altos de ansiedad, depresión y vergüenza corporal, así como menor autoestima y apreciación corporal. Este efecto está mediado por la autoobjetificación, lo que indica que dichos mitos exacerban los impactos emocionales en quienes han experimentado con mayor frecuencia este tipo de violencia (Vizcaíno-Cuenca et al., 2025). Asimismo, las víctimas sufren síntomas de estrés postraumático y problemas de sueño, los cuales median la relación entre la victimización cibersexual y la angustia psicológica (Morgan et al., 2025).

Más allá de las consecuencias, es necesario conocer la magnitud del problema y los perfiles de mayor riesgo. Los factores de riesgo asociados a la ciberviolencia sexual en España incluyen, según la Macroencuesta de 2019, ser menor de 25 años, tener educación superior, no estar en una relación de pareja, no tener creencias religiosas y presentar una discapacidad certificada (Benítez-Hidalgo et al., 2024). Las mujeres que han experimentado otras formas de violencia de género también muestran mayor riesgo de sufrir ciberviolencia sexual (Benítez-Hidalgo et al., 2024). Esta vulnerabilidad diferenciada se manifiesta de manera especialmente intensa en las etapas juveniles: las mujeres menores de 18 años presentan tasas de victimización por grooming de 2,55 por cada 100.000 habitantes, frente a 0,95 en varones de la misma edad; mientras que en la adultez joven (18-25 años) las mujeres muestran tasas superiores en acoso sexual y abuso sexual. Las proyecciones a 2035 indican que estas brechas de género no sólo persistirán, sino que se ampliarán, particularmente entre las menores de 18 años y en el grupo de 26 a 40 años (Mármol et al., 2025).

Desde una perspectiva criminológica, la teoría de las actividades rutinarias online ayuda a comprender por qué se produce la victimización: convergen un objetivo adecuado (mujeres jóvenes con presencia digital activa), una motivación del agresor (favorecida por la desinhibición digital y el anonimato) y la ausencia de un guardián capacitado (moderación insuficiente de las plataformas y baja denuncia). La desinhibición digital explica que los agresores expresan conductas que no manifestarían en el mundo offline debido al anonimato, la invisibilidad y la asincronía. Además, los perpetradores de deepfakes utilizan técnicas de neutralización, como la negación del daño («es solo una

---

<sup>1</sup> Entre los cuales se encuentran la minimización o negación de la violencia, la culpabilización de la víctima, la culpabilización de las plataformas digitales y la exoneración del perpetrador (Vizcaíno-Cuenca et al., 2025)

foto»), la negación de la víctima («ella lo provocó») o la condena de los condenadores («todo el mundo lo hace»), para minimizar su responsabilidad (Flynn et al., 2025).

La importancia del contexto social y temporal se hizo especialmente evidente durante la pandemia. Un estudio de 2022 con 2.515 jóvenes españoles de entre 18 y 35 años encontró que las mujeres tenían casi el doble de probabilidad que los hombres de sufrir acoso sexual (49% frente al 22,2%) (Casanovas et al., 2022). Durante el confinamiento, el acoso a través de canales electrónicos aumentó (32,6%, frente al 16,5% y 17,8% antes y después del período), mientras que disminuyó en la vía pública (22,9%, frente al 63,4% y 54,4% antes y después). Estos datos evidencian que, durante el confinamiento, el acoso sexual se desplazó de los espacios públicos a las redes sociales (Casanovas et al., 2022).

Por último, ante este sufrimiento, las supervivientes despliegan diversas estrategias de afrontamiento y búsqueda de ayuda. Las más frecuentes son revelar lo sucedido a personas de confianza, emprender acciones legales y denunciar el contenido. En el extremo opuesto, las estrategias de evitación incluyen reubicarse, aislarse o intentar actuar como si nada hubiera pasado. Sin embargo, las víctimas se topan con importantes barreras para buscar ayuda: el estigma, la falta de conciencia sobre los recursos disponibles y las experiencias negativas previas con las autoridades dificultan que muchas mujeres accedan al apoyo que necesitan (Karasavva, 2025).

### 3.3. INTELIGENCIA ARTIFICIAL EN LA PERPETRACIÓN

La inteligencia artificial (IA) ha emergido como una herramienta que aumenta significativamente las capacidades de los perpetradores de ciberviolencias sexuales, representando una escalada profunda en el abuso sexual basado en imágenes (Williams, 2025). Desde 2017, la proliferación de tecnologías de código abierto ha facilitado como nunca antes la creación y difusión de *deepfakes*. Esto ha ido acompañado de un aumento paralelo de los casos de ciberabuso sexual, especialmente contra mujeres (Flynn et al., 2025). La inmensa mayoría de los *deepfakes* que circulan en línea son de naturaleza pornográfica, y las personas que aparecen en ellos rara vez han dado su consentimiento. Cualquier persona con presencia en internet puede convertirse en víctima (Karasavva y Noorbhai, 2021), siendo la población femenina la más vulnerable. Un estudio de 2025 que analizó 29 aplicaciones dedicadas a esta práctica concluyó que estas plataformas no solo facilitan, sino que fomentan activamente la creación de imágenes íntimas no consentidas (NCII). Con ello, normalizan la cosificación de las mujeres y contribuyen a una cultura donde su privacidad y autonomía quedan sistemáticamente socavadas (Williams, 2025).

Aún más preocupante es el comportamiento de los propios agresores. Una investigación cualitativa de 2025, realizada con diez perpetradores y quince víctimas de abuso mediante *deepfakes* sexualizados, reveló pautas muy graves: la facilidad de uso de estas herramientas, la normalización de la sexualización sin consentimiento y la constante minimización del daño causado a las víctimas. Todo ello, según los autores, puede afectar negativamente a cualquier esfuerzo de prevención y respuesta (Flynn et al., 2025). Los agresores justifican y restan importancia a lo que hacen, y aunque hay similitudes con otras formas de violencia sexual facilitada por tecnología, la gran diferencia es la accesibilidad y la facilidad con la que se puede generar un *deepfake* (Flynn et al., 2025).

Otra cara de este problema es la sextorsión, que aparece en contextos muy diversos: violencia de pareja, ciberacoso, aplicaciones de citas, tráfico sexual o crimen organizado (Ray y Henry, 2025). Mientras que la sextorsión tradicional solía depender de que la víctima compartiera voluntariamente sus propias imágenes íntimas, la IA ha eliminado esa barrera (Lazard et al., 2025). Herramientas de IA generativa, pueden crear desnudos falsos hiperrealistas a partir de cualquier foto de una red social, como una imagen de perfil. Esto permite a los perpetradores convertir a cualquier persona con presencia en internet, especialmente a mujeres, niñas y adolescentes, en una víctima potencial, chantajeándola con imágenes falsas que parecen reales (Lazard et al., 2025). La IA actúa como un acelerador: facilita la creación de imágenes falsas, la automatización de los chantajes y la personalización de las amenazas a gran escala. La denuncia y la búsqueda de ayuda siguen siendo muy bajas debido a la vergüenza, el miedo y las percepciones negativas de la policía y las plataformas digitales (Lazard et al., 2025; Ray y Henry, 2025).

En este contexto, la explotación y el abuso sexual infantil en línea (OCSEA) se consideran un problema urgente que está escalando, facilitado por el llamado "motor triple-A": accesibilidad, asequibilidad y anonimato (Fry et al., 2025). La inteligencia artificial potencia cada uno de estos tres ejes: hace más accesible la generación de material de abuso, reduce aún más los costes de producción y difusión y refuerza el anonimato de los agresores. Según el CyberTipline del Centro Nacional para Niños Desaparecidos y Explotados de Estados Unidos, se recibieron más de 36,2 millones de reportes de imágenes y vídeos sospechosos de OCSEA en 2023, lo que supone un aumento del 13% respecto a 2022 y del 23% respecto a 2021 (Fry et al., 2025). El desarrollo acelerado de las redes sociales y otros entornos virtuales permite que emerjan nuevas modalidades tecnológicas y tipos de abuso, lo que hace extremadamente difícil estimar la extensión completa de estos crímenes (Fry et al., 2025).

La dificultad para dimensionar estos delitos no impide que, paralelamente, exista una conversación activa sobre la pornografía generada por IA, un análisis de contenido cuantitativo de 390 publicaciones de Reddit relacionadas con esta temática reveló que las experiencias abordadas van desde la indignación y la preocupación por sus daños reales y potenciales hasta la curiosidad, el disfrute e incluso los beneficios económicos (Döring et al., 2025). La producción (59,5%) y el contenido (60,8%) de la pornografía con IA fueron los temas más discutidos, mientras que las implicaciones ético-legales solo aparecían en aproximadamente un tercio de las publicaciones (35,1%). Esto subraya la necesidad de una respuesta matizada por parte de legisladores, desarrolladores de tecnología, educadores y profesionales de salud mental (Döring et al., 2025). El uso de imágenes de personas en contextos pornográficos sin su consentimiento es una infracción cada vez más extendida, y las actividades ilegales realizadas con imágenes generadas por IA son una variante de este fenómeno que evidencia lo inadecuados que resultan los sistemas legales frente a una realidad cambiante (Mania, 2024).

La violencia en línea contra las mujeres es un problema global creciente, y los *deepfakes* aplicados a la violencia contra la población femenina han atraído considerable atención (Lazard et al., 2025). A medida que las ciencias sociales comienzan a estudiar las implicaciones de la creación y difusión de *deepfakes* en el contexto de la violencia sexual, resulta necesario investigar también cómo se utilizan estos *deepfakes* para silenciar a las mujeres en los espacios públicos digitales, es imprescindible reconocer empíricamente las discriminaciones sistémicas de género inherentes tanto a la tecnología

*deepfake* como a sus usos (Lazard et al., 2025). La investigación debe ir más allá de las técnicas de detección y de la credibilidad percibida y avanzar hacia un análisis de las dinámicas de poder interseccionales que operan en esta forma de violencia.

### 3.4. CIBERSEGURIDAD COMO HERRAMIENTA DE PREVENCIÓN

La ciberseguridad puede actuar como herramienta preventiva mediante estrategias tecnológicas, educativas y de diseño de plataformas, aunque la evidencia actual indica que las respuestas tecnológicas son necesarias pero no suficientes por sí mismas, requiriendo que sean complementadas con recursos humanos especializados y enfoques centrados en las supervivientes (Harkin y Merkel, 2023).

Una revisión sistemática de 2023 identificó 136 aplicaciones para la prevención de violencia doméstica, clasificadas en cinco categorías (Sumra et al., 2023):

**Tabla 1**  
*Categorías de las aplicaciones para la prevención de violencia doméstica*

<b>Categoría</b>	<b>%</b>	<b>Descripción y contexto de uso</b>
Asistencia de emergencia	44,9%	Generación de alertas de emergencia. No se limita a situaciones de evitación; también aborta contextos de violencia en curso, amenazas inminentes o cualquier situación de riesgo que requiera intervención inmediata (p. ej., agresión activa, acoso, peligro para la integridad física).
Evitación	21,3%	Geo-cercas, alertas basadas en acelerómetro, alertas basadas en sacudidas. Orientadas principalmente a prevenir el encuentro con el agresor o a detectar movimientos bruscos que puedan indicar una agresión en contexto de desplazamiento o acecho.
Informativas	21,3%	Proporcionan información sobre recursos de ayuda, derechos, casas de acogida, teléfonos de emergencia, etc.
Información legal	7,4%	Asesoramiento legal básico, pasos para denunciar, documentación necesaria.
Autoevaluación	5,1%	Asesoramiento legal básico, pasos para denunciar, documentación necesaria.

Nota. Adaptado de Sumra, M., Asghar, S., Khan, K. S., Fernández-Luna, J. M., Huete, J. F., y Bueno-Cavanillas, A. (2023).

Smartphone Apps for Domestic Violence Prevention: A Systematic Review.  
International Journal of Environmental Research and Public Health, 20(7), 5246.

A pesar de su utilidad, las aplicaciones de ciberseguridad presentan limitaciones importantes. Más de la mitad de las alertas de emergencia requieren activación manual por parte de la posible víctima, sin ningún tipo de automatización, y ninguna de las aplicaciones revisadas incorporaba inteligencia artificial para asistir a las personas en situación de riesgo. Las aplicaciones futuras deberían priorizar la automatización y hacer un mejor uso de la IA mediante recursos multimedia, reconocimiento de voz y detección

del tono, con el fin de contribuir al análisis de la situación en tiempo real (Sumra et al., 2023).

Por otro lado, integrar la seguridad en internet en programas ya consolidados y basados en evidencia –los que actualmente abordan daños relacionados como el acoso general, el abuso en las relaciones de pareja o la prevención del abuso sexual– ofrece ventajas significativas (Finkelhor et al., 2021). Estas ventajas derivan de cuatro factores: la considerable superposición entre los daños online y offline; la mayor prevalencia de los daños fuera de la red; los mismos factores de riesgo subyacentes; y la base empírica más sólida de los programas de mayor antigüedad, desarrollados originalmente para entornos fuera de línea (Finkelhor et al., 2021). Además, las intervenciones de prevención deberían enfocarse en modificar las oportunidades, facilidades e infraestructuras que permiten la perpetración, así como en abordar actitudes y normas sociales problemáticas (Henry y Beard, 2024). Esto implica que las plataformas tecnológicas asuman una responsabilidad activa en el diseño y regulación de sus servicios.

En este contexto, los denominados patrones de diseño oscuro (dark patterns), técnicas que manipulan a los usuarios para que tomen decisiones contrarias a su propio interés, resultan especialmente relevantes. Se categorizan bajo el acrónimo FORCES: Frame (enmarcar), Obstruct (obstruir), Ruse (engaño), Compel (compeler), Entangle (enredar) y Seduce (seducir). Dichas técnicas explotan principios psicológicos como el sesgo de negatividad, la brecha de curiosidad y la fluidez cognitiva para favorecer que el contenido social se vuelva viral (Fagan, 2024). Asimismo, las plataformas digitales incorporan elementos que pueden facilitar o exacerbar la ciberviolencia sexual (Fagan, 2024; Munzer et al., 2026

Asimismo, las plataformas digitales frecuentemente incorporan elementos que pueden facilitar o exacerbar la ciberviolencia sexual (Fagan, 2024; Munzer et al., 2026):

**Tabla 2**  
*Elementos que pueden facilitar o exacerbar la ciberviolencia sexual*

Recompensas frecuentes por juego	Sistemas de notificaciones y "me gusta" que generan comportamientos compulsivos y aumentan el tiempo de exposición a contenido potencialmente abusivo
Distracciones incrustadas	Anuncios o elementos interactivos excesivos que dificultan la navegación segura y la configuración de privacidad
Algoritmos de viralización	Sistemas que priorizan contenido sensacionalista o provocativo, potencialmente amplificando la difusión de contenido abusivo
Configuraciones de privacidad predeterminadas	Ajustes que favorecen la visibilidad pública sobre la privacidad del usuario

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

Con el avance de tecnologías como los algoritmos predictivos, la inteligencia artificial generativa y la realidad virtual, estas técnicas serán cada vez más poderosas (Fagan, 2024). Por ello es clave que las plataformas apuesten por un diseño ético que ponga la seguridad de los usuarios en primer lugar, especialmente cuando se trata de grupos vulnerables como las mujeres o las minorías sexuales (Ray y Henry, 2025).

Sin embargo, el marco normativo europeo y español presenta insuficiencias significativas para abordar las nuevas formas de ciberviolencia sexual. El Reglamento Europeo de Inteligencia Artificial (AI Act) clasifica los sistemas de IA según su nivel de riesgo, pero los deepfakes sexualizados no están explícitamente regulados en sus categorías de riesgo inaceptable. El Digital Services Act (DSA) impone obligaciones de moderación de contenidos a las plataformas, pero su aplicación efectiva a la pornografía deepfake no consentida enfrenta desafíos de detección y escala. En España, la Ley Orgánica 10/2022 de garantía integral de la libertad sexual ("ley del solo sí es sí") incorpora algunas formas de violencia digital, pero la regulación de los deepfakes no consentidos sigue siendo insuficiente (Mania, 2024).

La jurisprudencia del Tribunal Europeo de Derechos Humanos ha establecido obligaciones positivas de los Estados en materia de violencia digital. En *Buturugă v. Romania* (2020), el TEDH condenó a Rumania por no proteger a una mujer acosada online, considerando que el artículo 8 (derecho a la vida privada) y el artículo 3 (prohibición de tratos inhumanos o degradantes) imponen a los Estados el deber de adoptar medidas razonables para prevenir la violencia digital. En *Volodina v. Russia* (2019 y 2021), el Tribunal subrayó que la inacción estatal frente al ciberacoso reiterado constituye una violación de los derechos humanos. Estas sentencias son especialmente relevantes para los casos de sextorsión y difusión no consentida de imágenes íntimas. Complementariamente, el Comité CEDAW ha emitido recomendaciones específicas sobre violencia de género digital (Recomendación General N° 35), instando a los Estados a tipificar como delito las formas de violencia contra la mujer facilitadas por tecnología. El Instituto Europeo de Igualdad de Género (EIGE) y Europol han publicado informes recientes alertando sobre el aumento de deepfakes sexualizados y la necesidad de armonización legislativa, y ONU Mujeres ha desarrollado directrices para la prevención de la violencia online contra las mujeres.

A pesar de este marco, las víctimas rara vez denuncian. Según Colburn et al. (2023), solo el 7,3% de los incidentes de violencia online se reportan en los sitios web, y de ese porcentaje la mayoría quedan insatisfechos: menos de la mitad (42,2%) siente que el sitio hizo algo útil, y solo el 29,8% valora como útil la respuesta de la policía, cuando se llegó a denunciar. El riesgo de que la tecnología termine facilitando el abuso es real, por lo que, como señalan Shirzad et al. (2025), es fundamental asegurarse de que su uso en contextos de violencia sexual sea seguro y ético.

#### **4. LIMITACIONES Y LÍNEAS FUTURAS**

A pesar de la rigurosidad en la búsqueda y el análisis, este estudio presenta una serie de limitaciones que deben tenerse en cuenta a la hora de interpretar sus conclusiones.

En primer lugar, se trata de una revisión narrativa y no de una revisión sistemática con metaanálisis. Aunque el enfoque narrativo permite integrar hallazgos de diseños muy

diversos y ofrece una visión amplia del fenómeno, carece del nivel de estandarización y reproducibilidad que garantizaría un metaanálisis.

En segundo lugar, la mayoría de los estudios incluidos en la revisión son de corte transversal, lo que impide establecer relaciones causales sólidas entre victimización y consecuencias en salud mental. No se puede determinar con certeza si la ansiedad y la depresión son consecuencias de la ciberviolencia o si, por el contrario, ciertos perfiles de vulnerabilidad previa aumentan el riesgo de sufrirla. Tampoco se dispone de estudios longitudinales españoles que permitan analizar la evolución temporal de la victimización.

En tercer lugar, se ha prestado una atención desigual a las distintas formas de ciberviolencia sexual. El grueso de la evidencia se centra en el acoso sexual digital (comentarios, insinuaciones, envío de imágenes no solicitadas), mientras que fenómenos como la sextorsión, el abuso basado en imágenes o el grooming aparecen con menor frecuencia en los estudios nacionales. Esto puede deberse tanto a la menor visibilidad de estas violencias como a la ausencia de instrumentos específicos validados en población española para todos los tipos.

En cuarto lugar, el estudio no ha podido abordar de manera sistemática las experiencias de mujeres con identidades interseccionales (mujeres migrantes, mujeres con discapacidad, mujeres gitanas, mujeres LGTBIQ+). Aunque se menciona en algún momento que la discapacidad o la edad son factores de riesgo, no se dispone de suficiente evidencia desglosada que permita analizar cómo interactúan diferentes ejes de desigualdad en la victimización y sus consecuencias.

En quinto lugar, el trabajo se enfrenta a las limitaciones propias de las fuentes secundarias: los datos de prevalencia dependen de lo que las víctimas están dispuestas a reportar, y se sabe que las tasas de denuncia y revelación son muy bajas (apenas el 7,3% en plataformas (Colburn et al., 2023), y el 9,2% en violencia sexual por no pareja (Pastor-Moreno et al., 2022)). Esto implica que las cifras ofrecidas probablemente infraestiman la magnitud real del problema, especialmente en formas de violencia más estigmatizadas o menos reconocidas socialmente como tales.

Finalmente, en cuanto al análisis de la inteligencia artificial y la ciberseguridad, la revisión se ha basado en una literatura que avanza muy rápidamente. Dado que la fecha de corte de la búsqueda fue febrero de 2026, es posible que no se hayan incluido algunos estudios o informes publicados después de esa fecha, especialmente aquellos que evalúan la efectividad de las medidas de prevención más recientes.

A partir de estas limitaciones, se sugieren las siguientes líneas de investigación futura. Sería necesario investigar todo lo que estas limitaciones señalan, haciendo especial énfasis en tres aspectos. Por un lado, estudiar con mayor profundidad las poblaciones interseccionales y las formas de violencia menos visibilizadas. Por otro lado, investigar la efectividad de las respuestas actuales, incluyendo la formación en ciberseguridad con perspectiva de género, el desarrollo de protocolos específicos y la integración de las tecnologías digitales en la educación sexual. Finalmente, dada la rápida evolución de la IA y la ciberseguridad, se recomienda actualizar periódicamente la evidencia y diseñar estudios longitudinales que permitan evaluar el impacto real de las intervenciones y la efectividad de las reformas legales. En conjunto, se necesitan respuestas integrales que

combinen estrategias tecnológicas, reformas legales y programas educativos obligatorios con enfoque de género para abordar eficazmente las ciberviolencias sexuales en España.

## 5. CONCLUSIONES

Los hallazgos de esta revisión confirman que las ciberviolencias sexuales constituyen un fenómeno generalizado en España, con una afectación desproporcionada sobre las mujeres jóvenes: el 25,3% de las mujeres de 16 a 24 años ha sufrido acoso sexual online. La elevada prevalencia, especialmente en el grupo de 16 a 34 años, indica que el acoso sexual digital no es una experiencia excepcional, sino una norma dentro de las interacciones cotidianas de las mujeres en entornos digitales. Este patrón por grupos de edad coincide con estudios internacionales (Latcheva, 2017) y sugiere que la socialización digital temprana y la presión por mantener una presencia activa en redes sociales actúan como factores de vulnerabilidad específicos. Las consecuencias psicológicas documentadas –ideación suicida, ansiedad, depresión, trauma, estrés postraumático, problemas de sueño, baja autoestima y autoobjetificación– son graves y consistentes con la literatura internacional (Champion et al., 2022; Iroegbu et al., 2024).

El hallazgo más relevante desde una perspectiva teórica es el papel exacerbador de los mitos sobre la ciberviolencia sexual. Las mujeres que internalizan estas creencias presentan un peor estado de salud mental tras la victimización, y este efecto está mediado por la autoobjetificación (Vizcaíno-Cuenca et al., 2025). Este mecanismo, que no había sido explorado previamente en el contexto español, aporta evidencia empírica a la teoría de la objetificación aplicada al entorno digital y sugiere que la cultura de la violación digital no solo justifica la violencia, sino que amplifica activamente el daño psicológico.

En cuanto a la inteligencia artificial, los resultados indican que la IA está transformando cualitativamente la perpetración. La facilidad de creación de deepfakes y la automatización de la sextorsión eliminan barreras que antes limitaban este tipo de abuso (Williams, 2025; Lazard et al., 2025). A diferencia de formas más tradicionales de TFSV, donde la víctima solía tener algún grado de interacción previa o compartir voluntariamente sus imágenes, la IA permite convertir a cualquier mujer con presencia online en víctima potencial, desbordando los marcos legales y de prevención actuales (Mania, 2024). La novedad que aporta esta revisión es la constatación de que el debate público en foros como Reddit sigue priorizando la producción y el contenido sobre las implicaciones ético-legales (Döring et al., 2025), lo que indica una normalización preocupante.

En el ámbito de la ciberseguridad, los resultados confirman que las aplicaciones existentes son insuficientes. La falta de automatización y la ausencia de inteligencia artificial en las herramientas actuales (Sumra et al., 2023) contrastan con la sofisticación de los métodos de perpetración. Las tasas de denuncia no superan el 7,3% y la insatisfacción con las respuestas institucionales es mayoritaria (Colburn et al., 2023), lo que apunta a una desconfianza estructural que no puede resolverse solo con mejoras tecnológicas, sino que requiere cambios en los protocolos de atención y en la formación de los profesionales.

Comparando estos hallazgos con estudios previos, se observa una continuidad con lo documentado para la violencia sexual offline en cuanto a factores de riesgo y consecuencias psicológicas. Sin embargo, la especificidad digital introduce elementos

novedosos, la permanencia de la huella digital, la viralización instantánea y la facilidad de anonimato para los agresores, que explican por qué las estrategias de prevención offline no son directamente trasladables al entorno online.

La principal contribución de este artículo es ofrecer una síntesis actualizada de la evidencia disponible en España que integra, por primera vez, la perspectiva de género, el análisis de los mitos sobre ciberviolencia, el papel de la inteligencia artificial como herramienta de perpetración, las aproximaciones criminológicas (teoría de las actividades rutinarias online, desinhibición digital, técnicas de neutralización) y el análisis jurídico-penal (jurisprudencia del TEDH, AI Act, DSA, recomendaciones del CEDAW, EIGE y ONU Mujeres) en un marco único. Frente a la literatura previa, que tiende a tratar estas violencias de forma segmentada, esta revisión muestra su interconexión y cómo las desigualdades estructurales de género se trasladan y amplifican en el espacio digital.

Este artículo ha dado respuesta a los objetivos planteados en la introducción. Los resultados confirman la alta magnitud de las ciberviolencias sexuales en España, especialmente entre mujeres jóvenes; sus graves consecuencias en salud mental; el papel agravante de los mitos sobre la ciberviolencia a través de la autoobjetificación; el efecto acelerador de la inteligencia artificial en la perpetuación; y las carencias de la ciberseguridad actual, que se traducen en tasas de denuncia muy bajas.

Como recomendaciones prácticas, se sugiere: (a) incorporar preguntas sobre ciberviolencia sexual en los protocolos de salud mental; (b) diseñar programas educativos obligatorios que aborden los mitos sobre la ciberviolencia y promuevan una sexualidad digital con enfoque de género; (c) exigir a las plataformas digitales un diseño ético que elimine los patrones oscuros y priorice la privacidad de las mujeres; (d) formar a profesionales de la ciberseguridad y de las fuerzas de seguridad en perspectiva de género y atención centrada en las supervivientes; y (e) armonizar legislativamente la regulación de los deepfakes sexualizados no consentidos en línea con las recomendaciones del TEDH, CEDAW, EIGE y ONU Mujeres.

## 6. REFERENCIAS BIBLIOGRÁFICAS

- Benítez-Hidalgo, V., Henares-Montiel, J., Ruiz-Pérez, I., y Pastor-Moreno, G. (2024). Cyber sexual harassment against women and 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., y Pastor-Moreno, G. (2025). International Prevalence of Technology-Facilitated Sexual Violence Against Women: A Systematic Review and Meta-Analysis of Observational Studies. *Trauma, Violence y 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., y 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., y CIBER Program of Violence and Young People team. (2023). COVID-19 and sexual violence against women: A qualitative study about young people and professionals' perspectives in Spain. *PloS One*, 18(8), e0289402. <https://doi.org/10.1371/journal.pone.0289402>
- Champion, A. R., Oswald, F., Khera, D., y Pedersen, C. L. (2022). Examining the Gendered Impacts of Technology-Facilitated Sexual Violence: A Mixed Methods Approach. *Archives of Sexual Behavior*, 51(3), 1607-1624. <https://doi.org/10.1007/s10508-021-02226-y>
- Colburn, D. A., Finkelhor, D., y Turner, H. A. (2023). Help-Seeking From Websites and Police in the Aftermath of Technology-Facilitated Victimization. *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., y O'Brien, J. E. (2025). Life impact following childhood Image-Based Sexual Abuse victimization among a sample of young adults. *Child Abuse y Neglect*, 167, 107584. <https://doi.org/10.1016/j.chiabu.2025.107584>
- Comité para la Eliminación de la Discriminación contra la Mujer. (2017, 26 de julio). Recomendación general núm. 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19 (CEDAW/C/GC/35). ACNUR. <https://www.acnur.org/fileadmin/Documentos/BDL/2017/11405.pdf>
- Cunha-Oliveira, A., Camarneiro, A. P., Gómez-Cantarino, S., Cipriano-Crespo, C., Queirós, P. J. P., Cardoso, D., Santos, D. G., y Ugarte-Gurrutxaga, M. I. (2021). The Integration of 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., y Miller, D. J. (2025). Experiences with AI-Generated Pornography: A Quantitative Content Analysis of Reddit Posts. *Archives of Sexual Behavior*. <https://doi.org/10.1007/s10508-025-03227-x>
- Durán, M., y Rodríguez-Domínguez, C. (2023). Sending of Unwanted Dick Pics as a Modality 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., y Collier, A. (2021). Youth Internet Safety Education: Aligning Programs With the Evidence Base. *Trauma, Violence y Abuse*, 22(5), 1233-1247. <https://doi.org/10.1177/1524838020916257>
- Flynn, A., Powell, A., Eaton, A., y Scott, A. J. (2025). Sexualized Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualized Deepfake Imagery. *Journal of Interpersonal Violence*, 8862605251368834. <https://doi.org/10.1177/08862605251368834>
- Fry, D., Krzeczowska, A., Ren, J., Lu, M., Fang, X., y 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 y Adolescent Health*, 9(3), 184-193. [https://doi.org/10.1016/S2352-4642\(24\)00329-8](https://doi.org/10.1016/S2352-4642(24)00329-8)
- Fuentes, P. A., y Berger, T. C. (2025). Pornografía y sexualidad en OnlyFans: El rol de la subjetivación femenina. *Persona y Sociedad*, 39(1), 11-25. <https://doi.org/10.53689/pys.v39i1.467>
- García Mingo, E., Lorca, J. G., y Ruíz Repullo, C. (2025). “La tecnología al servicio de la igualdad”: Agenda de investigación sobre violencia sexual digital en España. <https://doi.org/10.5565/rev/athenea.3687>
- García-Vázquez, J., Ruiz-Azcona, L., Pellico-López, A., y Paz-Zulueta, M. (2024). Characteristics of emotional and sexuality education programs in the Spanish school population. *Heliyon*, 10(20), e39368. <https://doi.org/10.1016/j.heliyon.2024.e39368>
- Harkin, D., y 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., y 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., y Beard, G. (2024). Image-Based Sexual Abuse Perpetration: A Scoping Review. *Trauma, Violence y Abuse*, 25(5), 3981-3998. <https://doi.org/10.1177/15248380241266137>

- Henry, N., Flynn, A., y 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., y 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., y Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence y Abuse*, 19(2), 195-208. <https://doi.org/10.1177/1524838016650189>
- Iroegbu, M., O'Brien, F., Muñoz, L. C., y 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 Nonconsensual Intimate Image Dissemination Victimization: A Scoping Review. *Trauma, Violence y Abuse*, 15248380251383940. <https://doi.org/10.1177/15248380251383940>
- Karasavva, V., y Noorbhai, A. (2021). The Real Threat of Deepfake Pornography: A Review of Canadian Policy. *Cyberpsychology, Behavior 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., y Stavropoulou, N. (2025). Deepfake Technology and Gender-Based Violence: A Scoping Review. *Trauma, Violence y 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). La reparación del daño en mujeres afectadas por prácticas de abuso sexual basado en imágenes en España. *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 y Abuse*, 25(1), 117-129. <https://doi.org/10.1177/15248380221143772>

- Mármol, C. J., Luna, A., y Legaz, I. (2025). Disproportionate Cybersexual Victimization of Women from Adolescence into Midlife in Spain: Implications for Targeted Protection and Prevention. *Behavioral 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 victimization (p. 1). <https://dialnet.unirioja.es/servlet/tesis?codigo=362106>
- Martínez-Bacaicoa, J., Henry, N., Mateos-Pérez, E., y Gámez-Guadix, M. (2024). Online Gendered Violence Victimization 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., y 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., y Aliaga-Pacora, A. A. (2023). La regulación de la trata de personas para fines de explotación laboral y la captación de víctimas mediante redes sociales de Lima. *Ciencia Latina Revista Científica Multidisciplinar*, 7(3), 452-471. [https://doi.org/10.37811/cl\\_rcm.v7i3.6206](https://doi.org/10.37811/cl_rcm.v7i3.6206)
- Medina-Bravo, P. (2021). Empoderamiento femenino: La trampa de un feminismo domesticado. *Discurso y Sociedad*, 15(3), 588-600. <https://doi.org/10.14198/dissoc.15.3.4>
- Ministerio de Igualdad. (2025). Macroencuesta de Violencia contra la Mujer 2024. Delegación del Gobierno contra la Violencia de Género. <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., y López, C. (2025). Sleep-Related Concerns Mediate the Association Between Cyber-Sexual Victimization and Psychological Distress Among Diverse University Students. *Cyberpsychology, Behavior 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., y 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>

- ONU Mujeres. (2024). *Violencia contra las mujeres y las niñas facilitada por la tecnología: una amenaza en rápida evolución*. En *Intensificación de los esfuerzos para eliminar todas las formas de violencia contra las mujeres y las niñas: Informe del Secretario General (A/79/500)*. ONU Mujeres. <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., y 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>
- Parlamento Europeo y Consejo de la Unión Europea. (2024, 13 de junio). *Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial)*. *Diario Oficial de la Unión Europea*, L 2024/1689. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689>
- Parlamento Europeo y Consejo de la Unión Europea. (2022, 19 de octubre). *Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)*. *Diario Oficial de la Unión Europea*, L 277, 1–102. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R2065>
- Ray, A., y Henry, N. (2025). Sextortion: A Scoping Review. *Trauma, Violence y Abuse*, 26(1), 138-155. <https://doi.org/10.1177/15248380241277271>
- Rodríguez-Castro, Y., Martínez-Román, R., Alonso-Ruido, P., Adá-Lameiras, A., y 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., y 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., y 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., y 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>

Tribunal Europeo de Derechos Humanos. (2020, 11 de febrero). Buturugă c. Rumanía (Demanda núm. 56867/15). <https://hudoc.echr.coe.int/eng?i=001-201342>

Tribunal Europeo de Derechos Humanos. (2019). Volodina c. Rusia, Demanda núm. 41261/17, sentencia de 9 de julio de 2019. Consejo de Europa. <https://www.cepc.gob.es/sites/default/files/2021-12/sentencia-volodina-v-rusia.pdf>

Vizcaíno-Cuenca, R., Carretero-Dios, H., y 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 in Women That 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 Normalization of Nonconsensual Intimate Deepfakes. *Violence Against Women*, 10778012251397966. <https://doi.org/10.1177/10778012251397966>