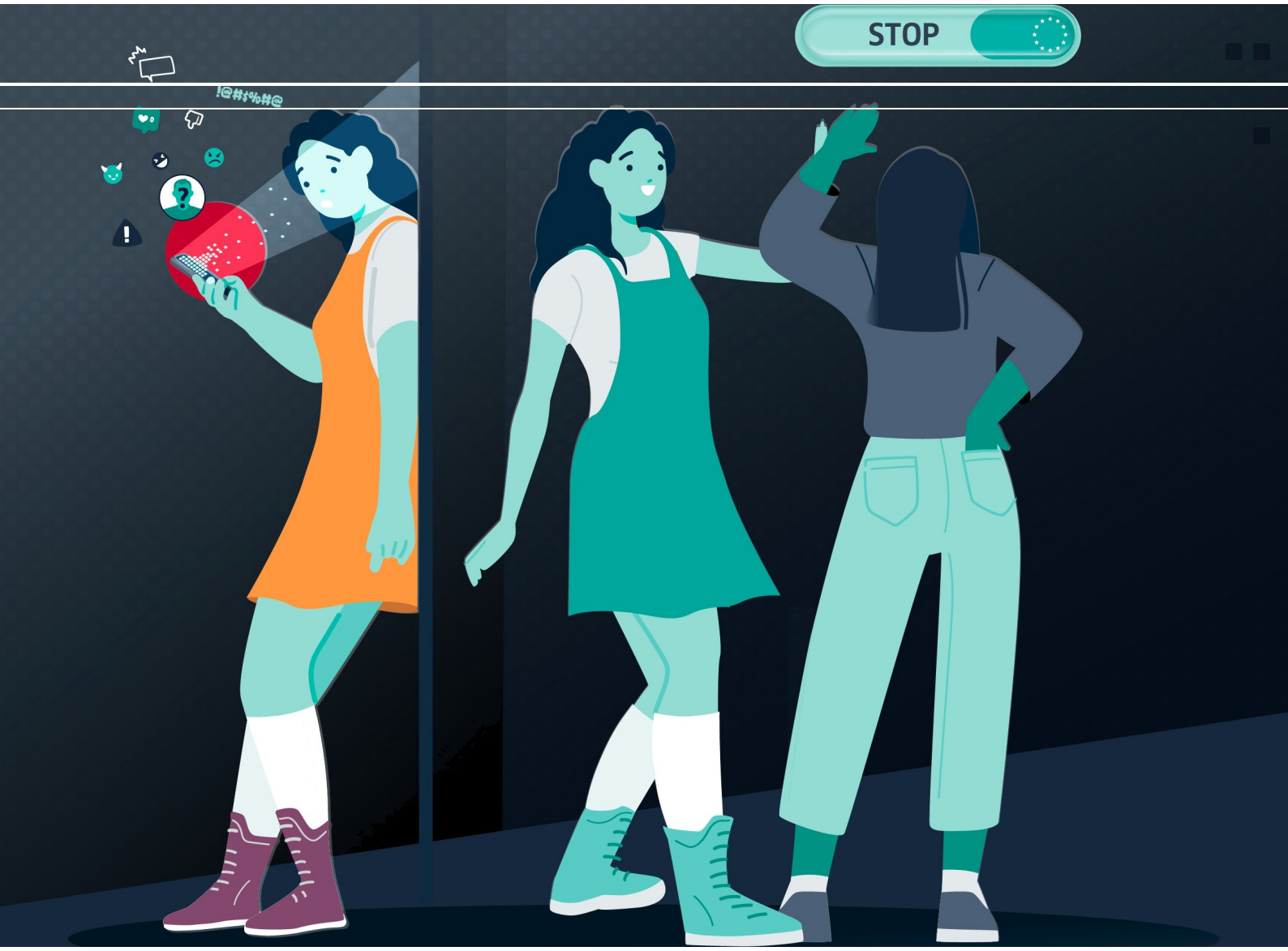
Instituto Europeo para la Igualdad de Género

DE LA REALIDAD VIVIDA A LA ACCIÓN POLÍTICA:

Combating cyber violence against girls in the EU ...



Una Agencia

European Institute for Gender Equality

Instituto Europeo para la Igualdad de Género

El Instituto Europeo de la Igualdad de Género (EIGE) lleva a cabo investigaciones independientes y difunde las mejores prácticas para promover la igualdad de género y eliminar la discriminación por motivos de género. Como agencia de la UE para la igualdad de género, ayudamos a las personas a alcanzar la igualdad de oportunidades para que todos puedan prosperar, independientemente de su género y origen.

Combinamos investigación, datos y herramientas para ayudar a los responsables políticos a diseñar medidas que sean inclusivas y transformadoras y que promuevan la igualdad de género en todos los ámbitos de la vida. Comunicamos nuestros conocimientos y nuestra investigación de forma eficaz.
Colaboramos estrechamente con nuestros socios para sensibilizar a la sociedad. Lo hacemos tanto a nivel de la UE como a nivel nacional, así como con los países candidatos y los posibles candidatos a la adhesión a la UE.

Citar esta publicación:

EIGE, *De la realidad vivida a la acción política: Lucha contra la ciberviolencia contra las niñas en la UE*, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2026.

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2026

PDF ISBN 978-92-9486-350-8 doi:10.2839/5514733 MH-01-26-045-EN-N

Instituto Europeo para la Igualdad de Género
Gedimino pr. 16
LT-01103 Vilna,
LITUANIA

Tel. +370 52157400
Internet: https://eige.europa.eu
Correo electrónico:
eige.sec@eige.europa.eu

Síguenos

Índice

Lista de figuras

Lista de tablas

Lista de cajas

Colaboradores

Este informe se basa en un estudio sobre la ciberviolencia que afecta a las niñas, encargado por el Instituto Europeo para la Igualdad de Género y realizado por el Istituto per la Ricerca Sociale (IRS) en colaboración con el Instituto Mediterráneo de Estudios de Género (MIGS). Los colaboradores del IRS fueron la Prof. Dra. Flavia Pesce, Elena Ferrari, Nicola Orlando, Maria Juliana Charry Camargo y Francesco Sanguineti, y los del MIGS fueron Susana Pavlou, Christina Kaili, Stalo Lesta y Maria Angeli. Las siguientes investigadoras nacionales supervisaron los grupos de discusión: la Prof. Dra. Fabienne Glowacz, Maria Angeli, la Dra. Anu Laas, Bianca Grafe, la Dra. Elaine Byrnes, la Dra. Lucia Beltramini, Agata Teutsch, Camelia Florina Proca, Virginia Gil Portolés y la Dra. Runa Baianstovu.

También contribuyeron expertos de la Unidad de Igualdad de Género de la Dirección General de Justicia y Consumidores. La Dra. Leonie Tanczer, profesora asociada de Seguridad Internacional y Tecnologías Emergentes en el University College London, aportó comentarios a un borrador inicial. Se agradece sinceramente a los participantes en la reunión de consulta del EIGE, celebrada de forma virtual el 12 de noviembre de 2025, por sus comentarios sobre el borrador de recomendaciones políticas. Entre los participantes se encontraban Elizabeth Ávila González, la profesora Kim Barker, Stephanie Futter-Orel, Inès Girard, la profesora Olga Jurasz, Zuzanna Kowalska, Marlene Matos, la Dra. Janine Mc Ginn, Eva O'Byrne, Adèle Philtjens, Lisa Robinson, Silvia Semenzin, Sara Sighinolfi, Sylwia Spurek y la Dra. Leonie Tanczer. También se recibieron comentarios sobre el borrador de las recomendaciones políticas por parte de Thomas Yaqoubi y

Abreviaturas

IA	inteligencia artificial
DSA	Ley de Servicios Digitales
EIGE	Instituto Europeo para la Igualdad de Género
UE-Violencia de género	Violencia de género en la UE (encuesta)
FRA	Agencia de los Derechos Fundamentales de la Unión Europea
RGPD	Reglamento General de Protección de Datos
GREVIO	Grupo de Expertos sobre la Lucha contra la Violencia contra las Mujeres y la Violencia Doméstica
HBSC	Comportamientos de salud en niños en edad escolar (encuesta)
TIC	tecnologías de la información y la comunicación
LGBTIQ+	lesbianas, gais, bisexuales, transgénero, intersexuales y queer
ONG	organización no gubernamental
OMS	Organización Mundial de la Salud

o ejecutivo

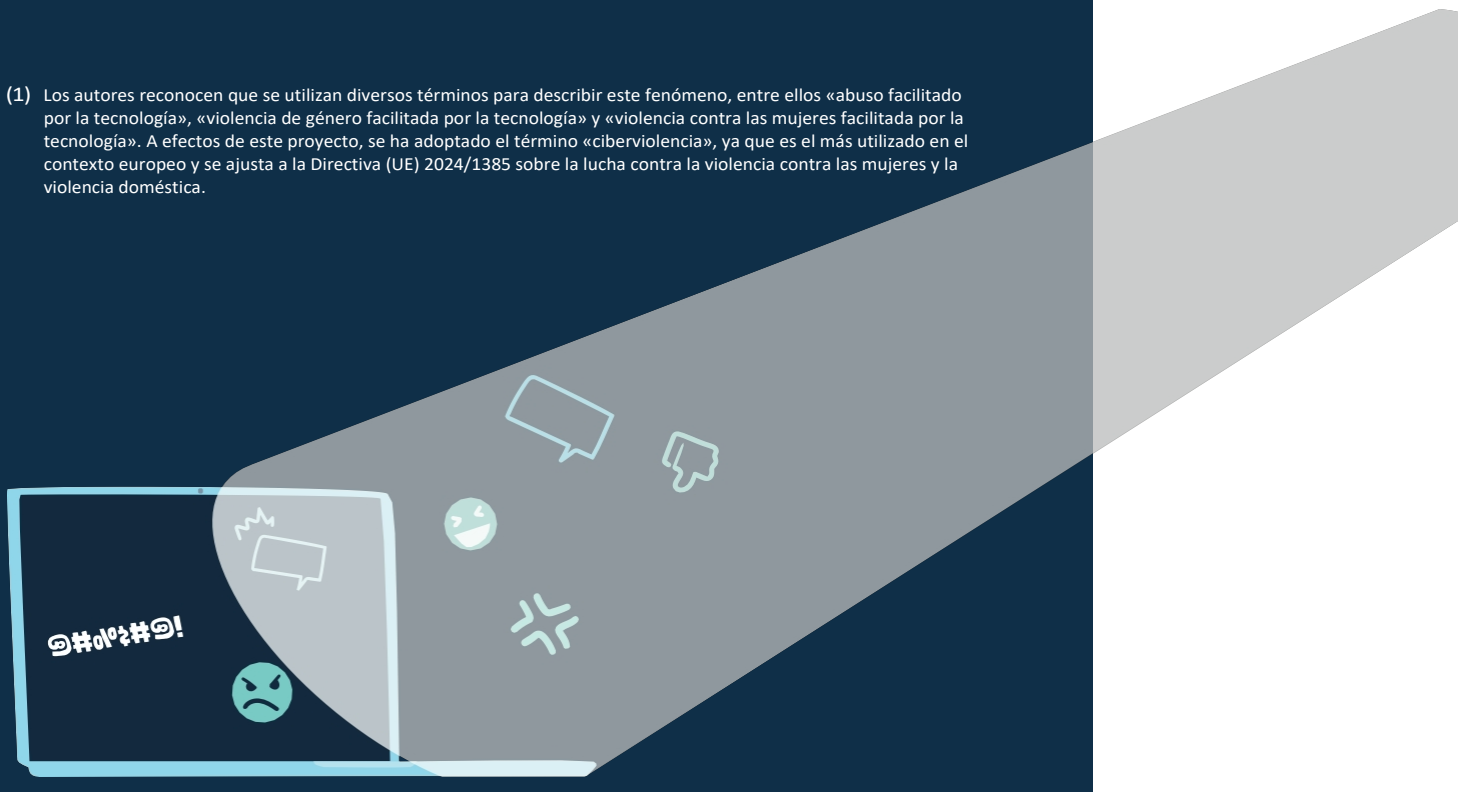
Este informe examina la ciberviolencia que afecta a las niñas y las adolescentes ([1]) en la Unión Europea, analizando su prevalencia, los factores subyacentes y consecuencias, y revisa la eficacia de las respuestas políticas y jurídicas existentes. Se basa en un diseño de investigación de métodos mixtos que combina el análisis jurídico y político, los datos estadísticos y las aportaciones participativas de adolescentes de diez Estados miembros de la UE, lo que proporciona una comprensión exhaustiva tanto de las dimensiones estructurales como de las vividas de la ciberviolencia y respalda la adopción de medidas políticas basadas en datos empíricos a nivel de la UE y nacional.

El estudio se concibió como un puente entre la investigación y la política, garantizando que los resultados empíricos sirvan de base directa para las medidas de la UE y nacionales destinadas a prevenir y responder a la ciberviolencia de género.

El estudio explora cómo las chicas de entre 13 y 18 años definen, experimentan y responden a la ciberviolencia, tanto como víctimas como como testigos, y tiene en cuenta los contextos sociales e institucionales más amplios en los que tienen lugar estas experiencias. El análisis de las experiencias de los chicos (de 15 a 18 años) se centra en las normas sociales, la masculinidad, el comportamiento de los testigos y la empatía. Se presta especial atención a las formas en que las normas de género, las expectativas sociales y los patrones de interacción digital configuran las percepciones y los comportamientos de los jóvenes en línea.

La investigación se enmarca en la Plataforma de Acción de Pekín, centrándose en el Área D sobre la violencia contra las mujeres y el Área L sobre las niñas, y respalda los esfuerzos de la UE para prevenir y combatir la violencia de género en todas sus formas.

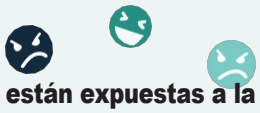
(1) Los autores reconocen que se utilizan diversos términos para describir este fenómeno, entre ellos «abuso facilitado por la tecnología», «violencia de género facilitada por la tecnología» y «violencia contra las mujeres facilitada por la tecnología». A efectos de este proyecto, se ha adoptado el término «ciberviolencia», ya que es el más utilizado en el contexto europeo y se ajusta a la Directiva (UE) 2024/1385 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica.



Conclusiones principales

La ciberviolencia contra las mujeres y las niñas se reconoce cada vez más como una parte integral de la vida cotidiana de las niñas

- Para muchas niñas, la ciberviolencia no es una amenaza ocasional, sino una característica persistente de su vida cotidiana, que condiciona su forma de comunicarse y de interactuar en línea. Las niñas describen una exposición constante a comportamientos nocivos que hacen que los espacios digitales les resulten impredecibles e inseguros.
- La ciberviolencia forma parte de la vida digital cotidiana, con mensajes dañinos, insultos, rumores y atención no deseada que aparecen a diario, o incluso cada hora, en todas las plataformas. Los jóvenes experimentan su extensión del ámbito en línea al físico, ya que el acoso y la exclusión suelen continuar en los centros educativos o en los grupos de iguales.
- Las chicas son blanco de estos ataques con mayor frecuencia que los chicos, sobre todo en lo que respecta al acoso sexual, el abuso basado en imágenes y los ataques a la reputación. La exposición repetida a estos comportamientos contribuye a crear la sensación de que la ciberviolencia es inevitable y difícil de eludir, ya que las chicas llegan a verla como parte del entorno en línea por el que deben moverse.
- Los debates en los grupos focales pusieron de relieve que los chicos suelen recurrir a la ciberviolencia para ganarse la aprobación social de sus compañeros. Los chicos destacan cómo las normas dominantes de masculinidad moldean su comportamiento en línea. Actos como compartir imágenes sin consentimiento o el acoso en grupo se enmarcan como actuaciones para impresionar a los demás o ajustarse a las expectativas de los compañeros.



Las niñas están expuestas a la ciberviolencia desde una edad temprana

- La ciberviolencia comienza cuando las chicas empiezan a utilizar las tecnologías digitales y las redes sociales; muchas recuerdan haber recibido mensajes ofensivos o no deseados ya desde muy temprano, a veces incluso antes de entrar en la escuela secundaria. Los datos de la encuesta confirman que los mensajes no deseados y los contenidos explícitos se encuentran entre las formas más comunes de abuso en línea, y una proporción significativa de chicas afirma haber tenido este tipo de experiencias antes de los 15 años.
- Las chicas más jóvenes (de 13 a 15 años) denuncian formas de agresión más relacionales y por parte de sus compañeros, como la exclusión, los chismes y las burlas sobre el aspecto físico, mientras que las chicas de más edad (de 16 a 18 años) se enfrentan con mayor frecuencia a formas de abuso sexualizadas y coercitivas, como el acoso sexual en línea coacción y extorsión ([2]), deepfakes y difusión de imágenes sin consentimiento.
- Aparecen contenidos inapropiados o sexualizados incluso en plataformas diseñadas para niños, lo que demuestra que las medidas de protección existentes son insuficientes. Las niñas reclamaron actividades de prevención y alfabetización digital más tempranas y adecuadas a su edad, señalando que las sesiones de sensibilización en los colegios a menudo solo se llevan a cabo después de que se hayan producido los incidentes.

2 La coacción sexual y la extorsión en línea de menores son definidas por la Agencia de la Unión Europea para la Cooperación Policial (Europol) como una forma de chantaje digital a menores en la que se utilizan información o imágenes de carácter sexual para obtener material sexual, favores sexuales o dinero de una víctima (Europol, 2017). También es una forma de violencia de género facilitada por la tecnología, a la que a menudo se hace referencia coloquialmente como «sextorsión» cuando afecta a víctimas adultas. Europol recomienda que este término coloquial no se utilice en los casos que afectan a menores.

El abuso sexual y basado en imágenes, incluidos los «deepfakes» generados por IA, es una forma creciente y especialmente dañina de ciberviolencia

- El abuso sexual y basado en imágenes es una de las formas más visibles y perjudiciales de ciberviolencia; las personas afectadas describen estas experiencias como profundamente angustiosas y perjudiciales para su privacidad, su reputación y su sensación de seguridad. A menudo se toman o se comparten fotos no consentidas en entornos escolares o entre compañeros, y se difunden rápidamente más allá del control de las niñas.
- La creación y distribución de imágenes manipuladas o generadas por IA («deepfakes» o «deepnudes») constituye una nueva y alarmante forma de abuso, utilizada para humillar o coaccionar a las niñas y que les deja con escasas posibilidades de reparación.
- La rapidez y el alcance de la difusión en línea amplifican el daño, ya que las fotos y los vídeos pueden circular ampliamente en cuestión de segundos. Incluso las imágenes aparentemente inofensivas, compartidas voluntariamente o con amigos, pueden convertirse en una fuente de acoso o chantaje cuando se utilizan sin consentimiento o se sacan de contexto.

Las medidas de protección y las respuestas institucionales no siguen el ritmo de los cambios tecnológicos

- Los análisis jurídicos y normativos muestran que las medidas de protección contra la ciberviolencia siguen siendo fragmentadas y desiguales en toda la UE. La Directiva (UE) 2024/1385 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica supone un importante paso adelante, y dar prioridad a su transposición íntegra al Derecho nacional y a su aplicación es fundamental para influir de manera significativa y positiva en la vida de las mujeres y las niñas.
- Las niñas suelen percibir que los centros educativos, la policía y otras autoridades como mal preparadas o poco receptivas, y denuncian que sus quejas a veces se desestiman o se ignoran. El miedo a ser culpadas, la vergüenza y la falta de confianza en la capacidad de los adultos para actuar de manera eficaz disuaden a muchas de denunciar, lo que deja a las víctimas a su suerte para hacer frente al daño.
- Las prácticas de moderación débiles e inconsistentes permiten que los contenidos nocivos circulen ampliamente, mientras que el anonimato en línea permite a los agresores actuar con impunidad. De acuerdo con las disposiciones de la Ley de Servicios Digitales (DSA), se necesita una mayor coordinación entre las autoridades de la UE y las nacionales, junto con una responsabilidad vinculante para las plataformas digitales, a fin de garantizar que el progreso tecnológico vaya acompañado de una protección jurídica e institucional adecuada.

La cultura de grupo y las normas de género influyen considerablemente en la aparición de la ciberviolencia y en la forma en que se aborda

- La cultura entre iguales desempeña un papel crucial a la hora de determinar cómo se desarrolla la violencia en línea y cómo responden los jóvenes ante ella. Los comportamientos nocivos suelen verse reforzados por la presión social para adaptarse o mantener el estatus, especialmente entre los chicos, y por las normas de género que fomentan la culpabilización de las víctimas y los dobles raseros.
- La ciberviolencia refleja desigualdades de género más amplias, en las que se recurre a la humillación y al control para regular la apariencia, el comportamiento y la autoexpresión en línea de las chicas. La inacción de los espectadores también perpetúa el abuso: la mayoría de los adolescentes han sido testigos de violencia en línea sin intervenir, a menudo por miedo o incertidumbre.
- Los factores interseccionales, como la edad, la raza, la discapacidad, la pertenencia a una minoría religiosa, la orientación sexual, la identidad de género y el tamaño corporal, aumentan la vulnerabilidad, lo que agrava los riesgos para algunos grupos de niñas. Los participantes abogaron por iniciativas de prevención inclusivas y participativas que involucren a los chicos y fomenten la empatía, el respeto y la responsabilidad.
- Las buenas prácticas identificadas a través de estudios de situación a nivel nacional y de la UE muestran que la educación transformadora en materia de género y los enfoques basados en el diálogo pueden cuestionar las normas nocivas, empoderar a los testigos y reducir la tolerancia hacia el abuso en línea.

Introducción

En toda la Unión Europea, la ciberviolencia se ha convertido en una forma de violencia de género en rápida expansión que afecta con especial intensidad a los adolescentes. A medida que la comunicación digital se integra profundamente en la vida social de los jóvenes, los espacios en línea determinan cada vez más la forma en que se establecen, se negocian y, en ocasiones, se explotan las relaciones. Análisis recientes a escala de la UE muestran que las mujeres y las niñas están expuestas de manera desproporcionada a comportamientos intrusivos, sexualizados u hostiles en línea (EIGE, 2022), lo que refleja normas de género arraigadas y la dinámica cambiante de las interacciones entre iguales en los entornos digitales.

Con el auge de la conectividad digital y la creciente importancia de las redes sociales en la vida de los adolescentes, se ha intensificado el riesgo de acoso facilitado por la tecnología, el intercambio de imágenes sin consentimiento, el ciberacoso y los
en línea se ha intensificado (Consejo de Europa, 2018). Al mismo tiempo, las instituciones europeas e internacionales han ido reconociendo progresivamente la violencia de género en línea como un reto político apremiante (Relator Especial de las Naciones Unidas sobre la violencia contra las mujeres y las niñas, 2018; Parlamento Europeo, 2021a), destacando su relevancia social y política y sus implicaciones para los derechos de los niños, la salud mental y la igualdad de género.

Los conjuntos de datos y los informes institucionales existentes ponen de relieve la magnitud y la diversidad de los abusos en línea. Sin embargo, se sabe mucho menos sobre cómo las adolescentes entienden e interpretan estos comportamientos en su vida cotidiana, cómo reaccionan cuando se produce un daño y qué mecanismos de apoyo consideran significativos, fiables o insuficientes. Al adoptar un enfoque cualitativo y participativo, este estudio sitúa explícitamente a las adolescentes como portadoras de conocimiento, en lugar de como encuestadas pasivas —una elección metodológica que permite captar y poner de relieve de manera significativa sus voces, percepciones y experiencias vividas—. Estas aportan la evidencia más valiosa para la acción política a nivel de la UE y nacional.

El objetivo principal de este estudio es ampliar el conocimiento sobre cómo las adolescentes de entre 13 y 18 años experimentan la ciberviolencia en la UE. Esto implica examinar las formas en que definen y reconocen la ciberviolencia —tanto como víctimas como como testigos—, al tiempo que se analizan sus percepciones sobre los esfuerzos de prevención institucionales y dirigidos por adultos, así como sus experiencias a la hora de denunciar incidentes a sus padres, profesores o plataformas en línea. De este modo, la investigación no solo arroja luz sobre los encuentros directos de las chicas con la ciberviolencia, sino también sobre sus valoraciones de los mecanismos de apoyo disponibles y sus reflexiones sobre su propio comportamiento en línea. Las conversaciones con chicos adolescentes reflejan su conciencia de cómo la ciberviolencia afecta a las chicas y abordan cómo se comportan cuando son testigos de ella.

El estudio adoptó un enfoque metodológico en múltiples niveles que combinaba la investigación documental y el trabajo de campo con el fin de captar tanto las dimensiones estructurales del fenómeno objeto de investigación como las experiencias vividas por las personas directamente implicadas. La triangulación entre los distintos tipos de datos —datos cuantitativos, marcos normativos y jurídicos, y perspectivas participativas— garantizó tanto la amplitud como la profundidad ([3]).

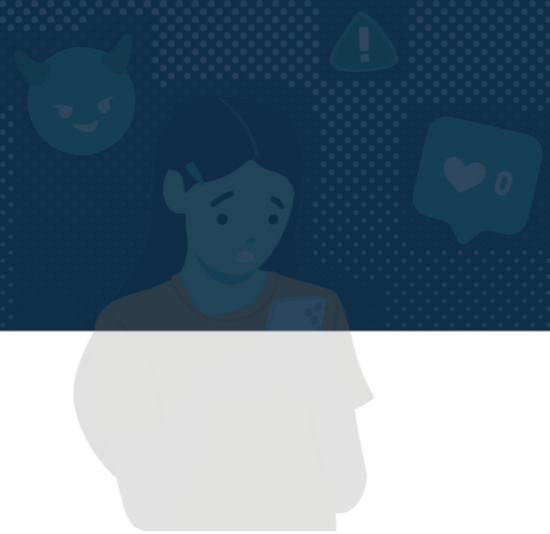
La investigación documental y la revisión bibliográfica proporcionaron la base conceptual y empírica para la investigación cualitativa. El mapeo normativo y jurídico de los marcos internacionales, de la UE y nacionales ayudó a identificar cómo se regula la ciberviolencia. Las fuentes oficiales se complementaron con técnicas de «bola de nieve» utilizadas para recabar medidas nacionales emergentes, lo que proporcionó una visión general comparativa de las respuestas jurídicas y normativas en los Estados miembros de la UE. El análisis estadístico de los datos contextualizó el fenómeno mediante encuestas a nivel de la UE y nacionales, estudios comparativos y proyectos financiados por la UE, como «EU Kids Online». Estos datos ayudaron a cuantificar las tendencias y a relacionar los datos estructurales con los resultados cualitativos.

El segundo pilar de la metodología fue el trabajo de campo cualitativo llevado a cabo en grupos focales, que recogió las experiencias vividas por los adolescentes. En diez Estados miembros (Bélgica, Alemania, Estonia, Irlanda, España, Italia, Chipre, Polonia, Rumanía y Suecia), se organizaron 37 grupos focales en los que participaron 133 chicas (de entre 13 y 18 años). También se celebraron debates en grupos focales con 38 chicos de entre 15 y 18 años en tres Estados miembros (Irlanda, Chipre y Rumanía). Las guías, adaptadas a la edad de los participantes, incluían herramientas interactivas para los grupos más jóvenes y debates basados en situaciones hipotéticas para los participantes de más edad; los grupos de chicos se centraron en las normas sociales, la masculinidad, el comportamiento de los testigos y la empatía.

El capítulo 1 presenta los fundamentos conceptuales y contextuales de la ciberviolencia, incluidas sus definiciones, sus principales formas y los datos sobre su prevalencia a nivel internacional, de la UE y nacional. También se analizan las causas percibidas y los factores que contribuyen a ella. El capítulo 2 presenta los resultados del trabajo de campo cualitativo, destacando el grado de concienciación y comprensión de la ciberviolencia que mostraron las chicas y los chicos que participaron
en los grupos focales de diez Estados miembros. El capítulo 3 explora con mayor detalle las experiencias de las niñas con la ciberviolencia, incluidos los contextos, los roles y las dinámicas implicadas. El capítulo 4 examina los impactos de la ciberviolencia en los jóvenes, destacando sus propias perspectivas sobre sus consecuencias sociales y psicológicas
. El capítulo 5 aborda la prevención y las respuestas, pasando revista a algunos ejemplos de marcos y medidas políticas a nivel internacional, de la UE y nacional, así como a las opiniones de los jóvenes sobre su eficacia. Por último, el informe concluye con conclusiones clave e implicaciones políticas, esbozando recomendaciones para futuras acciones a nivel de la UE y nacional.

3 Para una descripción más detallada de la metodología utilizada, véase el recuadro 7 del anexo.

1 El fenómeno de la ciberviolencia contra las niñas y las mujeres jóvenes



1.1. Conceptos y definiciones de la violencia ciber

La ciberviolencia contra las mujeres y las niñas es una forma multifacética e interseccional de violencia de género que abarca comportamientos como el acoso cibernético, el acoso sexual en línea, la difusión de imágenes sin consentimiento y el discurso de odio por motivos de género. Estos daños vienen determinados por normas sociales que refuerzan el dominio masculino, dinámicas relacionales como la coacción y la validación por parte de los compañeros, y factores de desarrollo que hacen que los adolescentes sean especialmente vulnerables al abuso en línea (Cybersafe, 2020). Aunque el discurso académico sobre la ciberviolencia se remonta a mediados de la década de 1990 ([4]), coincidiendo con el auge del uso de Internet y las plataformas en línea, el reconocimiento más amplio de la ciberviolencia contra las mujeres y las niñas solo ha recibido una atención sostenida en los últimos años. Estudios anteriores exploraron cómo la tecnología transformó los paradigmas dominantes en torno al género, la identidad
y la sexualidad (Gurumurthy et al., 2009), lo que suscitó preocupaciones sobre su papel a la hora de facilitar nuevas formas de violencia, en particular contra las mujeres. Tal y como ha argumentado Judy Wajcman (2004, 2010, 2015), la tecnología está profundamente arraigada en las relaciones de poder sociales y dista mucho de ser neutral: reproduce y reconfigura jerarquías de género que pueden sustentar formas simbólicas y estructurales de violencia.

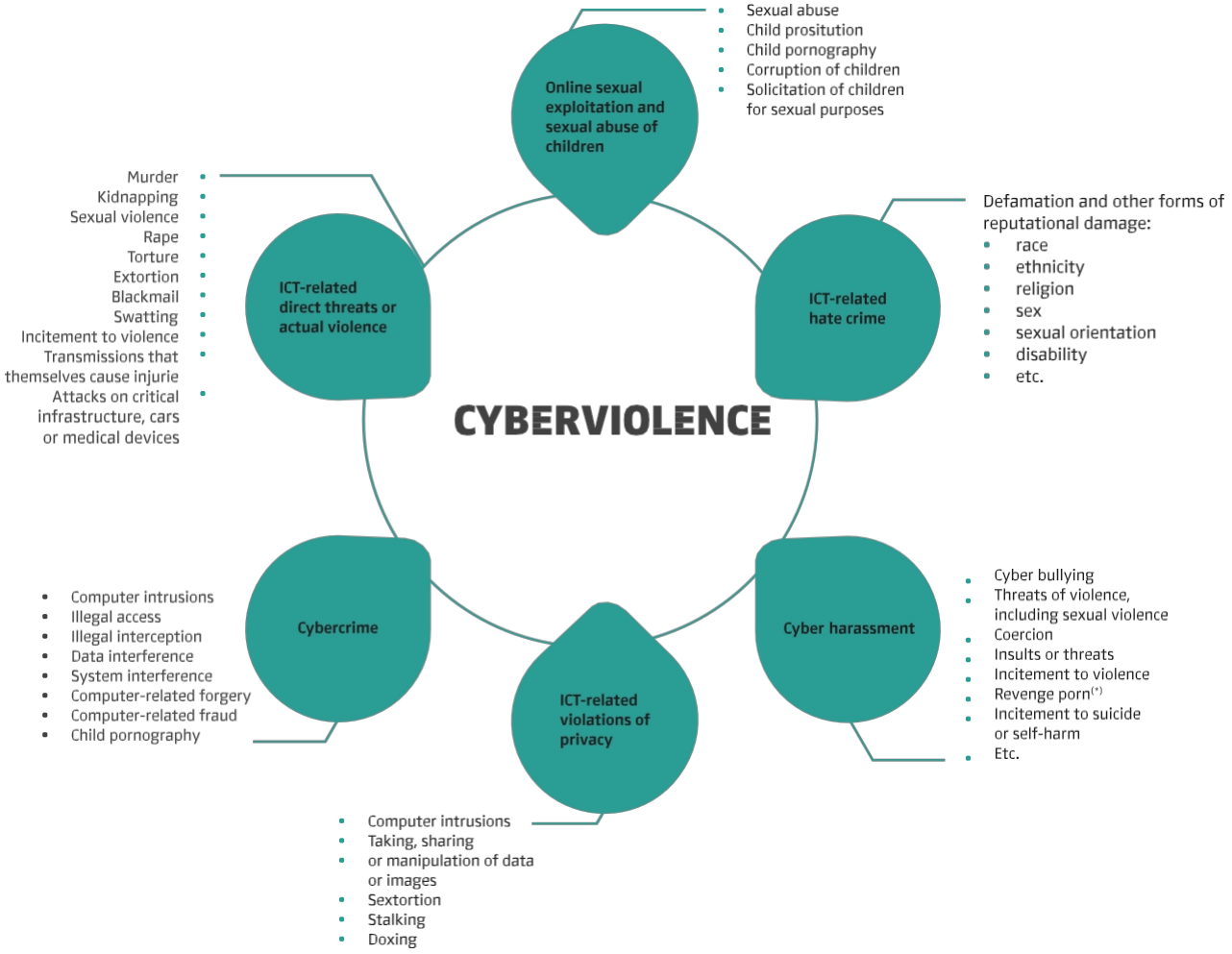
Dada su naturaleza en rápida evolución, la ciberviolencia se clasifica de diversas maneras, teniendo en cuenta el tipo de comportamiento, las características de las víctimas y los agresores, las herramientas tecnológicas utilizadas y las repercusiones resultantes (Mukred et al., 2024). Otros elementos clave a la hora de conceptualizar la ciberviolencia incluyen la percepción del daño por parte de la víctima y la falta de consentimiento (Koukopoulos et al., 2025).

4 Por ejemplo, los primeros estudios sobre la ciberviolencia —como «Acoso sexual en el ciberespacio: el problema del correo electrónico no deseado» de McGraw ([1995]) y «Ciberacoso y pornografía en Internet: género y la mirada» de Adam (2002)— ofrecen una visión del fenómeno y sus consecuencias.

La ciberviolencia contra las mujeres y las niñas abarca un amplio espectro de daños en línea, entre los que se incluyen el acoso, el bullying, el doxing, el trolling, el acoso sexual ([5]), la difamación, el discurso de odio y la explotación ([6]). Las víctimas suelen ser niños, adolescentes y mujeres, y hay determinados grupos que se ven afectados y son blanco de estos actos de forma desproporcionada. Los autores pueden actuar de forma individual, colectiva o a través de organizaciones, utilizando las redes sociales, las aplicaciones de mensajería, el correo electrónico, las comunicaciones telefónicas y otros canales digitales.

La naturaleza en constante evolución de la ciberviolencia plantea importantes retos para el desarrollo de definiciones conceptuales y jurídicas. Su magnitud y rapidez la convierten en una de las formas de violencia más generalizadas y graves de la sociedad contemporánea (USAID, 2023). Para mejorar la comprensión y reflejar mejor su complejidad, el Consejo de Europa propuso un marco multidimensional para la ciberviolencia (Consejo de Europa, 2018) que clasifica diversas formas de daño en línea, como las violaciones de la privacidad relacionadas con las tecnologías de la información y la comunicación (TIC), el ciberacoso, los delitos de odio y la explotación infantil en línea (Figura 1).

Figura 1 | Marco conceptual del Consejo de Europa sobre la ciberviolencia



Fuente: Consejo de Europa, 2018, p. 6.

(*) El término «pornografía de venganza» se utiliza habitualmente en los marcos jurídicos y normativos de los Estados miembros, mientras que la literatura académica suele referirse al «intercambio no consentido de imágenes íntimas». El término «pornografía de venganza» puede resultar engañoso, ya que minimiza la gravedad del delito, la diversa gama de formas de abuso relacionadas con el género o la sexualidad y su profundo impacto en las víctimas.

5 Este término abarca una amplia gama de acciones, como el acoso sexual basado en imágenes —incluidas las «creepshots», el «upskirting», el intercambio no consentido de imágenes o vídeos, el «cyberflashing», los «deepfakes» y las grabaciones de agresiones sexuales y violaciones—.

6 Este término abarca una amplia gama de situaciones, como las estafas con fines lucrativos o de extorsión, y la captación de niños o jóvenes con el fin de incitarlos a actividades sexuales o delictivas.

A nivel normativo, los documentos políticos de la UE han comenzado a hacer referencia a la definición de ciberviolencia de las Naciones Unidas, tal y como se expone en el informe de 2018 de la Relatora Especial de las Naciones Unidas sobre la violencia contra las mujeres y las niñas (Naciones Unidas, 2018). El informe define la ciberviolencia contra las mujeres como «la violencia de género contra las mujeres que se comete, se facilita o se agrava, en parte o en su totalidad, mediante el uso de las TIC,
como los teléfonos móviles y los smartphones, Internet, las plataformas de redes sociales o el correo electrónico, contra una mujer por el mero hecho de ser mujer, o que afecta a las mujeres de manera desproporcionada».

Esta definición fue reafirmada en la resolución del Parlamento Europeo de 2021 sobre la ciberviolencia (Parlamento Europeo, 2021a). A continuación se dio un importante paso legislativo con la adopción de la Directiva de la UE de 2024 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica (Directiva sobre la violencia contra las mujeres). Al ser la primera ley de la UE de carácter integral que aborda la violencia contra las mujeres, la directiva tipifica como delito una amplia gama de delitos cibernéticos, entre los que se incluyen el intercambio no consentido de material íntimo o manipulado, el acoso cibernético, el hostigamiento cibernético, la exhibición indecente en línea, la incitación cibernética a la violencia o al odio y el acoso sexual en línea. De este modo, constituye una base jurídica fundamental para definir y combatir la ciberviolencia en toda la UE, reconociendo su complejidad y su naturaleza cambiante. Además de ofrecer una definición muy necesaria, la directiva también incluye varias disposiciones fundamentales sobre la violencia cibernética, como la obligación de retirar contenidos, la definición de canales de denuncia adecuados y la necesidad de que los Estados miembros proporcionen
para las víctimas de la ciberviolencia. Teniendo en cuenta lo anterior, el recuadro 1 que figura a continuación resume las formas más frecuentes de ciberviolencia.

Recuadro 1 | Las formas más frecuentes de ciberviolencia

- Acoso cibernético. Esto incluye el acoso escolar en línea, el acoso sexual en línea, la recepción no solicitada de material sexualmente explícito, el acoso colectivo y el uso del nombre anterior. Según la directiva de la UE de 2024, el acoso cibernético incluye (i) participar de forma repetida o continua en conductas amenazantes dirigidas a una persona, al menos cuando dichas conductas impliquen amenazas de cometer delitos mediante las TIC; (ii) participar, junto con otras personas, mediante las TIC, en conductas amenazantes o insultantes de acceso público dirigidas a una persona; (iii) el envío no solicitado, mediante las TIC, de una imagen, un vídeo u otro material similar que muestre genitales a una persona; y (iv) poner a disposición del público, mediante las TIC, material que contenga los datos personales de una persona, sin el consentimiento de dicha persona.

- Ciberacoso. Someter a una persona a vigilancia de forma repetida o continua, sin su consentimiento ni autorización legal para hacerlo, mediante las TIC, con el fin de rastrear o supervisar sus movimientos y actividades.

- Violaciones de la privacidad relacionadas con las TIC. Esto incluye el acceso, la grabación, el intercambio, la creación y la manipulación de datos o imágenes privadas, especialmente el abuso sexual a través de imágenes, la creación o distribución no consentida de imágenes sexuales privadas, el «doxing» y el robo de identidad.

- La grabación y el intercambio de imágenes de violaciones u otras formas de agresión sexual.

- Control o vigilancia a distancia. Esto incluye el uso de aplicaciones espía en dispositivos móviles.

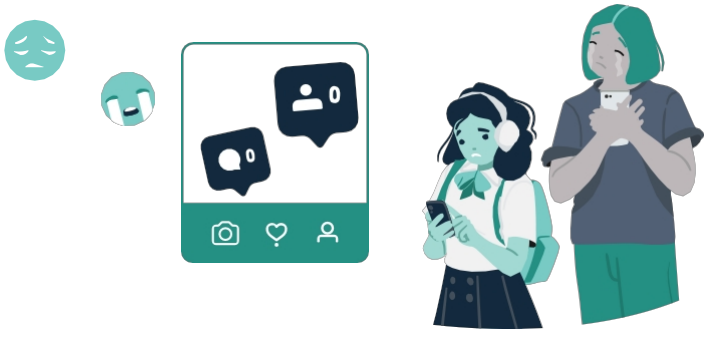
- Amenazas. Esto incluye amenazas directas y amenazas o incitaciones a la violencia, como amenazas de violación, extorsión, coacción sexual en línea y extorsión (sextorsión) y chantaje dirigidos hacia la víctima, sus hijos, sus familiares u otras personas que apoyan a la víctima y que se ven indirectamente afectadas.

- Discurso de odio sexista. Publicar y compartir contenidos que inciten a la violencia o al odio contra las mujeres o las personas LGBTIQ+ (lesbianas, gais, bisexuales, transgénero, intersexuales y queer) por motivos de su identidad de género, expresión de género o características sexuales.
- Incitación a infligirse violencia a uno mismo. Esto incluye actos violentos como el suicidio, la anorexia o el daño psicológico.
- Daños informáticos. Esto incluye el daño a archivos, programas o dispositivos, así como los ataques a sitios web y otros canales de comunicación digital.
- Acceso ilícito. Esto incluye el acceso ilícito a teléfonos móviles, correo electrónico, mensajes de mensajería instantánea o cuentas en redes sociales.
- Incumplimiento de las restricciones a la comunicación impuestas mediante órdenes judiciales.
- El uso de medios tecnológicos para la trata de personas. Esto incluye la explotación sexual de mujeres y niñas.

Fuente: Parlamento Europeo, 2021a.

A la luz de estas definiciones, las inconsistencias terminológicas entre los contextos jurídicos y académicos ponen de relieve la necesidad de interpretaciones amplias de la ciberviolencia que puedan abarcar las diversas formas y expresiones de violencia a las que puede referirse (EIGE, 2022).

Si bien la ciberviolencia puede dirigirse contra cualquier persona o grupo y abarcar una variedad de acciones y comportamientos, afecta de manera desproporcionada a las mujeres y a los niños (Consejo de Europa, 2018). Además, aunque los hombres también pueden sufrir ciberviolencia, las investigaciones (p. ej., Backe et al., 2018; Hicks, 2021) muestran que las mujeres y las niñas se enfrentan a mayores riesgos debido a las normas de género arraigadas y a las desigualdades, y a menudo sufren consecuencias más graves y duraderas (EIGE, 2022). Dado que los jóvenes son los usuarios más activos de las redes sociales y las TIC, las investigaciones internacionales ([7]) han puesto de relieve que las niñas y las mujeres jóvenes se enfrentan a una mayor vulnerabilidad ante formas específicas de ciberviolencia, entre las que se incluyen, entre otras, el ciberacoso y la difusión no consentida de imágenes íntimas. Esto subraya la necesidad de un enfoque centrado en la infancia ([8]) que tenga en cuenta cómo los factores psicológicos, de desarrollo y sociales influyen en las interacciones digitales de los jóvenes (Cybersafe, 2020).



7 Véase, por ejemplo, PLAN International, 2020; Vogels, 2022; Sciacca et al., 2023.

8 Véase Consejo de Europa, 2020. En la biblioteca del Consejo de Europa se encuentra disponible bibliografía adicional sobre este tema, que incluye investigaciones sobre la ciberviolencia clasificadas por grupo destinatario, entre ellas estudios centrados específicamente en los niños. Véase, por ejemplo, WeProtect Global Alliance, 2016, 2021. Para obtener más información, visite la biblioteca del Consejo de Europa sobre ciberviolencia: https://www.coe.int/en/web/cyberviolence/library1.

Recuadro 2 | Formas de ciberviolencia contra las mujeres y las niñas consideradas en este estudio de investigación

- Ciberacoso (incluido el ciberacoso escolar)
- Ciberacoso
- Difusión no consentida de material íntimo o manipulado
- Incitación cibernética a la violencia o al odio dirigida contra mujeres y niñas
- Estas formas de violencia cibernética se recogen en la Directiva de la UE de 2024 sobre la violencia contra las mujeres y se reconocen como las formas más extendidas de violencia cibernética (EIGE, 2022).

1.2. Prevalencia y contextos de la violencia ciber

La ciberviolencia contra las mujeres y las niñas se reconoce cada vez más como parte de un continuo más amplio de violencia que incluye comportamientos tanto en línea como fuera de línea (Dunn, 2020; Lu et al., 2021; Machado et al., 2022). Se basa en desequilibrios estructurales de poder y se perpetúa a través de los estereotipos de género de la sociedad (EIGE, 2024). Muchas formas de ciberviolencia, como el acoso, el bullying y el acecho, suelen tener su origen en interacciones fuera de línea, y el entorno digital amplifica su alcance e impacto.

En un mundo en el que las tecnologías digitales están integradas en la vida cotidiana, Internet y las herramientas relacionadas se han convertido en extensiones de los entornos en los que las mujeres y las niñas sufren violencia. Esta dimensión digital también tiene consecuencias directas para su seguridad, dignidad y bienestar general (OEA, 2021). Por ejemplo, el acoso callejero, el acoso escolar y la violencia de pareja pueden extenderse a los espacios digitales a través del ciberacoso, el ciberacoso escolar, la difusión de imágenes sin consentimiento y el acoso en línea. Por el contrario, las interacciones en línea con desconocidos en las redes sociales pueden ser aprovechadas por los agresores y derivar en amenazas en el mundo real, incluida la violencia sexual. Estos patrones de abuso ponen de relieve el vínculo entre la violencia digital y la física contra las mujeres y las niñas (OEA, 2021).

Los estudios revelan un solapamiento significativo entre la ciberviolencia y el abuso fuera de línea; por ejemplo, el 70 % de las víctimas de ciberacoso y acoso en la UE también han sufrido violencia de pareja, tal y como muestra la Agencia de los Derechos Fundamentales de la UE (FRA) (2015). Este solapamiento subraya la naturaleza generalizada de la ciberviolencia contra las mujeres y las niñas y cómo está arraigada en patrones más amplios de violencia sistémica.

Además, las TIC han desempeñado un papel significativo a la hora de facilitar nuevas estrategias de abuso y control, especialmente en el contexto de la violencia de pareja. Entre las parejas jóvenes, estos comportamientos se han normalizado en las interacciones tanto en línea como fuera de línea y, a menudo, se malinterpretan como muestras de amor (Lu et al., 2021). Este tipo de abuso en línea incluye exigir el acceso a las contraseñas de la pareja, supervisar sus actividades en línea y restringir sus interacciones en las redes sociales.

Las investigaciones muestran de forma sistemática que, entre las mujeres, el acoso sexual y el acoso son las formas de ciberviolencia más comúnmente denunciadas (ONU Mujeres et al., 2023). Un aspecto especialmente alarmante del acoso en línea es su potencial de difusión generalizada más allá del control tanto del remitente como del destinatario. En casos extremos, la creación y difusión de imágenes sexuales en las que participan menores constituye la creación y difusión de material de abuso sexual infantil (Smahel et al., 2020).

Los datos de la Encuesta de la UE sobre la violencia de género (EU-GBV) (ola de 2021) ([9]) indican además que recibir mensajes o correos electrónicos no deseados es la forma más extendida de (ciber)violencia perpetrada de forma reiterada por el mismo agresor (9 %), superando a los comentarios ofensivos en público (4 %) o al abuso basado en imágenes (1 %) (figura A.7 del anexo). Cabe destacar que algunas víctimas declararon haber sufrido este tipo de experiencias antes de los 15 años, lo que pone aún más de relieve que la exposición a la violencia comienza en la infancia (figura A.8 del anexo).

Los testimonios de los jóvenes participantes en los grupos focales de este estudio confirman además que incluso imágenes aparentemente inofensivas —como una foto en bañador— pueden desencadenar acoso, chantaje o daños a la reputación a largo plazo, lo que refleja investigaciones que ponen de relieve cómo los contenidos pueden volverse rápidamente incontrolables una vez compartidos.

Las investigaciones también indican que la edad, junto con el género, desempeña un papel crucial en la incidencia de la ciberviolencia (Comité FEMM et al., 2018; Pichel et al., 2021; López-Castro et al., 2023; Schittenhelm et al., 2024).
El uso de las redes sociales es más frecuente entre las niñas y las mujeres jóvenes y menos habitual entre las mujeres de más edad. Para las mujeres jóvenes y las niñas, estas plataformas tienen múltiples funciones, entre ellas mantener amistades, comunicarse con la familia, explorar oportunidades laborales e interactuar con redes sociales más amplias. Sin embargo, las mujeres no tienen por qué ser usuarias activas de Internet para sufrir ciberviolencia o abusos. Aún así pueden ser objeto de ataques, por ejemplo, a través de la distribución en línea de contenido sexual o la explotación sexual en sitios web de trata de personas (Comisión FEMM et al., 2018).

Una encuesta mundial realizada en 2020 por la World Wide Web Foundation y la Asociación Mundial de Guías y Scouts Femeninas ([10]) reveló que el 52 % de las mujeres jóvenes y las niñas declararon haber sufrido algún tipo de abuso en línea. Cabe destacar que las encuestadas de entre 15 y 19 años expresaron una especial preocupación por el intercambio no autorizado de imágenes y vídeos privados. Del mismo modo, Plan International (Plan International, 2020) ha estimado que el 58 % de las mujeres jóvenes y las niñas de todo el mundo han sufrido acoso en línea en las redes sociales, señalando que la mayoría de las niñas indican que su primera experiencia de acoso en las redes sociales tuvo lugar entre los 14 y los 16 años.

Se ha constatado que los adolescentes y los jóvenes varones son blanco específico de la coacción sexual y la extorsión en línea, a menudo denominadas «sextorsión» (Thorn, 2024; WeProtect Global Alliance, 2024; Foster, 2023). En estos casos, las víctimas se enfrentan a chantajes o amenazas de que se difundan imágenes íntimas. Dichas imágenes o vídeos pueden haber sido compartidos por las propias víctimas o generados por inteligencia artificial. A continuación, los depredadores exigen a la víctima favores sexuales, contenido sexual y, en la mayoría de los casos, dinero a cambio de no difundir las imágenes. Los datos de diversos países apuntan a que los autores actúan en redes delictivas organizadas, a menudo con sede en países menos desarrollados, siendo el lucro económico su principal motivación (Europol, 2017; Foster, 2023).
Con la creciente disponibilidad de herramientas gratuitas de IA generativa, los depredadores pueden utilizar fácilmente las fotos o vídeos de las víctimas publicados en las redes sociales para crear imágenes y vídeos «deepfake» (WeProtect Global Alliance, 20242024). Los datos de Australia, el Reino Unido y los Estados Unidos muestran un aumento en
los últimos años en el número de casos de adolescentes varones que sufren este tipo de violencia (Comisionado de eSafety y Autoridad Australiana de Comunicaciones y Medios de Comunicación (ACMA), 2022).

Los datos a nivel de la UE respaldan estas conclusiones, mostrando cómo los riesgos de la ciberviolencia varían tanto por edad como por género. Según datos de la Organización Mundial de la Salud (OMS), el ciberacoso es más frecuente tanto entre las niñas como entre los niños de 13 años en la mayoría de los Estados miembros y regiones de la UE. Como se observa en las figuras A.1 y A.2 del anexo, la encuesta de la OMS sobre los comportamientos de salud de los niños en edad escolar (HBSC)

9 La edición de 2021 de la Encuesta de la UE sobre la violencia de género incluye resultados de los 27 Estados miembros. En total, los resultados medios estimados para la UE-27 se basan en datos recopilados de 114 023 mujeres (de entre 18 y 74 años) de toda la UE. La recogida de datos tuvo lugar entre septiembre de 2020 y marzo de 2024. Eurostat coordinó la recogida de datos en 18 Estados miembros, y las autoridades estadísticas nacionales de estos países llevaron a cabo la encuesta. Italia aceptó compartir los datos de su encuesta nacional para proporcionar datos comparables sobre los principales indicadores. En los ocho Estados miembros restantes, la FRA y el EIGE se encargaron de la recogida de datos siguiendo el manual metodológico de Eurostat. Se puede consultar más información sobre la metodología de la encuesta en la página web de Eurostat: https://ec.europa.eu/eurostat/cache/metadata/en/gbv_sims.htm.

10 Esta encuesta mundial fue realizada en 2020 por la World Wide Web Foundation y la Asociación Mundial de Guías y Scouts Femeninas utilizando la plataforma de denuncias de UNICEF sobre las experiencias de los jóvenes en materia de abuso y acoso en línea. Hubo 8 109 encuestados, de los cuales el 51 % eran mujeres y el 49 % hombres. Los datos de la encuesta están disponibles en https://ureport.in/opinion/3983/.

(Cosma et al., 2024) indican que, en 2022, un porcentaje mayor de niñas de 13 años sufrió ciberacoso que de niños en casi todos los Estados miembros (22 Estados miembros) y en las regiones de Flandes y Valonia de Bélgica. Esta brecha de género también se observa entre los jóvenes de 15 años, ya que las niñas declaran tasas más elevadas de ciberacoso en 15 Estados miembros y en ambas regiones belgas.

Entre las niñas de 13 años, la prevalencia del ciberacoso oscila entre el 10 % en Portugal y los Países Bajos y el 29 % en Letonia. En el caso de los chicos de la misma edad, las tasas oscilan entre el 7 % en la región valona de Bélgica y el 32 % en Lituania. Entre los jóvenes de 15 años, la variación es similar: en el caso de las chicas, las tasas de ciberacoso declaradas oscilan entre el 7 % en Portugal y el 24 % en España, mientras que en el de los chicos, oscilan entre el 3 % en España y el 31 % en Lituania.

Si bien investigaciones anteriores sugerían que los incidentes de acoso cibernético eran más frecuentes en los Estados miembros con mayores tasas de acceso a Internet (FRA, 2015), esta relación ha perdido relevancia con el paso del tiempo. Desde 2015, las disparidades en el acceso a Internet entre los Estados miembros se han reducido significativamente ([11]), lo que sugiere que el nivel de conectividad no es un indicador significativo de la prevalencia de la violencia cibernética.

Además, aunque las redes sociales mejoran la comunicación y fomentan las relaciones sociales, su uso excesivo o compulsivo puede afectar negativamente al bienestar, y al de los niños y adolescentes en particular. El uso de las redes sociales entre los adolescentes muestra patrones de género, ya que son más las chicas que los chicos las que interactúan activamente con estas plataformas entre los 11 y los 19 años (Leonhardt et al., 2021). Además, los datos indican que las chicas experimentan efectos psicológicos negativos más intensos relacionados con el uso de las redes sociales.

Por ejemplo, las niñas de entre 11 y 13 años son más propensas que los niños a referir problemas de sueño, preocupaciones sobre la imagen corporal y síntomas depresivos (Academias Nacionales de Ciencias, Ingeniería y Medicina, 2024).

El uso excesivo de las redes sociales entre las niñas se ha asociado con una mayor vulnerabilidad a la depresión y la ansiedad, debido en gran medida a las presiones sociales relacionadas con la autoevaluación, la imagen corporal y el cumplimiento de los cánones de belleza. Estas presiones pueden contribuir a la insatisfacción, el malestar emocional y la baja autoestima (Sala et al., 2024). Las investigaciones muestran además que la susceptibilidad a estos efectos negativos varía según la edad y el género: las niñas de entre 11 y 13 años y los chicos de entre 14 y 15 años presentan un mayor riesgo de disminución de la satisfacción con la vida a medida que aumenta su uso de las redes sociales (Academias Nacionales de Ciencias, Ingeniería y Medicina, 2024).

Los resultados del estudio HBSC aportan pruebas adicionales de esta asociación, poniendo de relieve las preocupaciones relacionadas con el «uso problemático de las redes sociales», que se define como aquel uso que presenta síntomas similares a los de una adicción ([12]). Como se observa en las figuras A.3 y A.4 del anexo, en casi todos los Estados miembros en 2022, las niñas eran más propensas que los niños a declarar un uso problemático de las redes sociales tanto a los 13 como a los 15 años, con la excepción de Finlandia ([13]).
Entre los jóvenes de 15 años, el porcentaje más bajo de chicas que presentaban síntomas de uso problemático de las redes sociales se observó en los Países Bajos y Dinamarca (7 % en ambos), mientras que Rumanía registró la tasa más alta, con un 28 %. En el caso de los chicos, las tasas más bajas de «uso problemático de las redes sociales» notificadas se registraron en los Países Bajos, Hungría y Letonia (3 %), mientras que Rumanía volvió a presentar la tasa más alta, con un 18 %.

Como se observa en el recuadro 3, a nivel nacional, varios Estados miembros han realizado encuestas específicas sobre la ciberviolencia para comprender mejor su prevalencia, los grupos afectados y sus consecuencias.

11 Véanse los datos de Eurostat sobre el nivel de acceso a Internet en toda Europa: https://ec.europa.eu/eurostat/databrowser/view/tin00134/default/table?lang=en.

12 Los datos del estudio HBSC sobre el uso problemático de las redes sociales están disponibles en https://data-browser.hbsc.org/measure/problematic-social-media-use/.

13 En Finlandia, los chicos de 15 años eran más propensos que las chicas de la misma edad a declarar un uso problemático de las redes sociales (12 % frente a 8 %).

Recuadro 3 | Ejemplos de encuestas sobre ciberviolencia realizadas en los Estados miembros

- **Francia.** Una encuesta de 2022 realizada por Feministas contra el Acoso Cibernético ([14]) reveló que la mayoría de los encuestados que habían sido víctimas de ciberviolencia eran mujeres (84 %) y personas que sufrían discriminación en línea por su identidad de género y orientación sexual (43 %). Las personas con discapacidad y pertenecientes a minorías religiosas también se enfrentaban a riesgos desproporcionados y a mayores obstáculos a la hora de denunciar.

- **Eslovenia.** El proyecto ClickOFF! (2024) (Šulc et al., 2024) reveló que más del 50 % de las chicas de 13 años o más habían sufrido ciberviolencia. Los alumnos de más edad registraron tasas más elevadas tanto de victimización como de perpetración. Entre los alumnos de primaria, los de entre 15 y 16 años registraron las tasas más altas de victimización (57 %), mientras que los de 15 años eran los más propensos a cometer ciberviolencia (10 %).

- **Países Bajos.** Los datos de la Oficina Central de Estadística de los Países Bajos (2022/2024) ([15]) muestran que 1 de cada 5 jóvenes (de entre 15 y 24 años) sufrió amenazas en línea, acoso, acecho o la difusión de imágenes sin su consentimiento. En 2024, el 22 % de las chicas de entre 16 y 18 años declaró haber sufrido acoso sexual en línea, frente al 7-8 % de los chicos ([16]). En cuanto al acoso sexual fuera de línea, los datos revelaron además que las mujeres jóvenes se ven afectadas de manera desproporcionada ([17]).

- **Portugal.** La Asociación Portuguesa de Apoyo a las Víctimas ha dado a conocer los datos de la línea de ayuda «Safer Internet», que gestiona desde 2019. En 2019, la línea de ayuda registró 827 casos relacionados con la violencia sexual en línea, de los cuales 676 estaban relacionados con material de abuso sexual infantil. Además, la mayoría de los casos denunciados a la línea de ayuda para solicitar apoyo contra los delitos cibernéticos afectaban a jóvenes de entre 11 y 17 años.

- **Bélgica.** La encuesta #YouToo? de 2022 ([18]) reveló que 1 de cada 5 jóvenes había sufrido ciberacoso, a menudo a una edad temprana, lo que indica la necesidad de una alfabetización digital temprana y de medidas de prevención. En 2026, un estudio sobre la ciberviolencia en el contexto de las citas reveló que el 66 % de los encuestados afirmaba haber sido presionado para enviar fotos desnudo en aplicaciones de citas y que el 60 % de los encuestados que sí envió una foto desnudo a través de un sitio web de citas en línea fue posteriormente amenazado con su difusión ([19]).

- **Italia.** Una encuesta de 2023 realizada por el Osservatorio Indifesa ([20]) reveló que casi el 80 % de los adolescentes consideraba que Internet no era seguro. Entre las principales preocupaciones figuraban el ciberacoso (23 %), el robo de identidad y el aislamiento social (ambos con un 18 %), mientras que otras cuestiones incluían el abuso de imágenes íntimas sin consentimiento (14 %), el acoso (10 %) y el acecho (7 %).

- **Alemania.** El estudio «Cyberlife» de 2024, realizado por Bündnis gegen Cybermobbing (Alianza contra el ciberacoso) ([21]), reveló que 2 millones de estudiantes habían sufrido ciberacoso. Entre los principales problemas se encontraban la escasa concienciación de los padres y los centros educativos, así como la mayor vulnerabilidad de los jóvenes socialmente aislados. Resulta alarmante que 1 de cada 4 estudiantes afectados tuviera pensamientos suicidas, siendo el suicidio una de las principales causas de muerte entre los jóvenes de 15 a 25 años.

14 https://www.vscyberh.org/.
15 «2,2 millones de víctimas de delitos cibernéticos en 2022» – Oficina de Estadística de los Países Bajos.
16 «Estudio de prevalencia sobre la violencia doméstica y las conductas sexualmente transgresoras 2024» — Oficina de Estadística de los Países Bajos.
17 «Estudio de prevalencia sobre la violencia doméstica y las conductas sexualmente transgresoras 2024» – Oficina de Estadística de los Países Bajos.
18 «Ciberacoso: uno de cada cinco jóvenes en Bélgica ha sido víctima» – The Brussels Times.
19 «La violencia digital en el contexto de las citas y las relaciones entre (ex-)parejas en Bélgica» – Instituto para la Igualdad entre Mujeres y Hombres.
20 «Violencia en línea: protección y prevención de las víctimas menores de edad» – Terre des hommes.
21 Tensión entre fascinación y peligro: el ciberacoso entre los alumnos de secundaria – Cyberlife.

1.3. Causas percibidas y factores co es

La ciberviolencia está profundamente arraigada en estructuras sociales más amplias, normas de género, dinámicas entre iguales y el panorama digital en rápida evolución. No solo viene determinada por el comportamiento de los individuos, sino también por las desigualdades estructurales que hacen que ciertos grupos sean más vulnerables. **Entre las principales causas subyacentes se encuentran las relaciones de poder desiguales entre mujeres y hombres, los estereotipos de género y la falta de medidas de protección eficaces en las plataformas en línea.** La edad y otros factores que se entrecruzan, como la situación socioeconómica, la pertenencia a una minoría o la discapacidad, también pueden influir significativamente tanto en la exposición a la ciberviolencia como en su impacto. Los adolescentes, por ejemplo, corren un mayor riesgo al atravesar el desarrollo social, una mayor participación en línea y la presión de los compañeros, mientras que las niñas y las mujeres jóvenes se enfrentan de manera desproporcionada a formas sexualizadas de abuso en línea. Los estereotipos y normas de género persistentes, incluidas las expectativas sociales sobre cómo deben verse, comportarse o expresar su sexualidad las mujeres y los hombres, normalizan ciertas formas de acoso en línea y a menudo se utilizan para justificar y restar importancia al abuso.

Los primeros casos de ciberacoso suelen ser descartados por los propios niños como bromas o diversión inofensiva. Los niños más pequeños, en particular, pueden no reconocer estos comportamientos como ciberacoso, sino que los perciben como tolerables, sobre todo cuando las acciones carecen de lo que se percibe como intención maliciosa (Baas et al., 2013). **Esta minimización normaliza los comportamientos dañinos y retrasa el reconocimiento del abuso como un problema grave.**
Sin embargo, tres características clave diferencian el ciberacoso de las bromas inocentes o las interacciones lúdicas: la intención, la repetición y un desequilibrio de poder (Baas et al., 2013).

Los adolescentes de entre 15 y 16 años declaran estar más expuestos a contenidos sexuales en línea y recibirlos con mayor frecuencia que sus compañeros más jóvenes, de entre 12 y 14 años, y las chicas lo experimentan con mayor frecuencia que los chicos. Como se observa en la figura A.9 del anexo, a nivel de la UE existe una correlación significativa entre la edad y la recepción de mensajes de carácter sexual. En los 14 Estados miembros incluidos en el estudio «EU Kids Online», un mayor porcentaje de jóvenes del grupo de edad más mayor (15-16 años) declaró haber recibido este tipo de mensajes que en el grupo de edad más joven (12-14 años). Esto pone de relieve cómo una mayor actividad en línea, unida a las expectativas de género sobre la sexualidad femenina, aumenta los riesgos y la exposición, en particular para las adolescentes de más edad.
Como se ilustra en la figura A.10 del anexo, en la mayoría de los Estados miembros representados, salvo Croacia y Malta, las chicas se ven más afectadas por las solicitudes sexuales no deseadas que los chicos.

La edad es, por lo tanto, un factor determinante, ya que las transiciones de desarrollo que se producen durante la adolescencia aumentan tanto la participación digital como la vulnerabilidad a la ciberviolencia. Las adolescentes de más edad, que son más activas en línea y tienen más probabilidades de adoptar conductas de riesgo, se enfrentan a una mayor exposición a interacciones sexualizadas. Este mayor riesgo se ve agravado por las expectativas sociales en torno a la sexualidad, los dobles raseros de género y las prácticas de validación por parte de los compañeros. De hecho, aunque la exposición a contenidos sexuales se considera cada vez más una parte normal del desarrollo sexual de los adolescentes, también aumenta el riesgo de ciberviolencia (Murphy, 2024).

Los resultados de la Encuesta de la UE sobre la violencia de género confirman estas diferencias relacionadas con la edad en la exposición a la ciberviolencia. Las mujeres más jóvenes denuncian una mayor prevalencia de abusos basados en imágenes, como la publicación no consentida de fotos o vídeos. Por ejemplo, el 37 % de las mujeres de entre 25 y 34 años y el 23 % de las de entre 18 y 24 años denuncian este tipo de experiencias, frente a solo el 3 % de las mujeres de entre 55 y 74 años. Por otra parte, entre los tipos de violencia (cibernética) sufridos por las mujeres de más edad (55 años o más), los más comunes fueron los comentarios públicos ofensivos o vergonzosos (figura A.6 del anexo). Estos patrones indican que la edad, la etapa de la vida
y el tipo de participación digital son factores importantes que determinan los diferentes riesgos observados entre los distintos grupos.

Al igual que ocurre con todas las formas de violencia de género, la ciberviolencia contra las mujeres y las niñas también viene determinada por una serie de factores interseccionales que agravan la vulnerabilidad y la marginación en los espacios digitales. Entre ellos se incluyen la discapacidad, la orientación sexual, las creencias políticas, la religión, el origen social, la situación migratoria e incluso el estatus de celebridad (GREVIO, 2021). Estas identidades interseccionales pueden agravar la discriminación, haciendo que la ciberviolencia sea tanto más frecuente como más dañina.

Numerosos estudios hacen hincapié en la naturaleza interseccional de la ciberviolencia contra las mujeres y las niñas, y revelan que las mujeres y las niñas con identidades y orígenes diversos suelen enfrentarse a un mayor riesgo de sufrir abusos en línea. Por ejemplo, la FRA (2015) constató que el 34 % de las mujeres con discapacidad declararon haber sufrido violencia física, sexual o psicológica, incluidas amenazas en línea, en comparación con el 19 % de las mujeres sin discapacidad.
El estigma relacionado con la discapacidad, las barreras para denunciar y el aislamiento intensifican aún más el daño.

El origen étnico y la condición de minoría también influyen significativamente en el riesgo de sufrir abusos en línea. Un estudio de la FRA de 2017 (FRA, 2017) centrado en las minorías indicó que los migrantes más jóvenes sufren más acoso, tanto presencial como en línea, que los migrantes de más edad. Entre los migrantes y las minorías, estas formas de acoso minan la confianza en las instituciones y dificultan la integración social (FRA, 2015). Las perspectivas de los jóvenes expresadas en los grupos de discusión añaden una dimensión vivencial a estas conclusiones, ya que varios de ellos describieron cómo su origen étnico y las expresiones visibles de su fe los convierten en objetivos en Internet. Por lo tanto, los prejuicios y el racismo sistémico son factores que contribuyen de manera decisiva al acoso en línea.

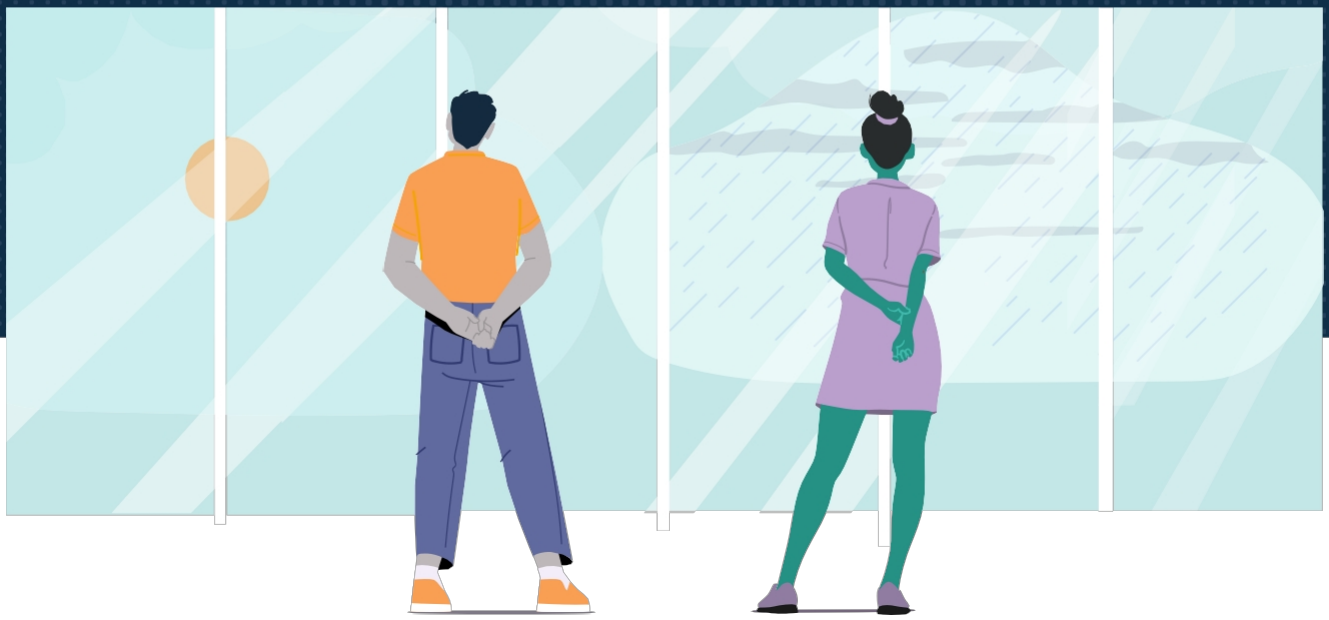
Desde la perspectiva de los niños, niñas y jóvenes, factores como la raza, la religión, el origen étnico (Ratajczak et al., 2019), la clase social, la discapacidad, la orientación sexual y la identidad de género aumentan el riesgo de sufrir (Proyecto deSHAME, 2017). Los estudios confirman que las adolescentes procedentes de entornos socioeconómicos desfavorecidos, de grupos minoritarios o con discapacidad se ven afectadas de manera desproporcionada. Por ejemplo, Wallace et al. (2023) descubrieron que alrededor del 40 % de la variación en la victimización por ciberviolencia entre las chicas de entre 14 y 18 años es atribuible a factores interseccionales. Del mismo modo, los datos del Pew Research Center (Vogels, 2022) muestran que las experiencias de ciberacoso entre los jóvenes estadounidenses varían no solo según la edad, sino también según el aspecto físico, el origen étnico, la orientación sexual y las creencias políticas. Estos hallazgos ponen de relieve cómo los marcadores de identidad personal
interactúan con las dinámicas de poder sociales para configurar los patrones de riesgo. Hallazgos recientes en Bélgica muestran que los adultos jóvenes y las personas LGBTIQI+ son especialmente vulnerables a la violencia en línea en las aplicaciones de citas debido a su mayor uso de herramientas digitales en las relaciones y las citas, lo que fomenta ciertas formas
de violencia en línea. En el caso de las personas LGBTIQ+, esta violencia puede verse agravada por riesgos específicos, como la revelación involuntaria de su orientación sexual o la explotación de datos personales sensibles, lo que aumenta aún más su vulnerabilidad (Gilen, A., et al., 2025).

Las vulnerabilidades también pueden derivarse de circunstancias personales, como problemas familiares, abusos previos o la participación en bandas (Proyecto deSHAME, 2017). La encuesta HBSC (Cosma et al., 2024) indica que la ciberviolencia entre iguales suele reflejar las circunstancias socioeconómicas, siendo los niños de familias con bajo nivel de riqueza los más propensos a verse afectados por la ciberviolencia. Este patrón se observa en varios Estados miembros de
la UE, con algunas excepciones en las que la prevalencia de la ciberviolencia es mayor entre los niños de familias con un alto nivel de riqueza ([22]). Además, el uso problemático de las redes sociales y el ciberacoso no muestran variaciones significativas entre los distintos grupos de nivel de riqueza familiar (tabla A.7 del anexo).

El capítulo 1 ha trazado el panorama conceptual de la ciberviolencia contra las niñas y las mujeres jóvenes, destacando sus formas y su prevalencia. Sin embargo, esto solo refleja parcialmente cómo se vive dicha violencia en la vida cotidiana. Para complementar este conjunto de datos con la experiencia vivida, el estudio contó con la participación directa de adolescentes. Como parte de esta investigación, se llevaron a cabo grupos de discusión con niñas y niños en Bélgica, Alemania, Estonia, Irlanda, España, Italia, Chipre, Polonia, Rumanía y Suecia para explorar cómo los jóvenes —especialmente las niñas— perciben, definen y experimentan la ciberviolencia. Estos debates proporcionaron información crucial de primera mano, que abarcaba tanto experiencias personales como observaciones de sus compañeros. Las conclusiones de los grupos focales se integran en los siguientes capítulos, ya que se utilizan las voces de los jóvenes para ilustrar
y ampliar la evidencia existente. De este modo, los siguientes capítulos desplazan su enfoque de los marcos teóricos hacia las realidades vividas, amplificando las perspectivas de las chicas y los chicos y vinculando sus experiencias al conjunto más amplio de la investigación.

22 Tal y como se muestra en la tabla A.6 del anexo. En estas áreas existe una diferencia significativa en la prevalencia de la ciberviolencia en función del nivel económico familiar ($^{con\ p < 0,05}$) tanto para las niñas como para los niños.

2. Percepciones de la ciberviolencia entre niñas y niños



2.1. Experiencia y comprensión de la violencia ciber

Tal y como se ha comentado en la sección 1, la ciberviolencia es una amenaza generalizada y en rápida evolución que afecta de manera desproporcionada a los niños, adolescentes y jóvenes adultos —en particular a las niñas—, y su etapa de desarrollo y las lagunas en la protección jurídica pueden agravar el daño que sufren (EIGE, 2022). La ciberviolencia se manifiesta de diversas formas, entre las que se incluyen el acoso verbal, la manipulación psicológica, los ataques a la reputación y el abuso sexual facilitado por la tecnología. Comprender estas diversas formas es esencial para que los jóvenes para reconocer los comportamientos abusivos y responder de manera eficaz.

Las experiencias y la percepción que tienen los jóvenes de la ciberviolencia difieren significativamente según la edad y el género (Vogels, 2022). Esta variación se analiza con mayor profundidad a través de los propios relatos de las niñas sobre la ciberviolencia en los grupos de discusión, tal y como se detalla en las secciones siguientes. Las niñas de más edad, por ejemplo, son más propensas a sufrir formas de abuso invasivas y sexualmente explícitas, como el envío no solicitado de imágenes explícitas, el intercambio no consentido de imágenes explícitas y las preguntas persistentes sobre su paradero y sus actividades por parte de personas que no son sus padres. Por el contrario, las niñas más jóvenes suelen sufrir insultos ofensivos y la difusión de rumores falsos sobre ellas (tabla A.4 del anexo). Esta evolución sugiere que, a medida que las niñas crecen, la ciberviolencia que sufren se vuelve cada vez más sexualizada y controladora. Además, estos patrones coinciden con las propias descripciones de las niñas sobre la humillación pública, la exclusión social y los juicios basados en la apariencia, lo que demuestra que la ciberviolencia se vuelve más compleja a medida que las niñas maduran.

La violencia de pareja facilitada por la tecnología como motivo de creciente preocupación

Un tema emergente en la investigación sobre la ciberviolencia dirigida contra niñas y mujeres jóvenes es la violencia de pareja facilitada por la tecnología. Esta forma de maltrato se caracteriza por acciones como el control, el acoso, el acecho y el maltrato a la pareja a través de la tecnología y las redes sociales (Zweig et al., 2014).

Esta forma de violencia de pareja puede darse tanto en el marco de una relación en curso como tras la ruptura de la misma, y puede manifestarse de forma emocional, física o sexual. Los agresores utilizan una amplia gama de métodos digitales: el acceso no autorizado a cuentas de correo electrónico o redes sociales, el rastreo por GPS y el uso de «stalkerware», la manipulación emocional y las amenazas en línea son prácticas habituales. También es habitual el uso de dispositivos domésticos «inteligentes» para la vigilancia y el acoso, junto con herramientas de inteligencia artificial. Cabe destacar que estos comportamientos suelen continuar incluso después de que la relación haya terminado.

La violencia de pareja facilitada por la tecnología suele estar entrelazada con formas presenciales de violencia en el noviazgo, y ambas formas suelen darse simultáneamente (Van Ouytsel et al., 2020). A los jóvenes —especialmente a las mujeres jóvenes— les puede resultar difícil reconocer estos comportamientos como abusivos, lo que complica los esfuerzos para identificarlos y abordarlos.

Los resultados de la Encuesta de la UE sobre la Violencia de Género confirman estos patrones: aproximadamente 1 de cada 9 mujeres declaró haber sido presionada por su pareja para revelar su paradero o haber sido rastreada digitalmente (a través del GPS, el teléfono o las redes sociales). Al desglosar los datos por edades, la incidencia es especialmente elevada entre las mujeres de 35 a 44 años, donde casi
1 de cada 4 (23 %) declaró haber sufrido este tipo de experiencias (figura A.5 del anexo).

La coacción para compartir imágenes sexuales está muy extendida

Los datos europeos del proyecto deSHAME (Proyecto deSHAME, 2017) en Dinamarca, Hungría y el Reino Unido muestran que 1 de cada 10 encuestados de entre 13 y 17 años (el 9 % en Dinamarca, el 7 % en Hungría y el 12 % en el Reino Unido) declaró haber sido presionado por su novio o novia para compartir imágenes de desnudos, siendo las chicas las más afectadas de manera desproporcionada. Además, 1 de cada 6 encuestados (16 %) declaró haber guardado una captura de pantalla de una imagen o conversación desnuda o sexualmente explícita para usarla en el futuro (el 13 % en Dinamarca, el 19 % en Hungría y el 16 % en el Reino Unido). Por otra parte, el 44 % de los encuestados reconoció que los jóvenes pueden incurrir en acoso sexual en línea como forma de venganza contra una expareja (el 51 % en Dinamarca, el 33 % en Hungría y el 47 % en el Reino Unido). El proyecto Cybersafe, que, a través de grupos focales con jóvenes de entre 13 y 17 años en Estonia,
Grecia, Italia e Irlanda del Norte, reveló que la violencia de pareja en línea —especialmente el maltrato de las mujeres por parte de los hombres— es un tema que se debate con frecuencia entre los adolescentes (Cybersafe, 2020).

El anonimato en Internet aumenta los riesgos para los grupos vulnerables

El anonimato que ofrecen las plataformas digitales permite a las personas ocultar fácilmente su identidad, lo que expone a las mujeres jóvenes, a las niñas y a las minorías sexuales, de género y étnicas a un mayor riesgo (Smith, 2023). Los participantes en los grupos focales se hicieron eco de estas preocupaciones y señalaron el acoso, los perfiles falsos y la vigilancia persistente de los espacios digitales personales como amenazas cotidianas. La facilidad con la que las personas pueden crear perfiles falsos o suplantar a otras en los espacios en línea aumenta los riesgos para quienes buscan conexión, lo que convierte estos entornos en lugares intrínsecamente inseguros y potencialmente violentos, con consecuencias emocionales (Smith, 2023).
Además, la naturaleza digital del abuso en línea puede llevar a los jóvenes a subestimar su impacto, al creer que el simple hecho de cerrar la sesión o bloquear al acosador ofrece protección suficiente (Afrouz et al., 2024).
Por lo tanto, comprender cómo el anonimato agrava los riesgos puede aumentar la concienciación de las chicas sobre las interacciones en línea potencialmente dañinas, animándolas a reconocer a tiempo los comportamientos peligrosos.

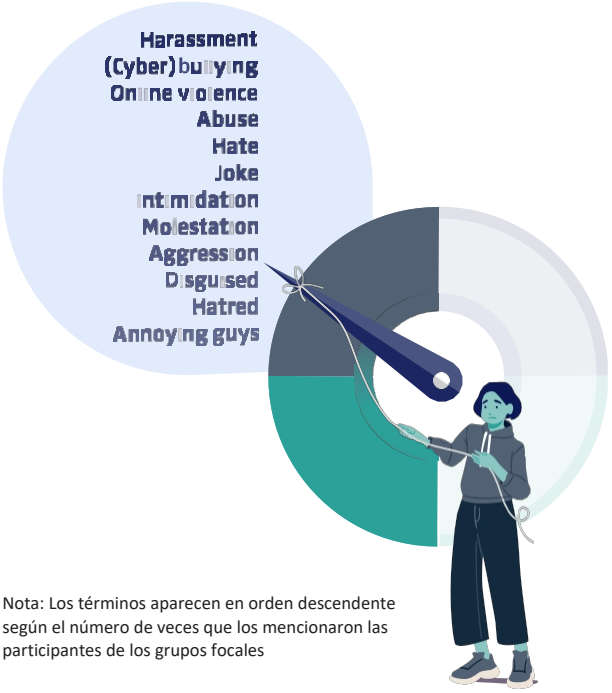
2.2. Comprender la ciberviolencia a través de las voces e es de los jóvenes

Las conclusiones de los grupos focales con chicas (de entre 13 y 18 años) llevados a cabo en el marco de este estudio proporcionan una comprensión más profunda de estos patrones. Las chicas demostraron una comprensión multifacética
de la ciberviolencia, moldeada por sus experiencias vividas y sus entornos sociales. Cuando se les preguntó sobre el término «ciberviolencia» ([23]), las chicas describieron un amplio espectro de comportamientos cotidianos, más que incidentes aislados o extremos. Entre ellos se incluían el abuso verbal y psicológico; formas sexualizadas de ciberviolencia; la coacción, la manipulación y el chantaje; y la humillación por el cuerpo y los juicios relacionados con la apariencia.

Antes de analizar en detalle temas específicos, es importante destacar las formas más generales de agresión en línea mencionadas anteriormente —acoso verbal, exclusión social y daño a la reputación—, que también fueron frecuentes en estos debates. Las chicas solían relacionar la ciberviolencia con patrones más amplios de acoso,
la intimidación y la exclusión social. Aunque estos comportamientos no siempre sean abiertamente sexuales o de carácter de género, contribuyen, no obstante, a crear entornos digitales en los que las chicas se sienten con frecuencia inseguras, sometidas a escrutinio o rechazadas.

Aunque menos frecuentes, otros temas importantes que surgieron y que son muy relevantes para la forma en que las chicas entienden y perciben la ciberviolencia que les afecta están relacionados con los grupos de chismes entre compañeras, las burlas por los errores, la difusión de rumores falsos y el acoso en grupo, todo lo cual refuerza una sensación de vulnerabilidad en los entornos en línea. Además, las chicas utilizaron términos como «patriarcado», «sexismo»
y «discriminación», lo que indica que son conscientes de que la ciberviolencia no es solo interpersonal, sino que tiene sus raíces en normas sociales más amplias, estereotipos de género y desigualdades de género.

FIGURA 2 | Términos principales utilizados por las niñas para describir la ciberviolencia en forma de agresión y violencia en general



Nota: Los términos aparecen en orden descendente según el número de veces que los mencionaron las participantes de los grupos focales

Fuente: Autores, a partir de los debates en grupos focales.

Las chicas también asociaron la ciberviolencia con una agresión en línea más generalizada, que incluye el acoso y la intimidación (Figura 2). Aunque no sean explícitamente de carácter sexual o de género, estos comportamientos fomentan un ambiente de hostilidad en el que las chicas se sienten inseguras, rechazadas o sometidas a un escrutinio constante. Otra preocupación recurrente entre las chicas es el uso indebido de la tecnología para distorsionar, manipular o robar
contenido personal. Las chicas expresaron su temor ante prácticas como la edición de fotos, el «doxing» y la creación de contenido falso utilizando imágenes privadas, lo que pone de relieve una creciente conciencia de que la ciberviolencia a menudo conlleva la pérdida de control sobre la información personal y la identidad digital. Además, las chicas identificaron comportamientos como el acoso, la invasión de la privacidad, el uso de cuentas falsas y las llamadas anónimas como formas de ciberviolencia. Esta percepción, aunque no siempre está vinculada a amenazas explícitas, pone de relieve una sensación persistente de estar siendo vigiladas, observadas o rastreadas en línea.

23 Esta sección ofrece una visión general de cómo las chicas interpretaron espontáneamente el término «ciberviolencia» durante los debates de los grupos focales y con qué lo asociaron, en respuesta a la pregunta «¿Qué te viene a la mente cuando oyes el término ciberviolencia?». Refleja sus percepciones y asociaciones iniciales, sin filtros. El objetivo no es redefinir ni desarrollar un marco conceptual formal para la ciberviolencia, ni introducir nueva terminología. En cambio, esta sección arroja luz sobre el lenguaje, las imágenes y las referencias que las propias chicas utilizan al reflexionar sobre el tema.

FIGURA 3 | Términos principales utilizados por las chicas para describir la ciberviolencia en forma de abuso verbal y psicológico

Fuente: Autores, a partir de los debates en grupos focales.

La agresión verbal en línea se describió como especialmente generalizada, y se produce con frecuencia en secciones de comentarios, mensajes privados o chats grupales (Figura 3). Los testimonios de las chicas refuerzan los resultados de las investigaciones que indican que los espacios en línea suelen caracterizarse por una hostilidad ambiental, donde los insultos, las amenazas y el acoso son habituales más que excepcionales.

Nota: Los términos aparecen en orden descendente según el número de veces que fueron mencionados por las participantes de los grupos focales.

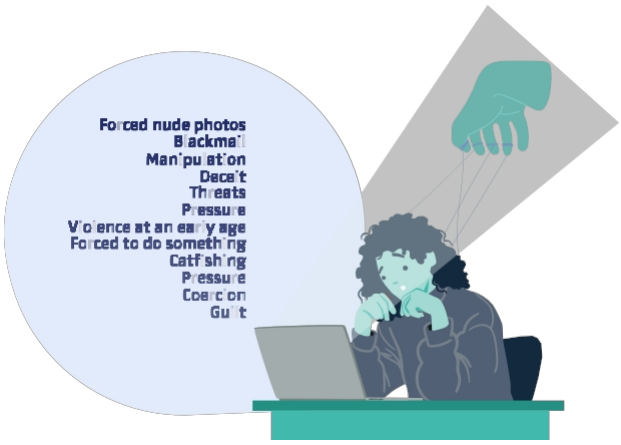
FIGURA 4 | Términos principales utilizados por las niñas para describir la ciberviolencia en forma de ciberviolencia sexual

Fuente: Autores, a partir de los debates de los grupos focales.

La ciberviolencia sexual se reveló como una preocupación central para las chicas (Figura 4). Estas asociaban la ciberviolencia con el envío no solicitado de desnudos, la captación de menores con fines sexuales, el abuso basado en imágenes y el porno vengativo. Su lenguaje reflejaba una profunda conciencia tanto de las formas como de las consecuencias emocionales de estos comportamientos.

Nota: Los términos aparecen en orden descendente según el número de veces que fueron mencionados por las participantes en los grupos focales

FIGURA 5 | Términos principales utilizados por las chicas para describir la ciberviolencia en forma de coacción, manipulación y chantaje

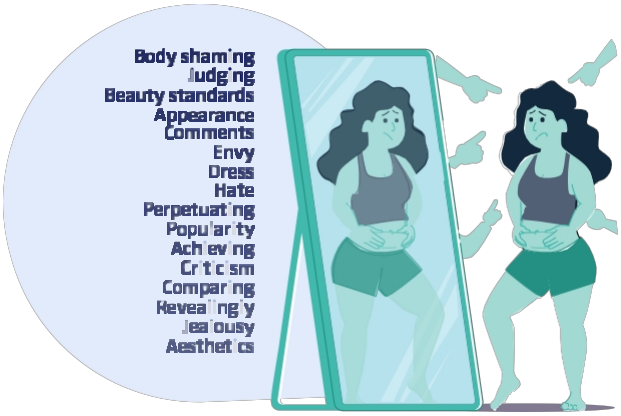


Fuente: Autores, a partir de los debates en grupos focales.

Las chicas señalaron con frecuencia la manipulación como un aspecto significativo de la ciberviolencia (Figura 5). Sus métodos —como el chantaje— se describían a menudo como estrategias continuas de control que se aprovechan de la confianza y la vulnerabilidad emocional. Una de las manifestaciones más claras de esta dinámica es la presión y la coacción para compartir contenido sexual. Los agresores se aprovechan de la confianza, manipulando a las víctimas para que envíen imágenes de desnudos o participen en interacciones sexuales en línea. Esta presión puede escalar hasta convertirse en chantaje,
como amenazas de filtrar mensajes o imágenes privadas a menos que la víctima acceda a lo que se le exige (Salazar et al., 2023).

Nota: Los términos aparecen en orden descendente según el número de veces que los mencionaron las participantes de los grupos focales

FIGURA 6 | Términos principales utilizados por las niñas para describir la ciberviolencia en forma de vergüenza corporal, juicios y cánones de belleza



Fuente: Los autores, a partir de los debates de los grupos focales.

Los juicios basados en la apariencia, la humillación por el aspecto físico y la comparación social también se citaron como formas comunes y perjudiciales de daño en línea (Figura 6), lo que pone de relieve cómo las expectativas de género y los cánones de belleza impuestos por la sociedad aumentan la vulnerabilidad de las niñas ante los daños en los entornos digitales.

Nota: Los términos aparecen en orden descendente según el número de veces que los mencionaron los participantes en los grupos focales.

Tal y como se desprende de la bibliografía especializada, la percepción que tienen las chicas de la ciberviolencia también variaba según la edad, lo que refleja sus etapas de desarrollo, su exposición al mundo digital y sus entornos sociales. Las chicas más jóvenes, de entre 13 y 15 años, tendían a centrarse en formas de ciberviolencia más inmediatas, visibles y relacionales. Sus preocupaciones estaban estrechamente vinculadas a entornos sociales familiares, como el colegio y los grupos de iguales. Muchas describieron experiencias de acoso, exclusión de chats grupales, comportamientos críticos y humillaciones por el aspecto físico como formas clave de daño en línea. También expresaron ansiedad en torno a su apariencia y a la comparación social, haciendo referencia con frecuencia a los cánones de belleza y a la evaluación del cuerpo. Un tema recurrente entre este grupo de edad fue el miedo a la visibilidad y al daño a la reputación, con términos como «humillación pública», «compartir capturas de pantalla» y etiquetas sexualmente despectivas que reflejaban la preocupación por quedar expuestas, ser juzgadas o ridiculizadas en los espacios en línea.

Las chicas de más edad, de entre 16 y 18 años, mostraron una comprensión más amplia y compleja de la ciberviolencia, que incorporaba dimensiones estructurales y psicológicas. Hicieron referencia con frecuencia a formas sexualizadas de daño, como la coacción y la extorsión sexuales en línea, el abuso sexual y basado en imágenes, y la captación de menores con fines sexuales. En este grupo se debatieron con mayor frecuencia los efectos sobre la salud mental, con referencias al trauma, el suicidio y el daño emocional a largo plazo, lo que refleja una profunda conciencia de las consecuencias psicológicas duraderas de la ciberviolencia.

> **“Los cánones de belleza hacen que a las chicas les resulte difícil sentirse ellas mismas y sentirse bien consigo mismas... en cuanto a cómo debería ser nuestro cuerpo, nuestro rostro o nuestro pelo. Y creo que por eso vemos más acoso y violencia hacia las mujeres.”**
>
> **(NIÑA DE 13 A 15 AÑOS, CHIPRE)**

Además, las chicas de más edad parecían estar más familiarizadas con el uso indebido de la tecnología, ya que describieron incidentes relacionados con deepfakes y deepnudes, fotos retocadas y doxing, y expresaron su preocupación por la manipulación y el robo de contenido digital personal. Sus temores se vieron agravados por el rápido avance de la IA, que consideraban que daba pie a nuevas y más dañinas formas de ciberviolencia. Uno de los fenómenos más alarmantes en este ámbito es la proliferación de «deepnudes» o vídeos que contienen imágenes íntimas sintéticas no consentidas (De Vido, 2024). La combinación de datos fácilmente accesibles, la capacidad tecnológica actual y la difusión de aplicaciones de deepfakes permite fabricar vídeos explícitos sin consentimiento

(EIGE, 2021). Esta facilidad tecnológica amplía drásticamente el número potencial de autores e intensifica el riesgo, ya que el contenido nocivo puede generarse y difundirse más rápido, de forma más amplia y con mayor anonimato que nunca.

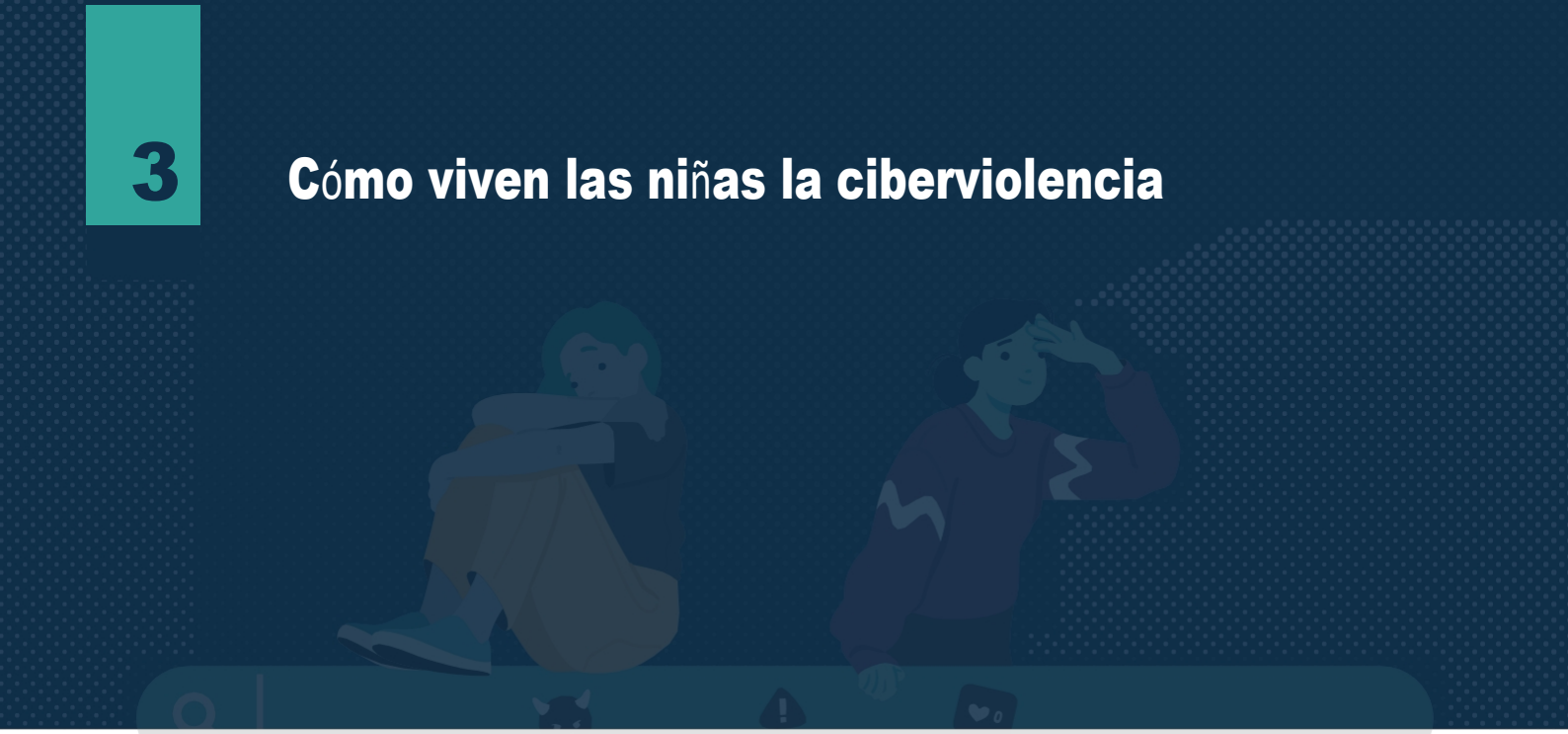
Los chicos de entre 15 y 18 años, por su parte, demostraron una comprensión multifacética de la ciberviolencia tal y como afecta a las chicas, identificando comportamientos que iban desde el acoso verbal hasta formas más graves de abuso sexual y psicológico. El acoso y el abuso verbal —como los insultos, las amenazas y las palabrotas— fueron las formas de ciberviolencia más citadas entre los chicos de este grupo de edad. Estos comportamientos se describían habitualmente como algo que ocurría en entornos entre iguales y, en ocasiones, se normalizaban o se restaba importancia a los mismos como parte de la cultura cotidiana en línea.

> **“Ahora, con la IA, he oído hablar de una chica que se suicidó porque los chicos de su clase le hicieron fotos y, gracias a la IA, hicieron que pareciera que estaba desnuda y se las enviaron a todo el mundo.”**
>
> **(CHICA DE 16 A 18 AÑOS, POLONIA)**

Los chicos de más edad identificaron con mayor frecuencia formas de ciberviolencia de carácter sexual, como la coacción y la extorsión sexuales en línea, el abuso sexual y el abuso basado en imágenes, y la captación de menores con fines sexuales. Esto sugiere que la concienciación sobre estos comportamientos o la exposición a ellos aumenta con la edad, aunque los contextos nacionales y culturales también pueden influir. De hecho, en Irlanda, Chipre y Rumanía —los tres países en los que se llevaron a cabo grupos de discusión con chicos— la legislación reciente ha tipificado como delito diversas formas de ciberviolencia. Estos cambios legales parecen haber reforzado la concienciación de los chicos, no solo ampliando su comprensión del tema, sino también fortaleciendo su reconocimiento del grave daño emocional y a la reputación que tales acciones pueden causar a las chicas, especialmente en los casos que implican el intercambio de imágenes personales o el chantaje en línea.

Por último, los chicos también señalaron plataformas digitales específicas en las que se producen estos comportamientos, como Fortnite y Snapchat. Describieron tácticas como el «catfishing» y la creación de cuentas falsas utilizadas para explotar, engañar o humillar a otras personas en línea.

3 Cómo viven las niñas la ciberviolencia



Los debates en grupos focales con chicas de todos los Estados miembros participantes revelaron un amplio espectro de experiencias de ciberviolencia, tanto como víctimas como testigos. A continuación, clasificamos estas experiencias en las formas de ciberviolencia enumeradas en la Directiva de 2024 para evitar introducir nuevos términos y conceptos y para alinear más estrechamente las experiencias de las chicas con los términos que en ella se recogen. Estos relatos apuntan a cuatro formas distintas, aunque interrelacionadas, de abuso: el acoso cibernético (sexual), el acecho cibernético, el ciberacoso y la violencia cibernética basada en imágenes ([24]). Estas formas se corresponden con las descripciones que ofrece la literatura sobre el abuso verbal, psicológico y sexual, así como con la coacción y los ataques a la reputación que suelen sufrir las chicas en su vida en línea. Las participantes describieron de forma sistemática los espacios digitales como hostiles e inseguros. Muchas hablaron abiertamente de sus experiencias personales de abuso, mientras que otras describieron incidentes que afectaban a sus compañeras.

Ciberacoso (sexual)

La violencia y la explotación sexuales se revelaron como las formas de ciberviolencia más citadas en todos los Estados miembros y grupos de edad. Las participantes informaron de que recibían contenido sexual no solicitado y se enfrentaban a comportamientos depredadores en línea. Entre los ejemplos se incluían recibir imágenes sexuales explícitas a través de Snapchat y encontrarse con hombres en plataformas como Omegle ([25]) que se exhibían de forma repentina durante conversaciones informales. Las participantes también mencionaron que les añadían cuentas con nombres de usuario sexualmente explícitos, como «Cachonda en [ciudad]» ([26]) o «enviando desnudos», lo que describieron como una parte normalizada y habitual de sus interacciones en línea. Algunas participantes relataron haber sufrido acoso por parte de hombres mayores que restaban importancia a su edad con frases como «no pasa nada, no me importa» cuando la joven revelaba que era menor de edad. Otras describieron un acoso persistente a pesar de haber bloqueado repetidamente a los agresores, quienes creaban múltiples cuentas falsas para seguir en contacto con ellas.

24 Véase la tabla A.5 del anexo para conocer ejemplos concretos de los tipos de ciberviolencia sufridos por las niñas como víctimas y testigos.

25 Omegle, una plataforma de chat en línea gratuita que conectaba a los usuarios de forma anónima, cerró en noviembre de 2023. La plataforma se enfrentó a un escrutinio cada vez mayor por su papel a la hora de facilitar interacciones perjudiciales, incluida la explotación y el abuso sexuales. Para más información, consulte https://www.bbc.com/news/business-67364634.

26 Se ha omitido el nombre de la ciudad para proteger la privacidad y el anonimato de las participantes.

> **Había un tipo que, por su perfil, parecía un hombre mayor que le enviaba mensajes a una chica porque ella tenía un perfil de Instagram, y él no paraba de mandarle mensajes provocativos, pidiéndole que le enviara fotos de ella en ropa interior o incluso sin [ropa interior], quizá en ciertas posturas, no precisamente las más adecuadas. Y cada vez que ella lo bloqueaba, él se creaba otros perfiles y seguía escribiéndole, así que no aceptaba el rechazo.**
>
> **(NIÑA DE 13 A 15 AÑOS, ITALIA)**

Acoso cibernético y coacción

El acoso cibernético y la coacción también fueron temas recurrentes, y las chicas describieron contactos en línea no deseados y persistentes. En Suecia, las participantes señalaron que las peticiones de fotos solían aparecer al principio de las conversaciones y se intensificaban hasta convertirse en presión para que enviaran fotos. En Italia, las chicas describieron cómo hombres mayores eludían los bloqueos con perfiles falsos y casos de chantaje emocional, como exparejas que amenazaban con suicidarse para manipular a las chicas y que mantuvieran el contacto.

Algunas participantes describieron situaciones de coacción que implicaban tácticas perturbadoras, como el envío de imágenes de autolesiones para obligarlas a ceder.

> **Creo que todos nos hemos fijado, ya sea en TikTok o en Instagram, en una chica que ha publicado fotos y ahora hay mensajes que puedes escribir a alguien cuando publica una historia, que son anónimos, y lo que la gente le escribe en esos mensajes es muy desagradable y tiene un contenido muy repugnante.**
>
> **(CHICA DE 16 A 18 AÑOS, CHIPRE)**

Ciberacoso (incluido el acoso cibernético)

Las participantes describieron el ciberacoso y la exclusión social como esfuerzos deliberados por aislar, avergonzar o humillar a las víctimas, a menudo en redes de compañeros. Esto incluía la exclusión de chats grupales, los chismes dirigidos a personas concretas y la creación de grupos en línea para ridiculizar a individuos específicos. Se mencionaron los mensajes anónimos en plataformas como Instagram y TikTok como un vector habitual de abuso.

> **Creo que todos nos hemos fijado, ya sea en TikTok o en Instagram, en una chica que ha publicado fotos y ahora hay mensajes que puedes escribir a alguien cuando publica una historia, que son anónimos, y lo que la gente le escribe en esos mensajes es muy desagradable y tiene un contenido muy repugnante.**
>
> **(CHICA DE 16 A 18 AÑOS, CHIPRE)**

Ciberviolencia basada en imágenes

La creación, el intercambio o la manipulación sin consentimiento de imágenes íntimas se señaló como una forma generalizada y especialmente dañina de ciberviolencia. Los participantes describieron incidentes relacionados con «deepnudes» /

imágenes íntimas sintéticas sin consentimiento, la grabación secreta de momentos íntimos y el chantaje basado en imágenes, incluso por parte de participantes de grupos de edad más jóvenes.

> **Ella no quería salir con él ni tener una relación, y él, literalmente, creó un deepfake de ella y empezó a difundirlo por todo el colegio.**
>
> **(CHICA DE 13 A 15 AÑOS, POLONIA)**

Una chica descubrió que su expareja la había fotografiado a escondidas durante momentos íntimos, lo que la dejó aterrorizada ante la posibilidad de que las imágenes volvieran a salir a la luz.

> **Estaba con un chico del que más tarde descubrí que me había hecho una foto mientras teníamos relaciones sexuales. No la ha compartido, pero sigo pensando: «que se la quede, que se la quede». Da miedo saber que está ahí, porque, aunque la haya borrado, podría seguir teniéndola en su móvil.**
>
> **(CHICA DE 13 A 15 AÑOS, SUECIA)**

Otra recordó un caso de abuso y chantaje con imágenes que le ocurrió en la escuela primaria.

> **Tenía una compañera de clase en primaria... y alguien le hizo una foto, y fue muy vergonzoso; él la amenazaba con publicarla si ella no le enviaba los deberes o no le ayudaba con los exámenes y cosas así, o incluso a veces le pedía dinero.**
>
> **(NIÑA DE 13 A 15 AÑOS, CHIPRE)**

3.1. Dónde y cómo se produce la ciberviolencia: roles e interacciones e es

Las chicas que participaron en el estudio describieron haber sufrido o presenciado ciberviolencia en una amplia variedad de plataformas digitales (Tabla 1). Destacaron que el abuso no se limitaba a un único sitio web o aplicación, sino que se adaptaba a las características técnicas, las culturas y las normas de cada plataforma. En otras palabras, el tipo de violencia sufrida solía venir determinado por las posibilidades que ofrecía la plataforma, ya fuera el anonimato, el intercambio de imágenes, la mensajería privada o las interacciones en tiempo real.

Tabla 1 | Formas de ciberviolencia asociadas a diferentes plataformas digitales según los participantes en los grupos focales

Plataforma	Descripción de la plataforma	Formas de violencia
Instagram	Plataforma de redes sociales centrada en compartir fotos y vídeos, incluyendo historias y carretes.	Acoso a través de mensajes directos; divulgación de fotos privadas; páginas de odio.
Snapchat	Aplicación de mensajería multimedia conocida por los mensajes que desaparecen, los filtros y los vídeos cortos.	Fotos íntimas no solicitadas; deepfakes; cuentas de exposición; amenazas de suicidio; ofertas de dinero a cambio de fotos por parte de hombres desconocidos.
TikTok	Plataforma de redes sociales centrada en la creación y el intercambio de vídeos cortos, popular por sus tendencias y su contenido musical.	Grooming; memes y comentarios sexistas; contenido pornográfico en los comentarios; solicitudes de «sugar baby» [*].
Discord	Plataforma de comunicación diseñada para chats de voz, vídeo y texto, utilizada a menudo por comunidades de videojuegos y de intereses específicos.	Acoso por parte de adultos; manipulación emocional; peticiones de fotos desnudas.
Omegle	Página web de chat en línea que empareja aleatoriamente a los usuarios para mantener conversaciones anónimas de texto o vídeo.	Exhibicionismo sexual repetido; interacciones sexuales coercitivas a través del chat.
Plataformas de videojuegos (p. ej., Valorant)	Plataformas interactivas en las que los usuarios juegan a videojuegos multijugador en línea, a menudo con chat de voz o de texto y elementos competitivos.	Abuso sexista en el chat de voz; menosprecio constante hacia las chicas.
Mensajería /chats	Aplicaciones de mensajería instantánea utilizadas para la comunicación en tiempo real mediante texto, voz y vídeo.	Grupos de acoso; contenido generado por IA para burlarse.
YouTube Kids	Aplicación de streaming de vídeo que ofrece contenido seleccionado y adecuado a la edad de los niños, con controles parentales y contenido educativo.	Contenido inapropiado camuflado como vídeos aptos para niños.

[*] Las solicitudes de «sugar baby» se refieren a situaciones en las que determinadas personas —a menudo hombres adultos— se acercan a chicas o mujeres más jóvenes ofreciéndoles apoyo económico y material a cambio de atención o favores sexuales. DM; mensajes directos.

Fuente: Autores, basado en debates de grupos focales.

Se destacaron plataformas como Instagram, TikTok, Snapchat y WhatsApp como los principales espacios donde se produce la ciberviolencia, desde el acoso y el bullying hasta el abuso verbal y el intercambio no consentido de imágenes íntimas. Las participantes también señalaron que el diseño de cada plataforma influye en los riesgos a los que se enfrentan, como las secciones de comentarios públicos de TikTok, los mensajes que desaparecen de Snapchat y los chats de grupo de WhatsApp, que se utilizan para cotillear o excluir a otras personas.

Incluso características de las plataformas como los emojis, las cuentas falsas y las funciones de comentarios se consideraban herramientas que podían utilizarse para el acoso y la intimidación. Las chicas también expresaron su preocupación por los riesgos derivados de los algoritmos, en particular el auge de los «deepfakes» generados por IA y los contenidos manipulados que refuerzan las normas sexistas y violentas.

En Instagram, las chicas denunciaron haber recibido mensajes de acoso a través de los mensajes directos, haber sido blanco de páginas de odio y que se hubieran compartido fotos privadas sin su consentimiento. Snapchat se describió como un espacio en el que circulaban ampliamente desnudos no solicitados e imágenes deepfake, a veces a través de cuentas de exposición ([27]). Algunas participantes también relataron haber sido presionadas con amenazas de autolesión por parte de los agresores —como amenazas de suicidio— como forma de presión o manipulación vinculada al abuso basado en imágenes.

TikTok se asoció con una cultura de sexismo normalizado. Se citaron como habituales los comportamientos de captación, los memes que ridiculizan el cuerpo y las tendencias sexualizadas, junto con comentarios que cosificaban o humillaban a las chicas. Algunas chicas describieron haber recibido propuestas para acuerdos de «sugar baby–sugar daddy», lo que sugiere que las formas comerciales de explotación sexual estaban llegando a un público más joven a través de la plataforma.
También se expresó preocupación por la falta de una normativa estricta en algunas plataformas de redes sociales.

En otras plataformas, como Discord, las chicas describieron haber sido manipuladas emocionalmente por usuarios mayores mediante la captación y la presión persistente para que enviaran desnudos. Se consideró que las funciones de chat privado y grupal de la plataforma facilitaban interacciones prolongadas y coercitivas, a menudo bajo el pretexto de intereses compartidos por los videojuegos o la pertenencia a una comunidad. Además, Omegle fue descrito como un espacio de exposición sexual constante. Las chicas
relataron haber sido víctimas de exhibicionismo o coaccionadas para mantener conversaciones inapropiadas por parte de desconocidos, que a menudo eran adultos.

> **Ya había estado en este Omegle con mis amigas durante una noche de pijamas... Me puse en contacto con un chico así. Le dije: «Hola», «¿De dónde eres?», charlamos un rato y, de repente, le pregunté: «Espera, ¿qué estás haciendo?»... Y me enseñó sus [genitales]. ¡Esto pasa todo el tiempo!**
>
> **(NIÑA DE 13 A 15 AÑOS, POLONIA)**

También se constató que otras aplicaciones de mensajería privada, como Messenger, eran escenario de acoso; las participantes describieron chats grupales que existían únicamente para acosar a las chicas y la difusión de contenido generado por IA diseñado para burlarse de ellas o intimidarlas. Ni siquiera las plataformas diseñadas específicamente para niños se libraron de ello. En YouTube Kids, las chicas describieron haber encontrado vídeos inapropiados o sexualizados disfrazados de contenido apto para niños, lo que las exponía a contenido nocivo a una edad muy temprana.

Por su parte, los entornos de videojuegos en línea exponían a las chicas a un sexismo explícito en sus chats de voz. Las chicas contaron que les decían que «volvieran a la cocina» o que se les menospreciaba independientemente de su rendimiento en el juego. Estas experiencias ilustran cómo la hostilidad de género sigue profundamente arraigada en la cultura de los videojuegos.

27 Las cuentas de exposición son perfiles en redes sociales —a menudo anónimos o no oficiales— que se crean y utilizan específicamente para compartir públicamente contenido personal, privado o sensible sobre personas, normalmente sin su consentimiento.

Perfiles de los agresores y relación con ellos

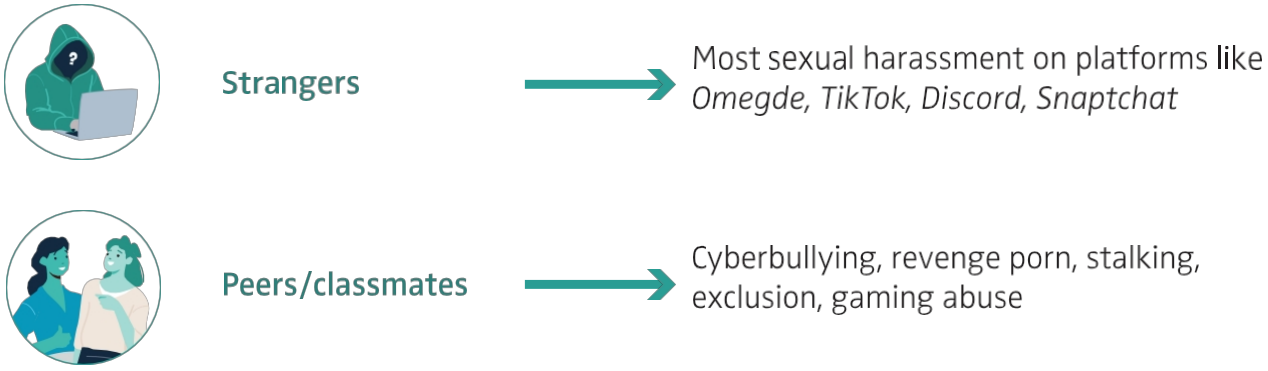
A diferencia de las formas de violencia de género fuera de línea, la ciberviolencia contra las mujeres y las niñas puede involucrar a un abanico más amplio y diverso de autores (Figura 8). Esto se debe en gran medida a la facilidad con la que las personas pueden participar en el abuso en línea y amplificar sus efectos nocivos (ONU Mujeres, 2024b). En este contexto, existen dos tipos principales de autores: los autores primarios y los autores secundarios (ONU Mujeres, 2024b). Los autores primarios son aquellos que inician e incitan a cometer actos de violencia de género en línea. Son responsables de dar inicio a las acciones o contenidos nocivos, ya sea mediante acoso, amenazas o violencia explícita. Los autores secundarios, por su parte, son personas que contribuyen a la difusión de la ciberviolencia contra las mujeres y las niñas al descargar, reenviar o compartir contenidos abusivos, amplificando así su alcance e impacto.

El Lobby Europeo de las Mujeres propone una lista de diferentes tipos de agresores en línea ([28]). Los agresores pueden ser desconocidos para la víctima, o bien personas de su entorno personal o profesional, como familiares, amigos o compañeros de trabajo. Un metaanálisis global sobre los autores de delitos en línea contra menores estima que, en general, el 68 % de todos los agresores eran familiares o conocidos de la víctima. Además, el 44 % de los autores eran menores de 18 años, lo que sugiere una gran proporción de violencia entre iguales (Sutton et al., 2023). Grupos más peligrosos y organizados, como los depredadores sexuales, los traficantes, las redes de pedofilia y las organizaciones criminales transnacionales, también se encuentran entre las categorías más significativas de autores en los casos de ciberviolencia contra las mujeres y las niñas (EWL, 2017).

Aunque los actos de ciberviolencia se producen en línea, las motivaciones subyacentes a estas acciones provienen del mundo fuera de Internet, influidas por factores emocionales, psicológicos, ideológicos y culturales que determinan el perfil y el comportamiento del agresor (Cybersafe, 2020). Muchos jóvenes (de entre 12 y 18 años) suelen percibir a los autores como víctimas a su vez, describiéndolos como personas solitarias, débiles o que también sufren violencia. Las dinámicas familiares y relacionales —incluidos el control y la supervisión de los padres, así como los conflictos y el apoyo familiares— también desempeñan un papel significativo a la hora de determinar la comisión de actos de ciberviolencia entre los jóvenes (López-Castro et al., 2019).

Los debates en grupos focales celebrados en los Estados miembros participantes ilustran cómo se viven estas dinámicas en la práctica.

FIGURA 7 | Autores y formas asociadas de ciberviolencia, según los participantes en los grupos focales



28 Véase la tabla A.8 del anexo.

Current/former intimate partners → Grooming, coercive control, sharing private material after breakups, threats

Friends/ former friends → Betrayal, spreading rumours, participation in mocking chats

Older men (often unknown) → Grooming, sexual coercion, deepfake distribution, 'sugar daddy' offers

Durante los grupos focales, las niñas destacaron de forma sistemática que la ciberviolencia suele tener su origen en sus círculos sociales o en sus relaciones íntimas. El ciberacoso y la exclusión social suelen involucrar a compañeros de clase o a otros jóvenes de su misma edad, lo que coincide con los resultados del estudio HBSC sobre la perpetración por parte de los compañeros. Según la encuesta HBSC, la perpetración
del ciberacoso alcanza su punto álgido a los 13 años, tanto en el caso de los chicos como de las chicas, en la mayoría de los Estados miembros y regiones de la UE ([29]). En el contexto de los grupos de compañeros, las normas y actitudes de estos influyen en gran medida en las acciones. El poder, la popularidad, el estatus y las nociones percibidas de masculinidad surgen como posibles motivaciones para participar en comportamientos dañinos en línea (Proyecto deSHAME, 2017).

Las relaciones íntimas también se revelaron como un contexto central en el que se produce la ciberviolencia: las chicas describieron experiencias de abuso basado en imágenes, coacción y ciberacoso por parte de parejas sentimentales o exparejas. Estos casos ilustran cómo los agresores se aprovechan de la confianza y la intimidad para acceder a material privado o para ejercer un control continuo.

> **"La persona con la que tienes una relación tiene un comportamiento que a ti, como persona, no te gusta; rompes con ella y, aun así, sigue escribiéndote y bombardeándote con mensajes. No acepta que se haya acabado y sigue acosándote. O se hace la víctima e intenta manipularte para que sigas en la relación."**
>
> **(CHICA DE 16 A 18 AÑOS, RUMANÍA)**

3.2. El carácter generalizado y normalizado de la violencia cibernética

Las chicas describieron sistemáticamente la ciberviolencia como un fenómeno generalizado e ineludible, lo que concuerda con los estudios que demuestran su exposición desproporcionada al abuso en línea. En lugar de considerar la ciberviolencia como un incidente aislado, las chicas la describieron como un aspecto generalizado y habitual de sus vidas digitales. Muchas chicas afirmaron que casi todas las chicas que conocían habían sufrido algún tipo de abuso en línea. Las secciones de comentarios, los chats grupales y los mensajes directos se describieron como espacios inseguros donde el odio, las burlas y los juicios eran habituales. El anonimato de los espacios en línea se mencionó con frecuencia como un factor que envalentona a los agresores y permite que se produzcan comportamientos dañinos sin consecuencias.

29 Véanse las figuras A.13 y A.14 del anexo.

Las conclusiones de los grupos focales también revelaron una percepción compartida de que las niñas son objeto de de la ciberviolencia que los chicos. Las chicas describieron el acoso sexualizado, los insultos relacionados con el aspecto físico, el abuso basado en imágenes y la exclusión social como formas de abuso especialmente relacionadas con el género. Aunque las chicas reconocieron que otras chicas también pueden causar daño —especialmente a través de la exclusión, las burlas o los juicios de valor—, dejaron claro que los chicos eran con mayor frecuencia los responsables de las formas graves de abuso, como la coacción o la difusión de imágenes íntimas.

La forma en que los compañeros reaccionan ante estos incidentes agrava aún más el daño. La culpabilización de la víctima desempeña un papel clave en la forma en que los jóvenes responden a estas formas de abuso. Las chicas temen que se les culpe por enviar imágenes o vídeos íntimos, por ejemplo, lo que puede impedirles buscar ayuda o denunciar el abuso. Este miedo al juicio ajeno puede verse agravado por factores psicológicos como la autoculpabilidad, la preocupación por la reputación y la vergüenza (Mclocklin et al., 2024).

Intersecciones entre el mundo digital y el real en la ciberviolencia

La ciberviolencia rara vez se limita a los espacios digitales. Las niñas describieron una difuminación de los límites entre los mundos en línea y fuera de línea, donde el acoso, las amenazas y el daño a la reputación que se originan en Internet con frecuencia se intensifican en situaciones de la vida real o viceversa. A este respecto, las investigaciones existentes sugieren que, para los niños y niñas, las experiencias de ciberviolencia suelen estar estrechamente vinculadas al acoso fuera de línea, especialmente en el ámbito escolar (Chiang et al., 2021).

Este solapamiento entre los espacios digitales y físicos también quedó patente en los relatos de las niñas, en los que la ciberviolencia se describía como un continuo que se desplaza sin fisuras entre plataformas, relaciones y entornos. Compartieron muchos ejemplos de abusos en línea que conducían directamente a daños en la vida real, como el seguimiento digital que degeneraba en acoso físico.

> **Conozco a alguien que había salido con un grupo de amigos y un amigo de su novio no paraba de escribirle. Y cuando ella le dijo: «No me interesa que seamos más que amigos», él siguió insistiendo. Y ella le dijo: «Te voy a bloquear y no vuelvas a dirigirme la palabra». Y el chico llegó incluso a ir a tirarle piedras a la ventana por la noche.**
>
> **(CHICA DE 16 A 18 AÑOS, RUMANÍA)**

También describieron cómo la violencia fuera de Internet se traslada a los espacios digitales. Las chicas relataron situaciones en las que los agresores, tras cometer acoso o actos de violencia cara a cara, continuaban con el acoso a través de las redes sociales o las plataformas de mensajería.

> **Y entonces decidió empezar a publicar vídeos en TikTok... algunas personas de su colegio la encontraron y le escribían comentarios negativos constantemente, y se hizo viral y todo el mundo empezó a burlarse de ella.**
>
> **(NIÑA DE 13 A 15 AÑOS, CHIPRE)**

En otros casos, las interacciones en línea sentaron inicialmente las bases para que se produjeran daños en la vida real, como el acoso prolongado y el acecho.

> **Todo fue bien durante unos meses, pero luego mi amiga tuvo muchos problemas y tuvo que acudir a terapia y ver a un psiquiatra porque este chico hacía cualquier cosa para recuperarla: la acosaba, le enviaba mensajes e intentaba privarla de todo.**
>
> **(CHICA DE 16 A 18 AÑOS, ITALIA)**

La superposición entre el ámbito digital y el offline también es evidente en los casos de manipulación emocional, en los que el abuso en línea se extendía a la vida cotidiana de las víctimas y alteraba sus rutinas.

> **Solía decirme: «Bueno, si no me respondes, ¿me voy a suicidar?», y es que él estaba en una zona horaria diferente, así que a menudo me quedaba despierta toda la noche para hablar con él, porque no quería que se suicidara.**
>
> **(NIÑA DE 13 A 15 AÑOS, POLONIA)**

Estos testimonios ilustran que los jóvenes no perciben la vida en línea y fuera de línea como espacios separados, sino como espacios interconectados, en los que las formas de violencia en línea y fuera de línea están profundamente entrelazadas.

3.3. Perspectivas de los jóvenes sobre los riesgos interseccionales en la violencia ciber

Las conclusiones cualitativas extraídas de los grupos focales revelan las realidades cotidianas de la ciberviolencia y los contextos sociales que dan forma a estas experiencias. Las conversaciones tanto con chicas como con chicos pusieron de relieve cómo los factores de identidad individual, junto con dinámicas sociales, estructurales y culturales más amplias, contribuyen de manera significativa a su exposición al abuso en línea y a sus experiencias al respecto. Estas experiencias vividas se hacen eco de los hallazgos de la bibliografía existente, que muestran que la edad, el género y otras vulnerabilidades sociales que se entrecruzan desempeñan un papel importante en las experiencias de ciberviolencia de las chicas.

Factores individuales o basados en la identidad

Los participantes en los grupos focales demostraron una comprensión profunda y matizada de cómo las características personales —como la raza, el género, la discapacidad, la apariencia, la religión y la edad— interactúan con las expectativas y normas sociales para aumentar su riesgo de exposición al abuso en línea.

Muchas describieron cómo los espacios en línea reproducen el sexismo del mundo real, reforzando los sistemas patriarcales que menosprecian y cosifican a las mujeres y las niñas. La publicación de contenido personal, especialmente imágenes en las que se muestra el cuerpo o aquellas que no se ajustan a los cánones de belleza convencionales, se relacionaba con frecuencia con un mayor riesgo de recibir comentarios negativos o sexualizados. Sin embargo, según las niñas, el mero hecho de ser visibles o estar activas en las redes sociales suele atraer atención no deseada y críticas.

Por ejemplo, se consideraba que las niñas que no cumplían con los cánones tradicionales de atractivo o que destacaban físicamente eran objetivos más probables de la humillación y la cosificación en línea. Varias niñas señalaron que

aquellas que «destacan entre la multitud son más propensas a recibir odio». En este contexto, los cánones de belleza perpetuados en Internet —que a menudo privilegian la delgadez y la piel blanca— conducen a la estigmatización y al acoso de quienes no se ajustan a ellos (Azzarito et al., 2017).

> **Las mujeres no son una minoría, pero siguen siendo discriminadas por diversas razones, y esto se refleja en Internet.**
>
> **(CHICA DE 16 A 18 AÑOS, ITALIA)**

> **Tengo amigas... que, por ejemplo, tienen fotos en bañador. Y basta con una sola foto de ese tipo para que tenga la impresión de que los hombres se sienten con derecho a escribirles.**
>
> **(CHICA DE 16 A 18 AÑOS, POLONIA)**

Se consideró que las chicas más jóvenes, especialmente las que se encuentran en los primeros años de la adolescencia, corren un riesgo especial debido a su limitada experiencia, su menor alfabetización digital y su mayor susceptibilidad a la influencia de sus compañeros o a la captación.

Las chicas también destacaron cómo la discriminación basada en la identidad —como la condición LGBTIQ+— agrava el riesgo. Por ejemplo, una participante señaló que las personas transgénero, en particular las mujeres trans, suelen enfrentarse a la deslegitimación y la exclusión.

> **A las personas transgénero se las suele tratar de forma diferente... se les dice «no eres una mujer de verdad».**
>
> **(NIÑA DE 16 A 18 AÑOS, ALEMANIA)**

Esta observación se ve respaldada por investigaciones que muestran que las minorías de género dentro de las comunidades LGBTIQ+ suelen sufrir estigmatización y acoso, y que la ciberviolencia se entrecruza con el abuso racista, anti-LGBTIQ+ y transfóbico (Gius, 2023). Las minorías de género registran tasas más elevadas de acoso en línea, amenazas y acoso sexual (Gámez-Guadix et al., 2022; Vogler et al., 2023). Más concretamente, las personas no binarias, de género no binario y transgénero se enfrentan a riesgos y retos distintos en comparación con otras minorías, lo que subraya la importancia de una investigación más específica en este ámbito (Ray et al., 2024).

La discapacidad también se señaló como un factor significativo que aumenta la vulnerabilidad. Las chicas comentaron que a menudo se burlan de las discapacidades a través de memes ([30]) o de un humor deshumanizador, y que las personas con discapacidad suelen ser objeto de lástima o menosprecio en Internet. Esto coincide con la conclusión de la FRA (2015) de que las mujeres con discapacidad sufren mayores índices de amenazas y abusos en línea.

30 Un meme es una imagen, un vídeo, un texto u otro tipo de contenido —normalmente humorístico— que se copia y se comparte rápidamente en línea, a menudo con ligeras variaciones. En este contexto, las participantes en los grupos focales se refirieron a los memes creados a partir de imágenes de personas (a menudo tomadas sin su consentimiento o procedentes de contenido privado), que se editan, se les añaden leyendas o se alteran para burlarse, ridiculizar o acosar a la persona y que luego se difunden ampliamente por Internet.

El racismo fue otra cuestión destacada planteada por los participantes en los grupos focales, en particular contra aquellas personas que pueden pertenecer a una minoría racial o étnica en su comunidad o país. También se mencionó la religión como motivo del odio en línea dirigido a las niñas, especialmente a aquellas que expresan visiblemente su fe.

> **Me refiero concretamente a las personas que llevan velo. Reciben mucho odio en Internet; es muy habitual.**
>
> **(NIÑA DE 13 A 15 AÑOS, SUECIA)**

Estas reflexiones ponen de relieve que la exposición a la ciberviolencia no solo viene determinada por el comportamiento individual, sino también por la intersección entre la identidad, la visibilidad y las jerarquías sociales arraigadas.

Los chicos, por su parte, señalaron los rasgos individuales y la posición social como factores que aumentan la exposición de las chicas a la ciberviolencia, sugiriendo que las diferencias en la apariencia, la personalidad, las creencias o el estatus social las convertían en objetivos más probables. Interpretaron los comportamientos de las chicas en Internet —en particular, compartir contenido percibido como provocativo— como una búsqueda de atención o como algo impulsado por una necesidad psicológica de validación.
Por su parte, a los agresores se les solía considerar «fracasados» socialmente marginados, que actuaban por aburrimiento, por venganza o con el deseo de afirmar su dominio. Esto complementa las investigaciones que muestran que las dinámicas entre iguales, la marginación social y los desequilibrios de poder son factores clave del ciberacoso y el acoso (Baas et al., 2013; Proyecto deSHAME, 2017).

Las explicaciones de los chicos sobre la ciberviolencia que afecta a las chicas reflejaban una conciencia de las normas culturales, las actitudes patriarcales y los estereotipos de género. Muchos reconocieron que las figuras sociales y el discurso público promueven la misoginia, creando una cultura que normaliza el dominio masculino y traslada la responsabilidad a las chicas, especialmente en los casos de abuso en línea basado en imágenes. Sin embargo, muchos expresaron actitudes de culpabilización de la víctima, y algunos chicos responsabilizaban a las chicas del abuso, sobre todo cuando publicaban «fotos provocativas». No obstante, una minoría rechazó esta actitud de culpar a la víctima, reconociendo que la responsabilidad recae en los agresores. Las explicaciones y justificaciones de los chicos refuerzan la bibliografía sobre la normalización y el doble rasero, según el cual a menudo se excusa a los agresores masculinos mientras se culpa a las víctimas femeninas, lo que pone de relieve los desequilibrios sistémicos de poder basados en el género (EIGE, 2025).

> **Algunas chicas publican fotos provocativas de sí mismas en Internet, y alguien podría apropiarse de ellas y hacer lo que quiera con ellas, y entonces viene el chantaje y todo lo demás que hemos mencionado antes.**
>
> **(CHICO DE 15 A 18 AÑOS, CHIPRE)**

Los chicos también percibían a las chicas como «blancos más fáciles» debido a suposiciones sobre su sensibilidad emocional o ingenuidad, mientras que las chicas menos visibles socialmente se consideraban menos expuestas al riesgo, lo que vincula la exposición con la visibilidad y la participación social.

Las normas y los estereotipos de género influyen aún más en cómo los chicos viven y responden a la ciberviolencia. El miedo a la exclusión social disuadía a los chicos de alzar la voz, especialmente cuando eran acosados por chicas, y las reacciones de los padres a menudo reforzaban las expectativas de que debían mostrarse duros.

> **Te dirán: «¿Eres un hombre y te importa lo que digan de ti?». Es como si le dijeras a tu padre: «Me ha pegado», y él te respondiera: «Pégale tú también». ¡Así son las cosas!**
>
> **(CHICOS DE 15 A 18 AÑOS, CHIPRE)**

Factores sociales, estructurales y culturales

Más allá de los rasgos individuales, muchas chicas señalaron factores estructurales y culturales más amplios que fomentan un entorno permisivo para la violencia cibernética. Destacaron que esta violencia no es el resultado de acciones aisladas en Internet, sino que está profundamente arraigada en normas sociales que culpan a las chicas por el abuso, mientras que excusan o recompensan a los chicos que lo cometen.

Normas de género y culturales

En todos los grupos de discusión, los chicos destacaron cómo las normas dominantes de masculinidad moldean su comportamiento en línea. Se observó una tendencia clara que muestra que los chicos suelen recurrir a la ciberviolencia para obtener reconocimiento y aprobación social de sus compañeros. Actos como compartir imágenes sin consentimiento o el acoso en grupo se enmarcaban como representaciones destinadas a impresionar a los demás o a ajustarse a las expectativas de los compañeros. En este contexto, se trata a las chicas como «trofeos para presumir ante los amigos» y «haber tenido muchas novias se considera un rasgo de macho alfa,
un hombre fuerte». Estas dinámicas impulsadas por los compañeros reflejan la bibliografía sobre la asunción de riesgos en la adolescencia, las jerarquías sociales y la exposición a interacciones sexualizadas en línea (Proyecto deSHAME, 2017).

Los chicos suelen considerar que poseer o compartir imágenes íntimas es un símbolo de poder y estatus, mientras que las chicas implicadas son objeto de vergüenza. La lógica de las «conquistas sexuales» y la cosificación se identificó como un factor clave del abuso en línea.

Las chicas más jóvenes, especialmente en Suecia, mostraron una conciencia considerable del papel que desempeñan las exigencias de los hombres en la explotación sexual en línea, cuestionando así los discursos que culpan a las víctimas. Esta perspectiva se ajusta estrechamente al enfoque jurídico de Suecia sobre la cuestión, que tipifica como delito la compra de servicios sexuales.

Sexualización y explotación

Las niñas de todos los Estados miembros relacionaron la ciberviolencia con problemas sistémicos más amplios, como la industria de la pornografía y la sexualización precoz de las niñas. La exposición temprana a la pornografía, especialmente cuando se produce en un contexto en el que la educación sexual integral y adecuada a la edad es limitada, puede moldear la percepción que los chicos tienen de las mujeres, a menudo de forma negativa. Esto respalda las pruebas que indican la existencia de factores sistémicos que impulsan el abuso sexual en línea y la exposición de los adolescentes a contenidos sexuales (Smahel et al., 2020).

> **Creo que también se debe en gran medida a Internet que las mujeres sean ahora tan fácilmente accesibles. Solo la pornografía... el hecho de que los chicos la vean a una edad tan temprana da mucho miedo. Y el hecho de que su visión de las mujeres cambie por completo.**
>
> **(NIÑA DE 13 A 15 AÑOS, ALEMANIA)**

Normalización y doble rasero

Un tema recurrente fue la tendencia generalizada a minimizar o restar importancia a los comportamientos nocivos de los chicos en Internet. Los compañeros, los adultos y las instituciones suelen excusar estas acciones achacándolas a la inmadurez o a las bromas, lo que contribuye a una cultura en la que dicha violencia se normaliza cuando la cometen los hombres, pero se considera un problema grave cuando la ejercen las mujeres. Tanto las chicas como los chicos describieron de forma sistemática cómo las chicas que sufren ciberviolencia suelen ser juzgadas, ridiculizadas o consideradas responsables del abuso, mientras que a los chicos se les excusa —o, en algunos casos, incluso se les elogia— por ese comportamiento.

> **Cuando lo hacen los chicos, es como: «Bah, solo se están divirtiendo».**
>
> **(CHICA DE 13 A 15 AÑOS, IRLANDA)**

> **Si un chico comparte una foto, se le considera «guay». Si lo hace una chica, se considera que ha hecho algo malo.**
>
> **(CHICA DE 16 A 18 AÑOS, ITALIA)**

Varias chicas reflexionaron sobre cómo la agresividad de algunos chicos en los espacios en línea puede deberse a la inseguridad, la inmadurez emocional o el miedo al rechazo. En estos casos, la ciberviolencia se percibía no solo como una forma de impresionar a los compañeros, sino también como un medio para ejercer control o enmascarar la vulnerabilidad personal. Otras, sin embargo, describieron tales acciones como deliberadas y maliciosas, especialmente en situaciones relacionadas con rupturas sentimentales o lo que se percibe como rechazo.

Las chicas también destacaron el papel de ciertas subculturas en línea e influencers a la hora de moldear actitudes misóginas. Espacios como los foros «incel» ([31]) se describieron como «cámaras de eco» que canalizan la frustración y la sensación de rechazo de los hombres hacia la hostilidad contra las mujeres, reforzando estereotipos nocivos y legitimando el comportamiento abusivo.

Aunque muchas chicas rechazaron rotundamente la idea de que las víctimas sean responsables de los abusos que sufren, algunas expresaron opiniones más ambivalentes. Estas participantes subrayaron que, aunque las chicas no tienen la culpa, deben ser conscientes de los posibles riesgos. Estas perspectivas ilustran la tensión entre rechazar las narrativas que culpan a las víctimas y el reconocimiento de cómo las normas sociales determinan las percepciones de «riesgo» y responsabilidad.

31 Los foros «incel» son comunidades en línea en las que personas que se identifican como «celibes involuntarios»(incels) comparten sus frustraciones por lo que perciben como su incapacidad para entablar relaciones románticas o sexuales. Estos espacios suelen incluir contenidos que expresan resentimiento y, en algunos casos, opiniones hostiles o misóginas.

Las relaciones como contextos de alto riesgo

Por último, las relaciones románticas e íntimas se identificaron repetidamente como contextos de alto riesgo para la ciberviolencia. Las chicas describieron experiencias que implicaban manipulación emocional, coacción para compartir imágenes íntimas y una traición a la confianza cuando esas imágenes se compartían posteriormente o se utilizaban para chantajearlas. Esta dinámica se ve agravada por la tendencia de algunos jóvenes a interpretar los comportamientos controladores o agresivos en línea como signos de afecto o atención, lo que normaliza inadvertidamente el abuso (Lu et al., 2021). Estas interpretaciones erróneas pueden retrasar la búsqueda de ayuda y contribuir a que no se denuncien todos los casos.

> **También tiene mucho que ver con la manipulación. Hasta qué punto el chico realmente quiere algo de ella y hasta qué punto consigue atraparla en sus garras para luego centrarse únicamente en conseguirlo y, una vez logrado, simplemente la deja de lado.**
>
> **También creo que en una relación la situación empeora o se vuelve más difícil, porque entonces te pones esas «gafas de color de rosa»... y luego está esa confianza total, que hace más difícil darse cuenta de que no es confianza o de que él no se merece esa confianza.**
>
> **(CHICAS DE 16 A 18 AÑOS, ALEMANIA)**

Las chicas explicaron que la confianza y la dependencia emocional dentro de las relaciones pueden hacer que les resulte difícil resistirse a la coacción o reconocer comportamientos dañinos. La violencia en las relaciones se consideraba a menudo «normal», difícil de identificar («estás tan cegada») o excusable. De hecho, existe una percepción contradictoria entre los jóvenes sobre lo que constituye un comportamiento aceptable durante las citas por Internet; algunos consideran que la violencia de pareja facilitada por la tecnología es un «problema de pareja» más que una forma de violencia. Esto se hace eco del debate actual sobre lo que es «normal» y lo que no ([32]).

Las rupturas sentimentales se identificaron con frecuencia como un punto crítico, que a menudo desencadenaba actos de venganza como el intercambio no consentido de imágenes privadas y, a menudo, íntimas, incluidas las generadas por IA; el acoso continuado; o la humillación pública. Estos patrones ponen de relieve cómo el abuso en línea está profundamente ligado al poder, al control y a la imposición de normas de género, incluso —y especialmente— en el seno de las relaciones íntimas.

Perspectivas de los chicos

La dinámica de los grupos de iguales se reveló como un factor central de la ciberviolencia. Los chicos explicaron que participar en el acoso puede elevar la posición social de uno, sobre todo cuando los chicos de alto estatus marcan la pauta del comportamiento abusivo. Esto puede fomentar una «mentalidad de turba» en la que la lealtad al grupo se valora por encima de las relaciones individuales.

Las normas de masculinidad y la presión de grupo se citaron como factores recurrentes del abuso. El acoso en línea —en particular, burlarse de las chicas o compartir imágenes íntimas— se presentaba a menudo como una forma de que los chicos demostraran su dureza, probasen su masculinidad u obtuviesen la aprobación de sus compañeros. Abstenerse de participar en este tipo de comportamientos podía considerarse «menos masculino», lo que convertía la participación en un medio para «demostrar que son más varoniles».

32 Para más información, consulte https://vision.city.ac.uk/news/tech-facilitated-abuse-and-the-new-normal/.

Estas dinámicas se vieron además condicionadas por los dobles raseros de género y la homofobia subyacente. Los participantes señalaron que comportamientos idénticos —como publicar fotos reveladoras— se juzgaban de forma diferente en función del género de la persona. A las chicas se las tachaba de provocativas, mientras que a los chicos se les burlaban o ridiculizaban. Algunos participantes masculinos demostraron ser conscientes de las desigualdades sistémicas más amplias, pero este reconocimiento solía coexistir con actitudes persistentes de culpabilización de la víctima.

> **Bueno, ¿publicas una foto desnudo en Internet y esperas una reacción diferente por parte de la gente?**
>
> **(CHICO DE 15 A 18 AÑOS, CHIPRE)**

En general, los debates revelaron cómo las normas de género profundamente arraigadas, los dobles raseros y los desequilibrios de poder sustentan una cultura en la que se normaliza la ciberviolencia, la responsabilidad recae con frecuencia en las chicas y los agresores apenas rinden cuentas.

3.4. El papel de los testigos y la influencia de los compañeros

Los testigos desempeñan un papel crucial a la hora de reducir el impacto de la violencia cibernética en las víctimas. Se reconoce que la intervención es una estrategia clave para combatir este tipo de violencia y mitigar sus efectos nocivos. Ofrecer apoyo directo, como consolar a las víctimas, puede ayudar a reducir el daño emocional que sufren. El apoyo indirecto, como denunciar los incidentes a las autoridades, puede reducir la prevalencia de contenidos nocivos en línea y fomentar acciones positivas entre los usuarios de Internet (Rudnicki et al., 2023).

A pesar de este potencial, muchos espectadores siguen manteniéndose pasivos cuando se enfrentan al odio en línea. Las investigaciones sobre el ciberacoso revelan que aproximadamente entre el 50 % y el 90 % de los adolescentes han sido, en algún momento, testigos pasivos de ciberacoso, sin intervenir ante este tipo de abuso (Allison et al., 2016). Además, los testigos son más propensos a actuar si sienten una conexión con la víctima y perciben que la situación es segura, lo que les garantiza que no se convertirán ellos mismos en objetivos.

Sin estas condiciones, los espectadores son menos propensos a actuar e incluso pueden contribuir a la propagación de la ciberviolencia.

Domínguez-Hernández et al. (2018) identificaron una serie de factores que influyen en la decisión de los jóvenes espectadores (menores de 20 años) de intervenir en situaciones de ciberacoso ([33]). Entre ellos se incluyen factores contextuales (p. ej., amistades, normas sociales, gravedad del incidente, miedo a las represalias y dinámica de los espectadores) y factores personales (p. ej., empatía, desvinculación moral, autoeficacia y experiencias pasadas). Surgieron temas similares en los grupos focales realizados con chicos, quienes expresaron actitudes complejas, debatieron los dilemas a los que se habían enfrentado y ofrecieron justificaciones sobre su papel como espectadores de la ciberviolencia contra las chicas. Surgieron tres patrones recurrentes: la actitud pasiva y la evasión como forma de autoconservación, las normas de grupo que desalentaban la intervención y la escasa confianza en la eficacia de actuar.

Actitud pasiva y evasión

Muchos chicos se describieron a sí mismos como observadores pasivos, y a menudo optaban por «limitarse a mirar» o grabar los incidentes en lugar de intervenir, especialmente cuando la víctima era una desconocida. El miedo a las represalias o a que la situación se agravara también influyó en la evasión.

33 Las principales conclusiones de su estudio se resumen en la tabla A.9 del anexo.

Los chicos solían expresar la creencia de que las víctimas debían resolver los problemas por sí mismas, sobre todo si no eran amigos cercanos. Estas respuestas sugieren una tendencia a enmarcar la ciberviolencia como un problema personal en lugar de
una responsabilidad colectiva, lo que refuerza los patrones de culpabilización de la víctima. La presión de los compañeros y la dinámica de grupo también influyeron considerablemente en el comportamiento de los espectadores. Muchos participantes temían la exclusión social o el ridículo si actuaban en contra del grupo. Algunos chicos afirmaron ofrecer apoyo discreto —como mensajes privados— en lugar de intervenir públicamente.

> **Si vieras que todos tus compañeros de clase simplemente están viendo esto y no hacen nada, no querrías ser el bicho raro.**
>
> **(CHICO DE 15 A 18 AÑOS, IRLANDA)**

Escasa confianza en la intervención de los testigos

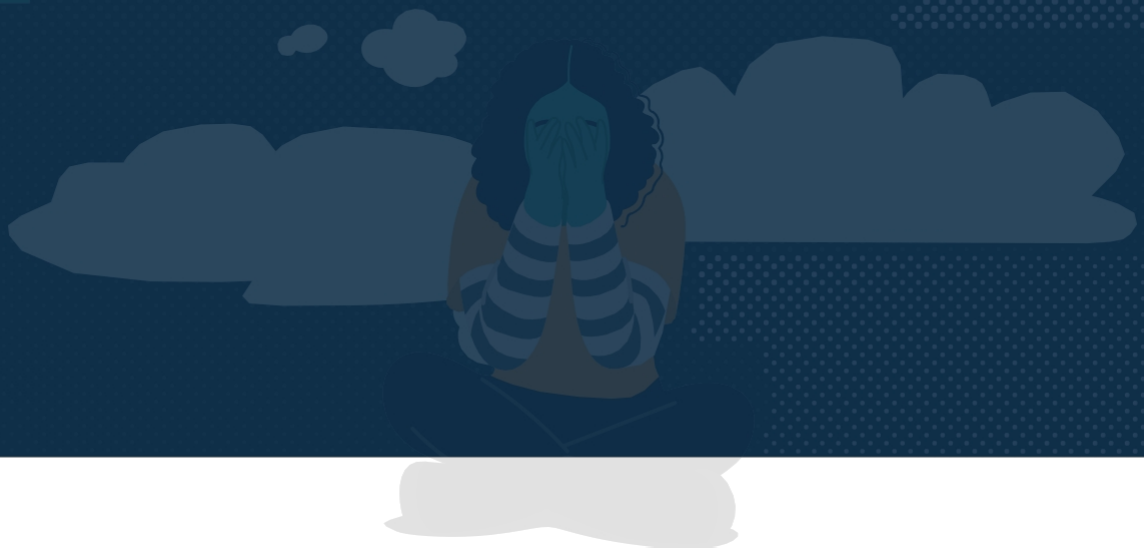
En general, los chicos se mostraron escépticos sobre la eficacia de intervenir para detener la ciberviolencia contra las chicas. Muchos pensaban que tomar partido les expondría a críticas. Otros destacaron la falta de motivación cuando no conocían personalmente a la víctima. Estos resultados se hacen eco de la bibliografía existente sobre el comportamiento de los testigos y la masculinidad en entornos en línea. Las investigaciones muestran que los grupos de compañeros varones suelen desalentar la intervención cuando son testigos de abusos en línea, ya que tomar partido puede amenazar el estatus social o la identidad masculina de uno (Connell, 2005; DeKeseredy et al., 2013). Los estudios sobre la ciberviolencia sugieren además que los entornos digitales amplifican estos riesgos sociales: intervenir contra contenidos sexistas o agresivos puede exponer a los chicos al ridículo o a represalias por parte de sus compañeros (Powell et al., 2017). Además, la evidencia empírica indica que la empatía y la conexión personal con la víctima son motivadores cruciales para la acción de los espectadores;
cuando estas faltan, la probabilidad de que se produzca una intervención ante el ciberacoso o el acoso en línea disminuye significativamente (Barlińska et al., 2013). En conjunto, estos estudios ponen de relieve cómo las normas de los compañeros, el miedo a las repercusiones sociales y la distancia emocional determinan la reticencia de los chicos a intervenir en casos de ciberviolencia contra las chicas.

> **Señorita, ya tengo mis propios problemas, no voy a quedarme aquí ocupándome de los problemas de los demás.**
>
> **(CHICO DE 15 A 18 AÑOS, CHIPRE)**

Varios chicos también creían que las simples peticiones a los compañeros para que dejaran de comportarse así son ineficaces, ya que «la gente no va a hacer caso si solo les dices: “Oh, para” o algo así. Las palabras no sirven de mucho». Sin embargo, algunos participantes reconocieron que la influencia de los compañeros —especialmente de un amigo o de un hermano mayor— podría ser eficaz para disuadir de comportamientos dañinos, sobre todo en una fase temprana.

Algunos chicos también reconocieron el valor potencial de dirigirse a las víctimas en privado. Aunque estas acciones demuestran empatía, también reflejan una reticencia a cuestionar públicamente los comportamientos nocivos.

4 Efectos de la ciberviolencia



4.1. Repercusiones de la ciberviolencia y las dinámicas de « » social

Aunque la ciberviolencia puede afectar a cualquier persona, las mujeres y las niñas se ven afectadas de manera desproporcionada, ya que a menudo sufren formas más graves y traumáticas de violencia que tienen efectos duraderos en su comportamiento, sus emociones, su salud mental, su bienestar físico y sus interacciones sociales. Las consecuencias no difieren de las del acoso, el bullying y el acecho en el mundo real, pero tienen repercusiones negativas más graves (EWL, 2017).

Para las niñas y las mujeres jóvenes, las repercusiones psicológicas de la ciberviolencia contra las mujeres y las niñas son especialmente graves. Las adolescentes víctimas de ciberacoso suelen manifestar depresión, ansiedad y tendencias a la autolesión (Nixon, 2014). Las víctimas más jóvenes suelen manifestar sentimientos de tristeza, desesperanza, ira y miedo; algunos estudios sugieren que el ciberacoso puede resultar incluso más estresante que el acoso tradicional debido al anonimato de los autores y al alcance generalizado de las plataformas en línea (Sourander et al., 2010).

Las diferentes formas de ciberviolencia provocan distintos niveles de daño, siendo los contenidos visuales, como las imágenes y los vídeos, los que causan los efectos psicológicos más graves (Nixon, 2014). El ciberacoso también perturba las relaciones sociales, lo que contribuye al aislamiento, a la pérdida de confianza, a la soledad y a la disminución de la autoestima (Sciacca et al., 2023). Estos retos se ven agravados por la reticencia de las víctimas a denunciar o buscar ayuda, motivada por el miedo al juicio ajeno, la incertidumbre sobre los resultados y las dudas sobre cómo podrían reaccionar los adultos (Project deSHAME, 2017). De hecho, el hecho de que los jóvenes busquen ayuda o intenten manejar la situación por su cuenta
depende de varios factores: si reconocen que el comportamiento es abusivo, si conocen los recursos de apoyo disponibles y si creen que la familia, los centros educativos o las plataformas digitales pueden ayudarles realmente. En la práctica, muchos jóvenes solo piden ayuda después de que el abuso haya causado un daño significativo —emocional, reputacional, físico o económico— (Freed et al., 2025). Otros estudios también han subrayado la necesidad de contar con herramientas y políticas para mitigar los daños de la ciberviolencia y mejorar la búsqueda de ayuda (Janickyj et al., 2025).

Los datos europeos confirman el efecto sobre el bienestar que tiene la mayor exposición de las niñas y las jóvenes a los daños en línea en comparación con los niños y los jóvenes. Como se muestra en la figura A.11 del anexo, en todos los Estados miembros estudiados, excepto Lituania, una proporción significativamente mayor de niñas denuncia haber sufrido daños ([34]), con una diferencia media entre géneros de 19 puntos porcentuales.

34 En el contexto de este proyecto, el término «daño» se refiere al nivel de angustia o malestar experimentado por el niño o adolescente encuestado.

Las tendencias por edades muestran menos coherencia (véase la figura A.12 del anexo). En países como Lituania, Malta y Polonia, los niños de más edad declaran niveles más elevados de daños, mientras que en otros, como Chequia, Estonia, Portugal, Rumanía y Eslovaquia, los niños más pequeños se ven más afectados.

4.2. Las opiniones de los jóvenes sobre las consecuencias de la violencia cibernética

Los debates en grupos focales con niñas confirmaron estas tendencias. Las niñas describieron el impacto de la ciberviolencia utilizando términos cargados de emotividad como «depresión», «suicidio» y «trauma», lo que refleja su conciencia no solo de los daños inmediatos, sino también de las consecuencias emocionales a largo plazo. Los chicos se hicieron eco de estos términos, reconociendo la tristeza, la inseguridad y la desesperación que suelen sentir las víctimas. El miedo al daño a la reputación se reveló como especialmente grave para las niñas y las jóvenes, a quienes con frecuencia se juzga con mayor dureza que a los chicos en situaciones similares (Proyecto deSHAME, 2017).

Malestar emocional y psicológico

El tema más recurrente que surgió de los grupos focales fue el impacto emocional y psicológico de la ciberviolencia. Los participantes describieron la ciberviolencia no solo como algo perjudicial en el momento, sino también como algo que tiene efectos duraderos en la salud mental y las interacciones sociales.

Las niñas expresaban con frecuencia sentimientos de tristeza, miedo, ansiedad, inseguridad y falta de autoestima, especialmente al enfrentarse al acoso, al bullying o al abuso basado en imágenes. El malestar emocional solía verse agravado por la autoculpa y la vergüenza, lo que hacía aún más difícil buscar apoyo o alzar la voz.

> **“Conozco a una chica a la que algunas personas, sobre todo chicos, le enviaban mensajes raros … diciendo que querían ver su cara, y ella, de hecho, les envió fotos de su cara y todo eso, y se sentía muy mal, así que empezó a taparse la cara en todas partes. Esto tuvo un gran impacto en su vida y, al final, la llevó a sufrir depresión y a no poder ir al colegio.”**
>
> **(CHICA DE 16 A 18 AÑOS, CHIPRE)**

Algunas chicas compartieron historias de compañeras que sufrían una angustia grave, incluyendo pensamientos suicidas, autolesiones y depresión, a menudo tras haber sido expuestas públicamente o haber sido objeto de humillación en Internet. El acoso por el aspecto físico, especialmente en lo relativo al peso o la forma corporal, se citó como especialmente dañino, ya que fomenta un escrutinio implacable, a menudo por parte de acosadores anónimos.

Pérdida de confianza y aislamiento social

Otra consecuencia clave de la ciberviolencia identificada por las participantes fue la pérdida de confianza, sobre todo hacia las compañeras, las parejas sentimentales y las comunidades en línea. Las víctimas describieron a menudo un retraimiento emocional y recelo ante futuras interacciones.

La ciberviolencia también puede conducir al aislamiento social y al rechazo por parte de los compañeros. Un participante sugirió que, cuando se comparten imágenes privadas sin consentimiento, la víctima ya no es vista como una persona completa, sino que queda reducida al contenido de esas imágenes. Como resultado, los compañeros pueden distanciarse activamente, lo que refuerza la exclusión.

> **Creo que probablemente acabará reduciéndose solo a eso... y la gente se olvidará de quién es en realidad. Pero entonces solo quedará esto: estas fotos, su cuerpo, y ya no será ella.**
>
> **(CHICA DE 16 A 18 AÑOS, ALEMANIA)**

Exclusión digital

La ciberviolencia puede limitar la participación de las chicas en los espacios digitales sociales y cívicos. El acoso y las reacciones sexistas suelen llevarles a alejarse de los videojuegos en línea, los debates políticos, la creación de contenidos y otros espacios interactivos. En muchos casos, la amenaza de sufrir abusos basta para silenciar sus voces o disuadirlas de participar en los espacios en línea. En algunos casos, las víctimas han llegado a desinstalar aplicaciones o incluso a cambiar de colegio para escapar del acoso.

> **Quieres empezar a jugar, pero no puedes hacerlo porque te encuentras con comentarios sexistas. Solo quieres participar en política, pero te encuentras con... amenazas que te envían directamente a tus redes sociales. Quieres actuar, pero te encuentras con abucheos. Quieres presentarte a las elecciones, pero alguien crea una cuenta para trollearte... La cuestión es si merece la pena. Así que, para mí, todo se reduce a ese intento de excluir.**
>
> **(CHICA DE 16 A 18 AÑOS, POLONIA)**

Normalización de la violencia

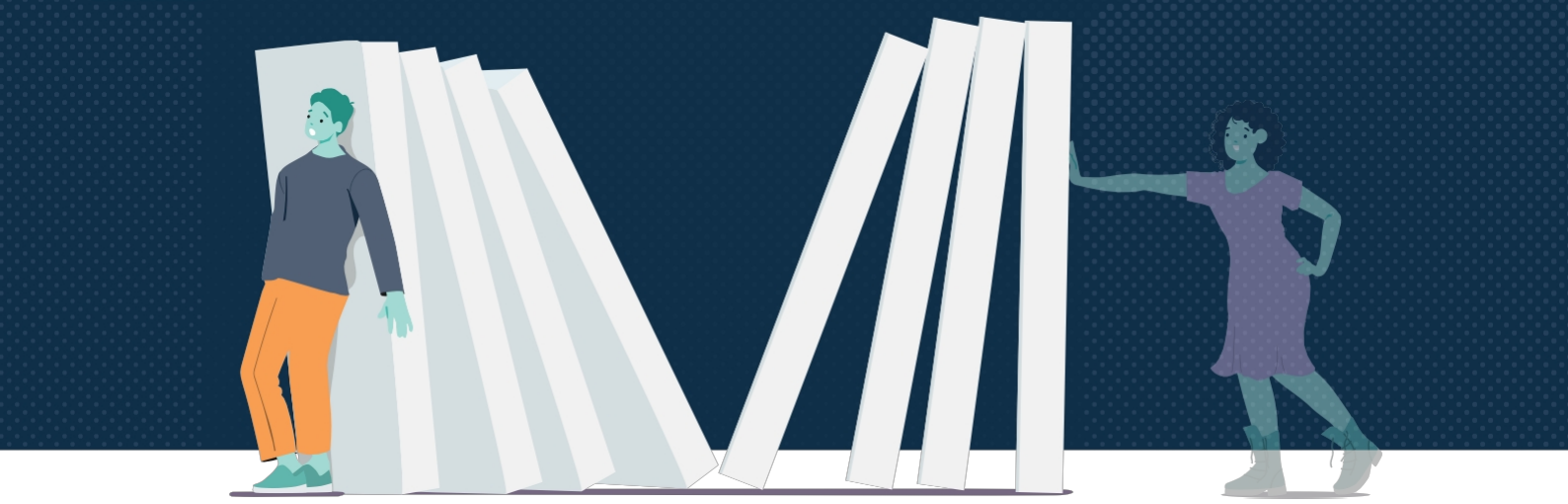
Un impacto sutil, pero significativo, identificado por las participantes de los grupos focales fue la normalización de los comportamientos nocivos. Muchas chicas observaron que la exposición frecuente a la ciberviolencia puede conducir a la desensibilización, lo que reduce la percepción de la gravedad de ciertas formas de abuso, ya que las generaciones más jóvenes aprenden a no «tomárselo tan en serio».

Varias participantes afirmaron haber crecido conscientes de los riesgos tanto en línea como fuera de línea. Recordaron que desde muy pequeñas se les enseñó a ser cautelosas. A pesar de esta concienciación, algunas chicas expresaron una sensación de resignación, al considerar la ciberviolencia como algo inevitable y, por lo tanto, ver la necesidad de adaptarse a esta realidad. Este sentimiento se expresó con fuerza en Bélgica, donde las participantes describieron el ciberacoso como «parte de la vida» y algo de lo que es casi imposible escapar.

> **Sinceramente, no creo que podamos hacer gran cosa. El sistema es así. Para evitarlo, solo tienes que pasar desapercibida y desaparecer. Una vez que se acaba, se acaba. Es una etapa de la vida: la superas y sigues adelante.**
>
> **(NIÑA DE 13 A 15 AÑOS, BÉLGICA)**

La naturaleza persistente del acoso en línea fue otra fuente importante de miedo y ansiedad. Las participantes describieron cómo el contenido perjudicial —como las fotos privadas— puede resurgir en cualquier momento, creando una sensación persistente de vulnerabilidad y amenaza. Señalaron que la misma imagen o mensaje podría reaparecer en otro chat grupal o contexto, lo que les hacía sentir impotentes para evitar volver a quedar expuestas.

5 Prevención y lucha contra la ciberviolencia



5.1. Marcos internacionales y de la UE para abordar la ciberviolencia contra las mujeres y las niñas

Aunque la UE no cuenta con un marco jurídico independiente dedicado exclusivamente a la ciberviolencia de género, entre los avances recientes destaca la adopción de la ya mencionada Directiva (UE) 2024/1385 (Directiva sobre la violencia contra las mujeres), que tipifica como delito cuatro formas principales de ciberviolencia: la difusión no consentida de material íntimo o manipulado, el ciberacoso, el acoso cibernético (incluido el «cyberflashing» ([35])) y la incitación cibernética a la violencia o al odio.

Esta directiva, cuya transposición está prevista para junio de 2027, supone un hito importante en la lucha contra la violencia cibernética: reconoce explícitamente la violencia cibernética como una forma de violencia de género y exige a los Estados miembros que adopten medidas preventivas, desarrollen canales de denuncia accesibles y seguros a través de las TIC, adopten las medidas adecuadas para garantizar la retirada de los contenidos relacionados con el delito, presten servicios especializados de apoyo a las víctimas, faciliten el acceso a la justicia y garanticen la coordinación y la cooperación entre las autoridades. Asimismo, anima a los Estados miembros a garantizar que sus procedimientos nacionales se mantengan al día con los avances tecnológicos. Esta directiva supone un paso histórico, ya que exige a todos los Estados miembros que tipifiquen como delito diversas formas de violencia cibernética.

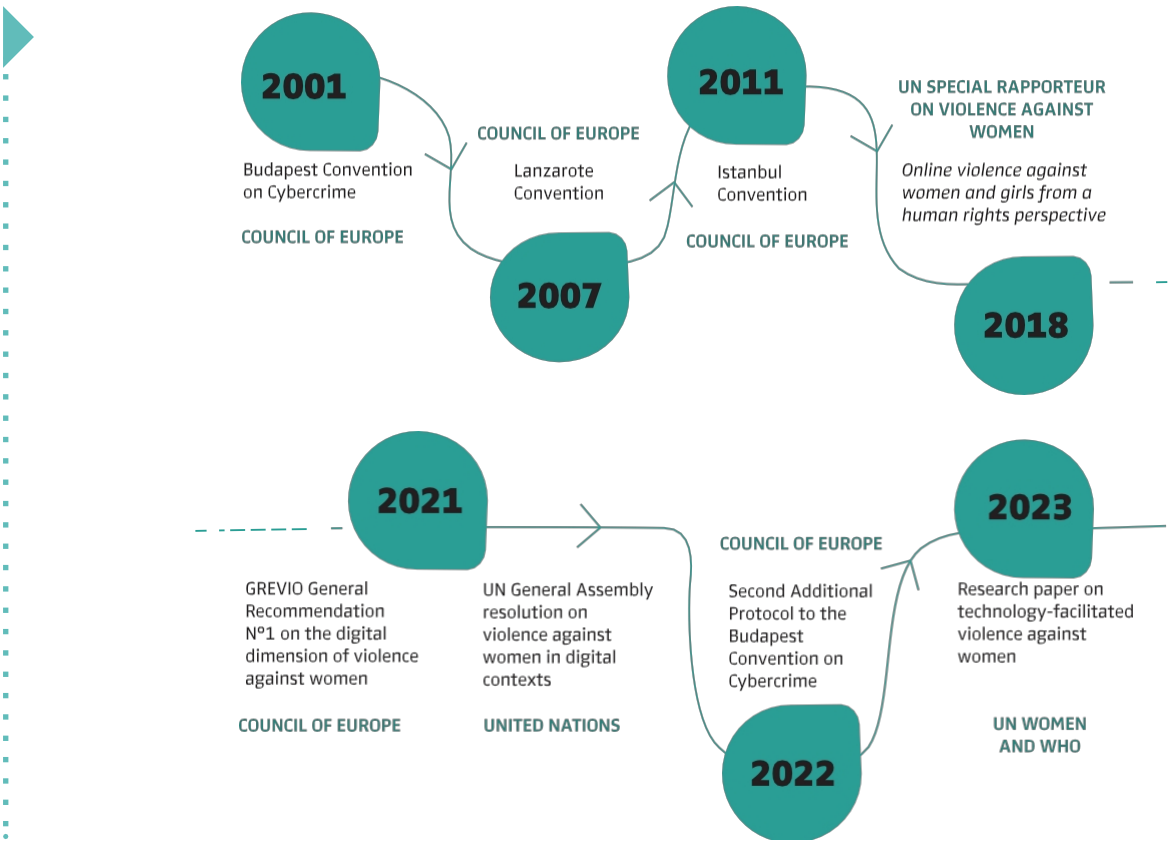
La evolución de la política de la UE refleja una creciente concienciación sobre las vulnerabilidades entrecruzadas de las mujeres y las niñas, que vienen determinadas por factores como la edad, el origen étnico y la situación socioeconómica. En el panorama normativo más amplio de la UE —que abarca la protección de datos, la moderación de contenidos en línea, los mecanismos de apoyo a las víctimas y las estrategias de protección de la infancia—, la Directiva (UE) 2024/1385 constituye el marco central que conecta estas iniciativas, armonizando las medidas en todos los Estados miembros para tipificar como delito y prevenir la ciberviolencia, proteger a las víctimas y promover la rendición de cuentas en línea. Así pues, aunque la legislación de la UE no adopta la forma de un marco único y unificado sobre la ciberviolencia, se ha recurrido a una combinación de mecanismos vinculantes y no vinculantes para abordar la cuestión de manera integral.

35 El «cyberflashing» se define en la directiva como «el envío no solicitado de una imagen, un vídeo u otro material similar en el que se muestren los genitales a una persona» (considerando 24).

5.1.1. Marcos internacionales para abordar la ciberviolencia

A nivel internacional, varios instrumentos clave ([36]) proporcionan normas y orientaciones que han dado forma a las acciones de la UE. Los documentos de las Naciones Unidas, entre ellos el Informe de 2018 de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, relativo a la violencia en línea contra las mujeres y las niñas desde una perspectiva de derechos humanos, y el documento de investigación de 2023 de ONU Mujeres y la OMS sobre la violencia contra las mujeres facilitada por la tecnología, hacen hincapié en la cooperación internacional, la responsabilidad de las plataformas, las soluciones centradas en las víctimas y la inclusión de perspectivas diversas durante la recopilación de pruebas y la elaboración de políticas. El Consejo de Europa ha impulsado marcos normativos relevantes, como el Convenio de Estambul (2011), que aborda explícitamente el abuso en línea; el Convenio de Budapest sobre la Ciberdelincuencia (2001) y su Segundo Protocolo Adicional de 2022, que permiten la cooperación transfronteriza en la persecución de los delitos cibernéticos; y el Convenio de Lanzarote (2007), que protege a los niños de la explotación sexual, incluso en los espacios digitales. Además, la Recomendación General n.º 1 del Grupo de Expertos sobre la Lucha contra la Violencia contra las Mujeres y la Violencia Doméstica (GREVIO) sobre la dimensión digital de la violencia contra las mujeres (2021) destaca la importancia de los planes de acción nacionales, la alfabetización digital y la formación especializada para el personal policial y judicial en materia de ciberviolencia.
En conjunto, estos instrumentos ofrecen orientación para la prevención, la elaboración de políticas y la prestación de servicios de apoyo.

FIGURA 8 | Cronología de ejemplos de los principales instrumentos jurídicos y políticos internacionales que abordan la ciberviolencia



Fuente: Autores.

En noviembre de 2025, el Consejo de Europa aprobó una recomendación sobre la rendición de cuentas por la violencia contra las mujeres y las niñas facilitada por la tecnología ([37]).

36 Véase la figura 9 a continuación. En la tabla A.1 del anexo se ofrecen descripciones detalladas de ejemplos de instrumentos internacionales.
37 «Aprobación de un instrumento clave sobre la rendición de cuentas por la violencia contra las mujeres y las niñas facilitada por la tecnología» – Comisión para la Igualdad de Género.

5.1.2. Evolución de la normativa de la UE en materia de violencia cibernética de género

La UE ha reforzado progresivamente su marco normativo para hacer frente a la ciberviolencia de género, recurriendo a una amplia gama de instrumentos jurídicos y políticos.

El Reglamento General de Protección de Datos (RGPD), adoptado en 2018, ha reforzado los derechos de las personas sobre sus datos personales y ha establecido garantías contra su uso indebido. Asimismo, ha establecido el derecho personal a solicitar la eliminación de contenidos personales perjudiciales o publicados sin consentimiento que hayan aparecido en Internet. Si bien las víctimas de la ciberviolencia han recurrido con frecuencia a la protección basada en la privacidad que ofrece, se ha constatado que los efectos de sus disposiciones a la hora de abordar con éxito las formas de abuso en línea por motivos de género han sido limitados (Dirección General de Servicios de Investigación Parlamentaria del Parlamento Europeo, 2024). Más recientemente, la Ley de Servicios Digitales (DSA) y la Ley de Inteligencia Artificial (2024/1689) han reforzado la seguridad en línea mediante la introducción de normas más estrictas de moderación de contenidos, una mayor protección de las víctimas y requisitos de transparencia en relación con el uso de la IA, incluidas las tecnologías de deepfake. Estos avances demuestran un creciente reconocimiento del problema de la ciberviolencia y de la necesidad de una acción coordinada entre los Estados miembros.

Las medidas de protección de las víctimas son igualmente importantes. La Directiva sobre los derechos de las víctimas (2012/29/UE), actualmente en proceso de revisión, establece normas mínimas para los servicios de apoyo, mientras que la estrategia de la UE sobre los derechos de las víctimas (2020-2025) destaca la necesidad de una mayor protección en los casos de ciberviolencia. Como complemento a ello, la estrategia de igualdad de género (2020-2025) insta explícitamente a combatir la violencia de género en línea.

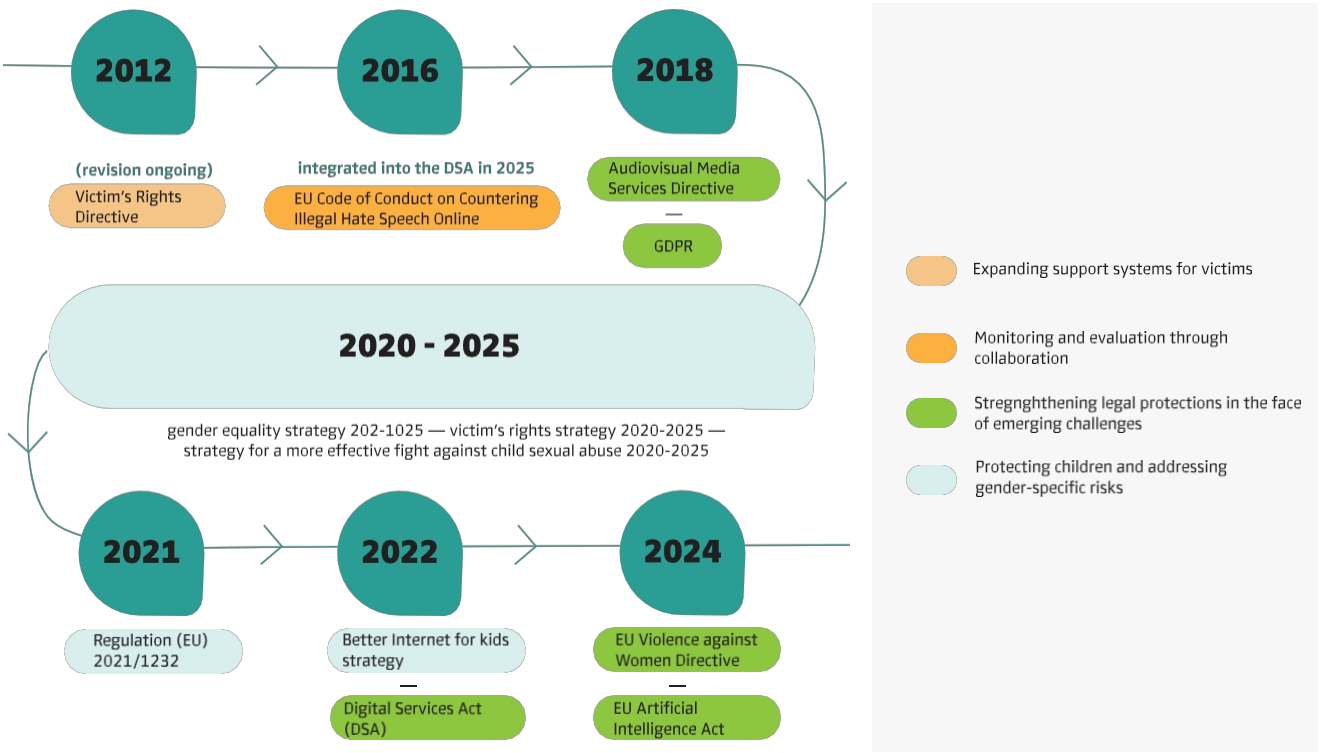
Los instrumentos de protección de la infancia también desempeñan un papel importante. La Directiva (UE) 2011/93 relativa a la lucha contra el abuso sexual y la explotación sexual de los niños y el material de abuso sexual infantil, principal instrumento jurídico
en este ámbito, se encuentra en proceso de revisión para reflejar los avances tecnológicos producidos desde su adopción en 2011 (Dirección General de Servicios de Investigación Parlamentaria del Parlamento Europeo, 2024). El Reglamento (UE) 2021/1232 permite a los proveedores detectar y bloquear el material de abuso sexual infantil, mientras que la estrategia de la UE para una lucha más eficaz contra el abuso sexual infantil (2020-2025) y la estrategia «Un Internet mejor para los niños» refuerzan la seguridad en línea de los menores. El Centro de la UE sobre el abuso sexual infantil propuesto tiene además como objetivo
centralizar los recursos y mejorar la asistencia a las víctimas.

Junto a estos marcos, las iniciativas que abordan el discurso del odio desempeñan un papel importante. El Código de Conducta de la UE de 2016 sobre la lucha contra el discurso de odio ilegal en línea —recientemente integrado en la DSA (en 2025)— refuerza los compromisos adquiridos por las principales plataformas para hacer frente al discurso de odio y adoptar las mejores prácticas. Del mismo modo, la Directiva sobre servicios de medios audiovisuales (2018/1808) incluye disposiciones contra el discurso de odio y mejora las protecciones en los entornos de los medios de comunicación en línea.

La adopción de la Directiva (UE) 2024/1385 (Directiva sobre la violencia contra las mujeres) en 2024 constituye el compromiso legislativo más reciente y significativo para combatir la ciberviolencia contra las mujeres y las niñas. Exige a los Estados miembros que tipifiquen como delito la violencia cibernética mediante el establecimiento de normas mínimas para la tipificación de las cuatro formas principales de violencia cibernética, a saber: la difusión no consentida de material íntimo o manipulado, el acoso cibernético, el hostigamiento cibernético y la incitación cibernética al odio o a la violencia.

Esto deja abierta la posibilidad de que los Estados miembros elaboren normas y sanciones nacionales más estrictas. Es probable que la transposición de la directiva aborde uno de los retos más persistentes a la hora de desarrollar un enfoque a escala de la UE para hacer frente a la violencia cibernética, a saber, la falta de definiciones armonizadas entre los Estados miembros y las jurisdicciones (EIGE, 2025, p. 66). Esto se debe a que también exige a los Estados miembros que recopilen datos sobre estas cuatro formas de ciberviolencia, allanando así el camino hacia la obtención de datos comparables entre los Estados miembros. Para facilitar este proceso, se encomendó específicamente al EIGE la tarea de establecer normas comunes y apoyar a los Estados miembros en la recopilación de datos administrativos comparables y estandarizados (EIGE, 2025).

FIGURA 9 | Cronología de ejemplos de los principales avances normativos de la UE en materia de violencia (cibernética) de género a diciembre de 2025



Fuente: Autores.

5.2. Enfoques nacionales en los Estados miembros

En toda la UE, las respuestas nacionales a la violencia de género y la ciberviolencia varían considerablemente, lo que refleja los diferentes marcos jurídicos, contextos culturales y capacidades tecnológicas de sus Estados miembros. En la mayoría de los Estados miembros, los delitos penales generales —como el acoso y el acecho— abarcan tanto las formas físicas como las digitales de violencia, incluidos el ciberacoso y el ciberacecho. Los precedentes jurídicos han ampliado estas definiciones tradicionales al ámbito en línea. Sin embargo, cuando la violencia cibernética se aborda en el marco de estos delitos generales, a menudo carece de un lenguaje específico de género y rara vez hace referencia explícita a las mujeres.

Aunque son pocos los Estados miembros que cuentan con leyes dirigidas específicamente contra la ciberviolencia hacia las mujeres y las niñas, en muchos de ellos se están llevando a cabo iniciativas legislativas para introducir disposiciones específicas de este tipo. En la mayoría de los casos, las leyes nacionales se basan actualmente en delitos penales generales como el acoso y el bullying, que se complementan con definiciones más amplias y protecciones civiles.

5.2.1. Enfoques jurídicos en la UE

Los Estados miembros han adoptado diferentes enfoques legislativos para abordar la violencia cibernética. Entre ellos se incluyen la creación de leyes específicas sobre violencia cibernética, la integración de delitos específicos del ámbito cibernético en la legislación existente o

la incorporación de medidas de protección en marcos más amplios sobre la privacidad o la violencia contra las mujeres. Muchos Estados miembros combinan estos enfoques, lo que da lugar a sistemas jurídicos mixtos.

El estudio del EIGE de 2022 sobre la lucha contra la ciberviolencia contra las mujeres y las niñas (EIGE, 2022) clasifica los enfoques jurídicos nacionales en tres categorías: los que tratan la ciberviolencia como un delito independiente, como un factor agravante o como parte de delitos generales. También identifica las leyes nacionales que mencionan explícitamente a las mujeres, las niñas o los niños, y examina las políticas nacionales sobre ciberviolencia que incluyen protecciones específicas para estos grupos.

Partiendo de las conclusiones de dicho estudio, se han identificado tres tipos principales de enfoques, tal y como se analiza en las subsecciones siguientes. El análisis revela un cambio proactivo entre los Estados miembros hacia enfoques centrados en las víctimas, la cooperación transfronteriza y la inclusión de la seguridad digital en estrategias más amplias contra la violencia y la ciberdelincuencia. Además, la tabla A.3 del anexo ofrece ejemplos detallados de jurisprudencia nacional relacionada con la ciberviolencia.

ELABORACIÓN DE LEYES ESPECÍFICAS CONTRA LA CIBERVIOLENCIA

Algunos Estados miembros, como Bélgica, Dinamarca, Francia y Portugal, han adoptado leyes o disposiciones independientes que tipifican directamente como delito diferentes formas de ciberviolencia. Entre ellas se incluyen medidas contra el ciberacoso, el acoso en el ámbito escolar y universitario, el abuso sexual basado en imágenes y la difusión no consentida de contenido íntimo. También han introducido obligaciones para que las plataformas en línea eliminen el contenido nocivo, faciliten la denuncia por parte de los usuarios y conserven las pruebas digitales. La tabla 1 contiene ejemplos de este tipo de medidas.

Tabla 2 | Ejemplos de legislación específica sobre la violencia cibernética a nivel nacional

Estado miembro	Nombre de la medida y año	Descripción
Bélgica	Ley destinada a combatir la difusión no consentida de imágenes y grabaciones de carácter sexualmente explícito (4 de mayo de 2020)	La ley amplía las competencias del Instituto para la Igualdad entre Mujeres y Hombres para emprender acciones legales y prestar asistencia a las víctimas adultas de violencia sexual digital, incluidas las víctimas de la difusión no consentida de imágenes, la sextorsión y los «deepnudes». El instituto ofrece asesoramiento y apoyo para la eliminación de imágenes difundidas sin consentimiento. Para ello, colabora con plataformas de Internet como Meta, Google y Pornhub, la plataforma stopncii.org y la policía federal. Otra institución, Child Focus, se encarga de las víctimas menores de edad.

Estado miembro	Nombre de la medida y año	Descripción
Dinamarca	Código Penal danés, artículo 264d	El artículo 264d tipifica como delito la difusión no consentida de imágenes o vídeos íntimos, lo que se castiga con penas de hasta tres años de prisión, con sanciones más severas en los casos en los que haya menores implicados o se produzca una difusión masiva. Aunque es una disposición de carácter neutro en cuanto al género, se centra en los abusos que afectan de manera desproporcionada a las mujeres y las niñas.
	Código Penal danés, artículos 225, 231 y 242	El artículo 225 tipifica como delito la sextorsión, el artículo 231 tipifica como delito la captación de menores con fines sexuales y el artículo 242 tipifica como delito el acoso.
Francia	Ley n.º 2020-766 destinada a combatir los contenidos que incitan al odio en Internet (Ley Avia)	La ley obligaba a las plataformas a eliminar los contenidos ilegales explícitos (por ejemplo, el discurso de odio o la pornografía infantil) en un plazo de 24 horas, con sanciones en caso de incumplimiento. Posteriormente, el Consejo Constitucional declaró inconstitucionales disposiciones clave de la ley, alegando preocupaciones relacionadas con la libertad de expresión. Sus disposiciones restantes dieron lugar a la creación de una fiscalía especializada en el odio en línea y de un Observatorio del Odio en Línea dentro de la Autorité de régulation de la communication audiovisuelle et numérique (Arcom).
	Ley n.º 2022-299 destinada a combatir el acoso escolar	La ley tipifica como delito el acoso escolar y universitario (incluido el ciberacoso), con penas de hasta 150 000 euros de multa y 10 años de prisión. Prevé la recogida y conservación de pruebas digitales en relación con los delitos cibernéticos.
	Ley n.º 2023-566 destinada a establecer una mayoría digital y a combatir el discurso de odio en línea	La ley impone a las plataformas la obligación de facilitar la denuncia de contenidos que vulneren los derechos personales y de proporcionar información preventiva a los usuarios.
	Ley n.º 2024-449 sobre la seguridad y la regulación del espacio digital (Ley SREN)	La ley regula los espacios digitales, centrándose en la protección de los ciudadanos, en particular de los menores, frente a contenidos nocivos y en la lucha contra el acoso cibernético, la sextorsión, las estafas en línea, el odio y la desinformación. La ley introduce un nuevo delito relacionado con los «deepfakes» sexuales. La pena es de dos años de prisión y una multa de 60 000 euros por difundir un «deepfake» sexual públicamente o a un tercero sin el consentimiento de la persona afectada. Las sanciones se elevan a tres años de prisión y una multa de 75 000 euros si se ha publicado utilizando un servicio de comunicación pública en línea. La ley también exige el uso de sistemas de verificación de la edad en los sitios web pornográficos, con sanciones que incluyen multas elevadas y el bloqueo de los sitios web en caso de incumplimiento. Esta ley entró en vigor en junio de 2025 y se aplica a todos los principales sitios web pornográficos.

Estado miembro	Nombre de la medida y año	Descripción
Portugal	Artículo 193 del Código Penal de Portugal, 2023	La Ley n.º 26/2023, de 30 de mayo, modificó el Código Penal de Portugal al modificar el artículo 193 para tipificar como delito la difusión no consentida de imágenes personales a través de los medios de comunicación, Internet u otros medios de difusión pública generalizada. Establece que toda persona que, sin consentimiento, difunda o contribuya a la difusión de imágenes, fotografías o grabaciones que invadan la vida privada de una persona, incluida la intimidad de su vida familiar o sexual, podrá ser castigada con una pena de prisión de hasta cinco años, reforzando así la protección jurídica contra la difusión no consentida de contenido íntimo en línea. La misma ley también modificó el artículo 197 para establecer circunstancias agravantes; las penas por determinados delitos se incrementan en un tercio si el delito se comete a través de las redes sociales, Internet u otros medios de difusión digital de amplio alcance.

AMPLIACIÓN DE LOS CÓDIGOS PENALES VIGENTES PARA ABORDAR LA VIOLENCIA CIBERNÉTICA

Otros Estados miembros han adaptado disposiciones penales preexistentes para abarcar los contextos en línea (véase el cuadro 2). Este es el caso de Estados miembros como Alemania, Irlanda, Italia, Austria, Polonia, Rumanía y Finlandia ([38]). Delitos como el acoso, el hostigamiento, la captación de menores con fines sexuales, la difamación y el discurso de odio se han ampliado para incluir los entornos digitales. Las modificaciones en este ámbito suelen reconocer la violencia cibernética como parte de la violencia de género o la violencia doméstica, lo que permite a los tribunales imponer penas más severas y medidas de protección cuando los casos involucran a parejas íntimas o a menores. Este enfoque proporciona continuidad y coherencia jurídica, pero puede dar lugar a ambigüedades, ya que los delitos no siempre se definen explícitamente como relacionados con el ámbito cibernético, lo que da lugar a una aplicación variable de la ley y a una sensibilidad de género limitada.

Tabla 3 | Ejemplos de legislación nacional ampliada para abarcar la violencia cibernética

Estado miembro	Nombre de la medida y año	Descripción
Bélgica	Artículo 417/8 y artículo 417/9 del Código Penal belga	El Código Penal belga tipifica como delito la creación y la distribución de «deepnudes» sin consentimiento. La creación de un «deepnude» sin el consentimiento de la persona se considera una forma de voyeurismo (artículo 417/8), mientras que la distribución de un «deepnude» constituye la distribución no consentida de contenido de carácter sexual (artículo 417/9 del Código Penal belga).

38 En Finlandia, las disposiciones penales son neutras desde el punto de vista tecnológico; es decir, su aplicación no depende de los medios utilizados.

Estado miembro	Nombre de la medida y año	Descripción
Alemania	Ley de aplicación de la normativa en la red (NetzDG), 2017	Esta ley exige la eliminación rápida de contenidos ilegales de las plataformas de redes sociales ([39]), incluido el discurso de odio, y obliga a dichas plataformas a publicar informes de cumplimiento. También incluye medidas de protección de la infancia y disposiciones contra la desinformación.
	Artículo 176 del Código Penal alemán (Strafgesetzbuch)	Ampliado en 2020, el artículo 176 tipifica como delito el acoso sexual a menores por Internet, incluido el intento de acoso sexual a menores por Internet.
	Reforma de la Ley de Protección de la Juventud (Jugendschutzgesetz), 2021	La ley se reformó para reforzar la protección digital de los menores ([40]).
Irlanda	Ley sobre acoso, comunicaciones nocivas y delitos relacionados, de 2020	También conocida como «Ley de Coco», la ley tipifica como delito los abusos en línea, como el intercambio no consentido de imágenes íntimas y el acoso cibernético. Las relaciones de pareja constituyen un factor agravante a la hora de dictar sentencia.
Italia	Decreto-ley n.º 11/2009	Este decreto introdujo el artículo 612-bis sobre el acoso en el Código de Procedimiento Penal italiano.
	Ley contra el ciberacoso (Ley n.º 71/2017)	La ley aborda el ciberacoso entre los jóvenes y establece la obligatoriedad de contar con programas de prevención en los centros educativos, la retirada de contenidos y servicios de apoyo y rehabilitación tanto para las víctimas como para los autores.
	Ley del «Código Rojo» ([41]), 2019	Esta ley da prioridad a los casos de violencia de género, reconociendo el papel cada vez más importante de las TIC en los casos de acoso y haciendo hincapié en la protección de las víctimas en el ámbito digital.
	Ley contra el «porno vengativo», 2019	Como parte de la legislación del «Código Rojo», esta ley tipifica como delito el intercambio no consentido de imágenes o vídeos íntimos, con penas de hasta seis años de prisión y sanciones más severas en los casos que afecten a menores o a parejas íntimas. Da prioridad a estos casos, así como a otras formas de violencia de género, para agilizar los procedimientos y reducir el trauma de las víctimas, al tiempo que ofrece protecciones como la denuncia anónima, el apoyo psicológico y medidas de protección contra las represalias.

39 La ley exige a las plataformas de redes sociales con más de 2 millones de usuarios que eliminen el contenido «claramente ilegal» en un plazo de 24 horas y todo el contenido ilegal en un plazo de 7 días desde su publicación, con una multa máxima de 50 millones de euros en caso de incumplimiento.

40 «Alemania: Alfabetización mediática y uso seguro de los nuevos medios» – Wiki de la Juventud de la Comisión Europea.

41 La Ley n.º 69/2019 tiene por objeto agilizar los procedimientos judiciales para determinados tipos de delitos que constituyen formas de violencia doméstica y de género.

Estado miembro	Nombre de la medida y año	Descripción
Austria	Artículo 107a del Código Penal austriaco	Este artículo tipifica como delito el acoso cibernético.
	Artículo 107c del Código Penal austriaco	Este artículo se centra en el acoso persistente en línea.
	Ley contra el odio en Internet, de 2021	Este paquete legislativo introdujo medidas para mejorar la situación jurídica de las personas afectadas por la ciberviolencia. Por ejemplo, facilita las demandas civiles contra el odio en línea. A las víctimas de la ciberviolencia se les concede una medida cautelar contra las publicaciones de odio que vulneren su dignidad humana. Dichas publicaciones deben eliminarse de inmediato. Las víctimas del odio en línea también tienen derecho a asistencia psicosocial gratuita y a asistencia jurídica en los procedimientos judiciales. Se ha reforzado el delito de incitación al odio y discurso de odio, y se ha ampliado el alcance del delito de ciberacoso. También se ha añadido al Código Penal austriaco el delito de «upskirting».
Polonia	Artículo 190a del Código Penal polaco, de 2011	Este artículo tipifica como delito el acoso y el hostigamiento, incluidos los actos cometidos a través de medios electrónicos. Las interpretaciones jurídicas confirman que el ciberacoso y el ciberhostigamiento están contemplados, aunque el artículo no utilice explícitamente el término «ciber».
Portugal	Artículo 152 del Código Penal portugués, de 2018	La Ley n.º 44/2018 modificó el Código Penal portugués para reforzar la protección penal de la vida privada en Internet. Introdujo en el apartado 2, letra b), del artículo 152 (sobre violencia doméstica) la difusión no consentida a través de Internet u otros medios públicos de amplio acceso, de datos personales, incluidas imágenes o grabaciones de sonido relacionadas con la vida privada, como forma agravante de violencia doméstica.
	Artículo 240 del Código Penal portugués de 2024	La Ley n.º 4/2024 modificó el Código Penal portugués añadiendo un apartado al artículo 240 sobre discriminación e incitación al odio. En él se especifica que, si los delitos se cometen a través de un sistema informático, el tribunal podrá ordenar la supresión de los datos o contenidos pertinentes, ampliando así las protecciones legales contra las formas digitales o en línea de discurso de odio y discriminación, incluido el acoso por motivos de género.
	Código Penal portugués	A través de diversas disposiciones penales generales, la legislación portuguesa ha tipificado como delito la invasión de la intimidad, los delitos contra el derecho a la propia imagen, las amenazas, el acoso, la incitación al odio y el discurso de odio, y estas disposiciones también se aplican cuando los delitos se cometen en línea o por medios electrónicos.

Estado miembro	Nombre de la medida y año	Descripción
Rumanía	Código Penal rumano	Rumanía modificó su Código Penal para tipificar explícitamente como delito el acoso cibernético y el acecho cibernético, endureciendo las penas en los casos de violencia de pareja. También se tipifica la difusión no consentida de contenido íntimo, imponiéndose sanciones severas, especialmente cuando la víctima es menor de edad o el autor es un familiar cercano. El discurso de odio en línea se sanciona de forma similar.
	Modificaciones a la Ley 217/2003 sobre la prevención y la lucha contra la violencia doméstica, 2020	Mediante estas modificaciones, la ley reconoce la violencia cibernética como un medio de coacción y control, lo que permite adoptar medidas de protección como la prohibición del contacto digital.
Finlandia	Código Penal finlandés	Aunque Finlandia se basa en disposiciones penales generales, una reciente modificación del Código Penal finlandés ha ampliado el ámbito de aplicación de la legislación sobre acoso sexual para incluir los contextos en línea, lo que proporciona una mejor protección a las víctimas de la violencia cibernética. En concreto, la ley tipifica como delito la difamación, el acoso sexual, las amenazas ilegales, el acoso, las violaciones de la privacidad y el discurso de odio. Estos delitos son punibles independientemente de si se cometen en línea o fuera de línea.

INTEGRACIÓN DE LA PROTECCIÓN CONTRA LA CIBERVIOLENCIA EN MARCOS JURÍDICOS MÁS AMPLIOS

El tercer enfoque consiste en integrar la ciberviolencia en una legislación más amplia sobre la violencia de género, los delitos sexuales o la protección de la infancia. En estos casos, el abuso digital se reconoce explícitamente como una forma de coacción, discriminación o violencia, lo que garantiza que los comportamientos en línea reciban el mismo trato que los que tienen lugar fuera de línea. Estos marcos suelen incluir medidas preventivas y educativas —dirigidas especialmente a los centros educativos y a los jóvenes— junto con servicios de apoyo a las víctimas (véase la tabla 3).

Tabla 4 | Ejemplos de disposiciones relacionadas con la violencia cibernética que se han incorporado a los marcos jurídicos nacionales existentes

Estado miembro	Nombre de la medida y año	Descripción
Bélgica	Artículo 6 de la ley de 31 de julio de 2023 ([42])	La ley modifica el artículo 584 ([43]) del Código Judicial belga para agilizar los procedimientos sumarios en los casos de difusión no consentida de contenido sexualmente explícito. Mediante un procedimiento acelerado, las víctimas pueden solicitar una orden judicial que obligue al autor o autores, o al proveedor de servicios, a retirar las imágenes o a hacerlas inaccesibles. La ley establece que el presidente del tribunal de primera instancia debe garantizar que la orden contenga todos los datos necesarios para identificar las imágenes o la grabación, facilitando así su retirada por parte de los proveedores de servicios.
Chipre	Ley de prevención y lucha contra la violencia contra las mujeres y la violencia doméstica, 2021	Esta ley tipifica como delito la publicación no consentida o la amenaza de publicación de material sexual o pornográfico a través de medios digitales o de otro tipo.
	Ley de protección contra el acoso y el acecho (L.114(I)/2021)	La ley amplía las garantías contra el acoso y el acecho al ámbito en línea.
Suecia	Código Penal sueco	En virtud del Código Penal sueco y la legislación relacionada, se tipifican como delito conductas tales como el acoso repetido en línea, el acoso cibernético y el intercambio no consentido de contenido privado o íntimo. El principio de que una conducta considerada ilegal en el mundo real es igualmente ilegal en línea contribuye a garantizar la coherencia entre los marcos jurídicos suecos digitales y físicos. Por ejemplo, la responsabilidad penal por violación y violencia sexual incluye los actos cometidos a distancia, por ejemplo, en línea.
	Reforma de la Ley de Delitos Sexuales, 2018	En 2018 se reformó la legislación sueca sobre delitos sexuales. Ahora constituye un delito realizar un acto sexual con una persona que no participe voluntariamente. Por lo tanto, para condenar a un autor de una violación ya no es necesario demostrar que se haya recurrido a la violencia o a amenazas, ni que se haya aprovechado la situación especialmente vulnerable de la víctima.

42 Ley de 31 de julio de 2023 destinada a hacer que la justicia sea más humana, más rápida y más firme IV.
43 Artículo 584 del Código Judicial belga.

5.2.2. Más allá de los enfoques legislativos a nivel nacional

Si bien muchos Estados miembros han elaborado legislación dirigida contra los autores de la ciberviolencia, algunos también han tomado medidas para ayudar a las víctimas mediante la puesta en marcha de políticas e iniciativas que ofrecen servicios de apoyo a las víctimas y medidas preventivas. Sin embargo, muchos de estos enfoques siguen careciendo de una perspectiva de género que tenga en cuenta específicamente las experiencias de las mujeres y las niñas. Como resultado, estas políticas a menudo no logran ofrecer una respuesta integral a la ciberviolencia de género contra las mujeres y las niñas, que se ven afectadas de manera desproporcionada por la ciberviolencia.

En algunos Estados miembros, las políticas para hacer frente a la ciberviolencia se centran principalmente en medidas y campañas educativas y de sensibilización, que a menudo se dirigen al público en general o a grupos especialmente afectados, como las mujeres y los jóvenes. En la tabla 4 se describen algunos ejemplos de estas iniciativas.

Tabla 5 | Ejemplos de medidas educativas y de sensibilización relacionadas con la ciberviolencia en diferentes Estados miembros

Estado miembro	Nombre de la medida y año	Descripción
Bulgaria	Programa «Cyberscout» ([44])	Creada en 2015, esta iniciativa educativa tiene como objetivo mejorar la concienciación sobre la seguridad en línea entre los niños de entre 11 y 12 años. Desarrollado por el Centro Búlgaro para una Internet más Segura, el programa pretende dotar a los jóvenes estudiantes de los conocimientos y habilidades necesarios para navegar por el mundo digital de forma segura.
Chequia	Campaña «Regiones por un Internet seguro»	Lanzada para sensibilizar sobre los riesgos en línea y promover medidas preventivas, esta campaña está dirigida a los escolares. Desde 2019, las regiones checas colaboran en esta iniciativa, que incluye cursos de aprendizaje en línea para niños, estudiantes, profesores, padres, agentes de policía y trabajadores sociales, así como cuestionarios interactivos en línea para que los estudiantes pongan a prueba sus conocimientos sobre seguridad en Internet. El proyecto también organiza seminarios educativos.
	Formación de agentes de policía	Desde 2023, más de 400 agentes de policía han asistido a seminarios formativos sobre violencia doméstica y de género, así como sobre ciberviolencia de género, diseñados específicamente para las fuerzas del orden.
Alemania	Centro de Coordinación contra la Violencia Digital ([45])	Esta iniciativa local, puesta en marcha por la organización Frauen helfen Frauen, presta apoyo a los profesionales que acompañan a las víctimas de la ciberviolencia: asesores, personal de centros de acogida para mujeres y expertos en el ámbito de la violencia de género. El centro ofrece talleres en los que se explica cómo funciona el abuso digital y cómo se puede identificar y detener. Algunos seminarios se centran en cuestiones prácticas, como el software espía y la seguridad de las cuentas, mientras que otros abordan las opciones legales y los retos que plantean las violaciones de la privacidad.
España	Iniciativa «PantallasAmigas» ([46])	Creada en 2004, la iniciativa promueve el uso seguro de las tecnologías digitales entre los niños y adolescentes. Ofrece contenidos educativos sobre el ciberacoso, el grooming, el sexting y la violencia de género en línea. Su programa de «cibergestores» utiliza enfoques dirigidos por compañeros para fomentar la responsabilidad digital.
	Campaña «#RedesSinMachismo» ([47])	Se trata de una campaña mediática lanzada en 2024 por la Junta de Andalucía para hacer frente al aumento de la violencia de género digital.

44 https://eucpn.org/document/cyberscout-program.
45 https://www.fhf-heidelberg.de/de/digitale-gewalt/koordinierungsstelle-digitale-gewalt/.
46 https://www.pantallasamigas.net/.
47 https://www.produccionesvinyl.com/proyecto/redessinmachismo/.

Estado miembro	Denominación de la medida y año	Descripción
Francia	Campaña «StopCybersexisme»	Lanzada en 2017, esta campaña tenía como objetivo sensibilizar sobre el acoso sexual digital y dotar a las víctimas y a los testigos de herramientas prácticas. Ofrece kits de prevención que incluyen un cartel, un folleto informativo, un vídeo de sensibilización y una página web específica ([48]). Esta plataforma define el cibersexismo, ofrece orientación a las víctimas, promueve la autoprotección e incluye testimonios.
	Laboratorio francés para los derechos de las mujeres en Internet	Creado en 2024 como plataforma de diálogo e innovación para combatir la violencia en línea contra las mujeres, este laboratorio también sirve de incubadora de proyectos concretos destinados a identificar, prevenir y frenar la violencia de género en línea y facilitada por la tecnología.
	Programa contra el acoso «pHARe»	Implantado plenamente en todos los centros educativos franceses desde 2023, el programa aborda el acoso escolar mediante la prevención, los mecanismos de respuesta y la sensibilización. Incluye la línea de atención 3018 contra el acoso en línea, que figura en todo el material didáctico, y forma al personal para que reconozca el acoso y actúe ante él. El elemento central del programa es el concurso escolar «Non au harcèlement». Este concurso anual invita a los alumnos a crear conjuntamente campañas contra el acoso escolar, fomentando la participación entre iguales para promover la empatía, el respeto y la igualdad de género. La campaña ganadora se difunde a nivel nacional en los centros educativos.
	Campaña de sensibilización «Parents, parlons numérique»	Lanzada por el Ministerio de Solidaridad, Autonomía e Igualdad entre Mujeres y Hombres, esta campaña proporciona a los padres las herramientas y los consejos necesarios para ayudar a los niños a desarrollar hábitos digitales saludables y respetuosos, especialmente en relación con los riesgos en línea, como la pornografía y la violencia entre iguales.
	Guía sobre la ciberviolencia en la pareja	El Gobierno francés publicó en 2025 una guía dirigida a los profesionales que atienden a mujeres víctimas de violencia de género, en colaboración con el Centro Hubertine Auclert, una organización no gubernamental (ONG) dedicada a la defensa de los derechos de las mujeres y especializada en ciberviolencia.
	Asociación para la lucha contra la ciberviolencia sexista (Echap)	Fundada en 2020, Echap es una asociación feminista que aborda el aumento de la violencia digital contra las mujeres y los grupos marginados. Colabora estrechamente con organizaciones de apoyo a víctimas de violencia doméstica y sexual, proporcionando asistencia técnica en casos relacionados con software espía, acoso en línea y violaciones de la privacidad. Echap también elabora guías accesibles sobre amenazas digitales y ofrece talleres.

48 https://www.stop-cybersexisme.com/.

Estado miembro	Nombre de la medida y año	Descripción
Italia	Campaña «Stop al sexting y al porno vengativo»	La campaña fue lanzada en 2021 por Mete Onlus para combatir la difusión no consentida de imágenes íntimas. Combinaba programas educativos, campañas de sensibilización pública y recursos en línea para empoderar a los jóvenes.
Chipre	Centro para una Internet más segura – CYberSafety ([49])	Creado por el Instituto Pedagógico de Chipre, el centro ofrece charlas y talleres prácticos para estudiantes, profesores y padres con el fin de compartir información sobre el uso seguro y responsable de Internet y las tecnologías digitales. Desde 2017, el instituto también organiza campamentos de verano centrados en la seguridad en Internet, además de eventos en torno al «Día de una Internet más segura», que se celebra cada año en febrero.
Letonia	Programa «Mensajeros de la seguridad»	Puesto en marcha por la policía estatal en 2022, el programa es una iniciativa de prevención que ayuda a los educadores y a los centros educativos a enseñar a los menores sobre los riesgos de seguridad y la autoprotección. La violencia en línea y los riesgos digitales se abordan específicamente a través de escenarios interactivos de juego de roles diseñados para dos grupos de edad (de 8 a 10 años y de 11 a 14 años). Estas actividades se centran en diferentes peligros del entorno en línea, incluidos los riesgos de abuso sexual, cómo reconocerlos y recomendaciones para su prevención.
	Herramienta «Amistades peligrosas en línea»	Desarrollada en 2022 por el Centro para una Internet más Segura en colaboración con la policía estatal y la línea de ayuda del Centro de Protección Infantil, esta herramienta en línea ayuda a los niños, adolescentes y educadores a reconocer el grooming y a recibir asesoramiento y ayuda ([50]).
Hungría	Programa de mentoría entre iguales «Netmentor» ([51])	Este programa se centra en promover el uso responsable de Internet entre los jóvenes a través de la tutoría entre iguales, para que comprendan sus riesgos y posibilidades. Entre otras actividades, el programa Netmentor forma a los alumnos de más edad para que se conviertan en «Netmentores» que imparten talleres a sus compañeros más jóvenes sobre temas como la privacidad en línea, las huellas digitales y el uso seguro de Internet. También se forma a los educadores para que apoyen y orienten a los mentores. Los talleres del programa están diseñados para ser atractivos e interactivos, fomentando la participación activa y la reflexión sobre el comportamiento en línea.

49 «Formación en los centros educativos» – Centro para una Internet más segura.
50 Página web sobre amistades peligrosas en línea.
51 https://digitalisgyermekvedelem.hu/en/netmentor-peer-mentoring-program/.

Estado miembro	Nombre de la medida y año	Descripción
Austria	#GemeinsamGegenCybergewalt (juntos contra la violencia cibernética)	Puesto en marcha en 2023-2024, el proyecto se centró en identificar las necesidades de asesoramiento de las víctimas y adaptar los servicios de apoyo en consecuencia. El proyecto elaboró materiales de asesoramiento y recursos informativos tanto para las víctimas como para el público en general. Incluso tras su finalización oficial, la red que respalda la iniciativa sigue compartiendo contenidos en plataformas como Facebook e Instagram y proporcionando orientación actualizada a los centros de asesoramiento.
	#netzamazonen ([52])	Dirigido por el servicio de asesoramiento «Mujeres que asesoran a mujeres» (Frauen beraten Frauen), este proyecto aborda la seguridad en las citas online, la privacidad y la seguridad de los teléfonos inteligentes. En 2024, el proyecto publicó un manual titulado «¿Esto ya es violencia digital?», que ofrece un análisis detallado del fenómeno.
Eslovenia	Proyecto «Odklikni»: ClickOFF! Detengamos la ciberviolencia contra las mujeres y las niñas	Llevado a cabo entre 2017 y 2019, el proyecto tenía como objetivo sensibilizar a los jóvenes sobre la violencia digital de género. El proyecto incluía anuncios de televisión, carteles, una aplicación móvil, una página web específica ([53]) y un manual para profesionales que trabajan con jóvenes. También organizó una amplia formación para educadores, trabajadores sociales, jueces y agentes de policía, haciendo hincapié en la necesidad de evitar los sesgos de género y los estereotipos a la hora de abordar la violencia en línea. Al mismo tiempo, otros proyectos eslovenos se centraron en la prevención de la violencia en el noviazgo entre los jóvenes desde una perspectiva de género.
Finlandia	Servicio «For you in social media» ([54])	Este servicio tiene como objetivo combatir el ciberacoso y el abuso sexual en línea entre jóvenes de entre 8 y 21 años. Gestionado por organizaciones sin ánimo de lucro, este servicio interactúa directamente con los jóvenes en las plataformas donde suelen encontrarse con la ciberviolencia. Más allá del apoyo individual, el servicio elabora contenidos educativos para sensibilizar sobre la seguridad en línea y las relaciones digitales saludables. Sus vídeos abordan temas como reconocer y responder al ciberacoso, comprender el consentimiento y desenvolverse de forma segura en las interacciones en línea.

Fuente: Autores.

Además de las iniciativas de sensibilización, algunos Estados miembros han incorporado medidas contra la ciberviolencia en sus planes de acción nacionales. En la tabla 5 se pueden ver algunos ejemplos de ello.

52 https://frauenberatenfrauen.at/projekt/netzamazonen/.
53 http://odklikni.enakostspolov.si/.
54 https://suavartensomessa.fi/in-english/.

Tabla 6 | Ejemplos de planes de acción nacionales de los Estados miembros que incluyen medidas contra la ciberviolencia

Estado miembro	Nombre de la medida y año	Descripción
Bélgica	Plan de acción nacional para combatir la violencia de género (2021-2025)	El plan de acción reconoce la naturaleza de género de la violencia cibernética e incluye objetivos para combatirla. Estos se logran mediante diferentes medidas, como una plataforma informativa sobre el cibersexismo, la mejora de las actuaciones policiales y judiciales, y la colaboración. El plan también apoya el desarrollo de capacidades de las fuerzas del orden y las campañas de sensibilización dirigidas a los usuarios adultos de las redes sociales.
Chequia	Estrategia de igualdad de género (2021-2030)	La estrategia aborda la violencia cibernética en el marco de la violencia de pareja. Destaca formas de violencia como la pornografía vengativa y el acoso a través de mensajes, que afectan especialmente a los jóvenes.
	Plan de acción para la prevención de la violencia doméstica y de género (2023-2026) y estrategia para la prevención de la delincuencia (2022-2027)	El plan de acción incluye medidas como la formación de la policía en materia de violencia doméstica y de género, incluida la ciberviolencia, y la sensibilización sobre prácticas seguras en Internet en los centros educativos.
Francia	Quinto plan para movilizar y combatir la violencia contra las mujeres (2017-2019)	En virtud del Código Penal sueco y la legislación conexa, se tipifican como delito conductas como el acoso repetido en línea, el ciberacoso y el intercambio no consentido de contenidos privados o íntimos. El principio de que una conducta considerada ilegal en el mundo real lo es igualmente en línea contribuye a garantizar la coherencia entre los marcos jurídicos suecos en el ámbito digital y en el físico. Por ejemplo, la responsabilidad penal por violación y violencia sexual incluye los actos cometidos a distancia, por ejemplo, en línea.
	Plan interministerial para la igualdad de género (2023-2027)	Las medidas de este plan incluyen mejorar la accesibilidad de los mecanismos de denuncia y la asistencia a las víctimas de ciberviolencia, así como reforzar las herramientas de formación.
Croacia	Plan de acción para la prevención de la violencia en las escuelas (2020-2024)	El plan incluye medidas dirigidas a la violencia sexual cibernética entre niños y jóvenes. Apoya los programas de prevención en los centros educativos y define formas específicas de violencia cibernética, como el discurso de odio en línea, el acoso cibernético, el hostigamiento cibernético, el acoso sexual y el sexting.

Estado miembro	Nombre de la medida y año	Descripción
Italia	Plan nacional para prevenir el acoso escolar y el ciberacoso en el ámbito escolar (2016-2017)	El plan estableció programas de formación y campañas de sensibilización para alumnos y profesores, e introdujo líneas de ayuda para los alumnos afectados y sus familias. Esta iniciativa ha ido evolucionando con el tiempo, con disposiciones actualizadas y la plataforma «ELISA» (E-Learning degli Insegnanti sulle Strategie Antibullismo), que ofrece formación en línea para los profesores que se ocupan de casos de ciberacoso.
Chipre	Estrategia nacional para la prevención y la lucha contra la violencia contra las mujeres (2023-2028)	La estrategia nacional aboga por una regulación más estricta de los medios de comunicación y una mejora en la recopilación de datos, integrando las recomendaciones del GREVIO sobre la violencia en línea.
	Estrategia de ciberseguridad de la República de Chipre 2020	La estrategia de ciberseguridad incluye medidas para garantizar la protección de las infraestructuras de información críticas, combatir las amenazas cibernéticas y mejorar la resiliencia.
	Estrategia nacional para una Internet mejor para los niños en Chipre (2018-2023)	La estrategia nacional para una mejor Internet para los niños en Chipre incluye acciones dirigidas a los niños, pero también a los profesores, los padres y el público en general.
Malta	Marco de políticas para la infancia 2024-2030	El marco incluye medidas específicas para hacer frente a los riesgos crecientes de la ciberviolencia, al tiempo que reconoce que las niñas se ven afectadas de manera desproporcionada. Aborda cuestiones como el ciberacoso y el acoso en línea.
Austria	Plan de acción nacional para combatir la violencia contra las mujeres y las niñas (2025-2029)	El plan incluye medidas contra la violencia digital, incluida la violencia que utiliza la inteligencia artificial. Contiene un capítulo específico sobre la violencia digital y aborda la aplicación de la Directiva de la UE sobre la violencia contra las mujeres, incluidos los delitos relacionados con la ciberviolencia.
Portugal	Estrategia nacional para la igualdad y la no discriminación – Portugal + Equal	El plan estratégico nacional para promover la igualdad y combatir la discriminación ha dado lugar a tres planes de acción. El plan de acción 2023-2026 para la prevención y la lucha contra la violencia contra las mujeres y la violencia doméstica incluye medidas como el refuerzo de las protecciones legales contra las formas de violencia en línea, en particular la violencia sexual basada en imágenes dirigida a mujeres y niñas y el discurso de odio en línea (Medida 242), así como la formación y la mejora de las competencias de los profesionales para hacer frente a estas formas de violencia en línea (Medida 418).

Fuente: Autores.

Otros Estados miembros han reconocido la importancia de la colaboración intersectorial a la hora de abordar la ciberviolencia. En la tabla 6 que figura a continuación se pueden ver algunos ejemplos de ello.

Tabla 7 | Ejemplos de Estados miembros que colaboran de forma intersectorial para hacer frente a la ciberviolencia

Estado miembro	Nombre de la medida y año	Descripción
República Checa	Proyecto «Be safe»	El proyecto aborda el ciberacoso y, al mismo tiempo, establece una conexión entre los colegios, las instituciones educativas y la policía. Los docentes tienen acceso a noticias e información actualizadas sobre las últimas tendencias en materia de ciberacoso y ciberdelincuencia, que pueden incorporar a su labor docente.
Dinamarca	Programa interministerial de 2017	El programa reunió a los Ministerios de Educación, Justicia e Igualdad de Género para abordar el abuso sexual digital. Esta iniciativa incluyó la creación de recursos educativos, campañas de sensibilización pública y colaboraciones con organizaciones de la sociedad civil.
Alemania	Proyecto InterAktion ([55])	Dirigido por la Asociación Federal de Refugios y Centros de Asesoramiento para Mujeres, el proyecto, puesto en marcha en 2023, conecta los centros de asesoramiento y las líneas de ayuda para mujeres con profesionales locales del ámbito de las tecnologías de la información. Gracias a estas colaboraciones, las partes implicadas pueden abordar casos complejos relacionados con la ciberviolencia.
Estonia	Programa «Targalt Internetis» (navegar con inteligencia por la web) ([56])	El programa integra a expertos en ciberseguridad en las iniciativas educativas, proporcionando a los jóvenes las herramientas y la formación necesarias para identificar y responder a las amenazas en línea, incluida la violencia de género.
Lituania	Consorcio «Safer Internet»	El consorcio es un modelo de colaboración en el que participan el Centro de Tecnologías de la Información, adscrito al Ministerio de Educación y Ciencia, la Autoridad Reguladora de las Comunicaciones, la ONG Child Line y la organización de alfabetización digital Langas j ateitj. Estos socios trabajan en diferentes sectores —entre ellos, el gubernamental, el tecnológico, los medios de comunicación y la sociedad civil— para crear un entorno digital más seguro para los niños y reducir su exposición a los riesgos en línea.

Fuente: Autores.

COORDINACIÓN A NIVEL DE LA UE E INICIATIVAS MULTIPARTITAS

A nivel de la UE, los esfuerzos de colaboración siguen impulsando el progreso. Un actor clave en estos esfuerzos es la Asociación Internacional de Líneas Directas de Internet (INHOPE), que comenzó en 1999 con ocho líneas directas europeas y desde entonces se ha convertido en una red mundial. Permite a las víctimas denunciar contenidos ilegales en línea, en particular material de abuso sexual infantil, captación de menores en línea y discurso de odio, incluida la xenofobia. Todos los Estados miembros forman parte de esta red.

55 https://www.frauen-gegen-gewalt.de/de/aktionen-themen/bff-aktiv-gegen-digitale-gewalt.html.
56 https://www.targaltinternetis.ee/en/.

Otra iniciativa importante es Insafe, que opera en el marco de la estrategia «Un Internet mejor para los niños» de la Comisión Europea. Gestiona Centros para un Internet más Seguro en 30 países europeos, que ofrecen formación y apoyo a través de líneas de ayuda y líneas directas para niños, padres y profesores. Estos centros también remiten las denuncias de contenidos ilegales o nocivos en línea a las autoridades competentes, como los proveedores de servicios de Internet, las fuerzas del orden o las líneas directas de INHOPE. Es importante destacar que «los centros cuentan con paneles de jóvenes para garantizar que estos tengan voz a la hora de definir las políticas y los recursos de seguridad en línea».

La UE también organiza el Foro anual de Internet más segura, que reúne a responsables políticos, investigadores, representantes del sector, fuerzas del orden y jóvenes para abordar los retos de la seguridad en línea. El foro de 2024 se centró específicamente en la ciberviolencia y en la protección de los jóvenes frente a contenidos nocivos y el acoso. Del mismo modo, el Día de Internet más segura, que se celebra cada año en más de 100 países, sensibiliza a nivel mundial sobre cuestiones como el ciberacoso y el acoso sexual en línea. La campaña #SaferInternet4EU, puesta en marcha en 2018, impulsa esta misión apoyando iniciativas a escala de la UE para hacer frente a los riesgos digitales emergentes. En el recuadro 4 se presentan otros ejemplos de proyectos financiados por la UE.

Recuadro 4 | Ejemplos de proyectos financiados por la UE que promueven un enfoque colaborativo

Proyecto CyberEqual (2024)

Este proyecto es una iniciativa de Erasmus+ en la que participan Chipre, Grecia, Lituania, Eslovaquia y Ucrania. Su objetivo es educar y sensibilizar a los jóvenes sobre la violencia cibernética contra las mujeres y las niñas. Entre sus objetivos principales se incluyen aumentar el conocimiento sobre la prevalencia de la violencia cibernética contra las mujeres y las niñas y la legislación al respecto, sensibilizar y educar a los jóvenes y a los profesionales, motivar a los jóvenes a protegerse a sí mismos y dotar a los trabajadores juveniles de herramientas para combatir la violencia cibernética contra las mujeres y las niñas.

DeStalk (2021)

DeStalk es una iniciativa europea llevada a cabo en España e Italia, coordinada por Blanquerna-URL con el apoyo del programa de derechos, igualdad y ciudadanía de la UE. Su objetivo es combatir la ciberviolencia y el ciberacoso de género. Hasta 2022, el proyecto había formado a más de 350 profesionales —principalmente en España e Italia— que trabajan en el ámbito de la violencia de género.
DeStalk cuenta con una plataforma de aprendizaje en línea, elabora herramientas prácticas y guías, y apoya campañas regionales para sensibilizar sobre la ciberviolencia y la seguridad digital.

Cybersafe: Cambio de actitudes entre los adolescentes respecto a la ciberviolencia contra las mujeres y las niñas (2019-2021)

El proyecto Cybersafe fue una iniciativa de 30 meses financiada por la UE que reunió a nueve socios de diversos países europeos: Austria, Dinamarca, Estonia, Grecia, Italia, los Países Bajos, Eslovenia y el Reino Unido. Su objetivo principal era desarrollar, promover y difundir herramientas educativas innovadoras para abordar la ciberviolencia contra las mujeres y las niñas entre los adolescentes de entre 13 y 16 años. A través del proyecto se desarrolló un conjunto de herramientas Cybersafe destinado a docentes y otros profesionales que trabajan con jóvenes y que deseen abordar la violencia cibernética contra las mujeres y las niñas en el aula o en otros entornos.
El conjunto de herramientas Cybersafe ofrece recursos y herramientas
para organizar e impartir cuatro talleres sobre la violencia de género en línea. Su objetivo es sensibilizar y promover un comportamiento seguro y responsable en Internet entre los jóvenes.

Proyecto «Targalt Internetis» (2019)

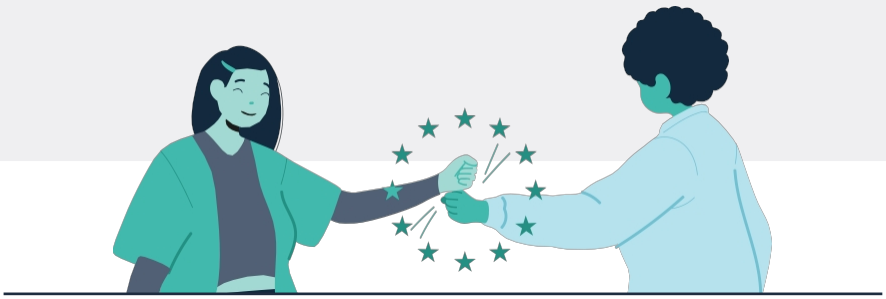
Este proyecto tiene como objetivo promover un uso más responsable de Internet entre los niños y sus padres, al tiempo que trabaja activamente para prevenir la distribución en línea de material de abuso sexual infantil. Cofinanciada por la Comisión Europea, la iniciativa abarca diversas actividades diseñadas para mejorar la sensibilización y la educación. Entre ellas se incluyen sesiones de formación y seminarios adaptados a niños, padres, profesores y trabajadores sociales, junto con eventos de sensibilización pública dirigidos a la población en general. Además, el proyecto implica la creación de materiales formativos que sirven para informar a los niños, profesores y padres sobre prácticas seguras en Internet. Para involucrar a los niños y estudiantes en el tema de forma creativa, el proyecto organiza concursos que fomentan la participación y la sensibilización. Asimismo, ofrece asistencia y asesoramiento a través de las líneas de ayuda para menores disponibles en el 116111, a las que se puede acceder por teléfono, SMS, Messenger y otros servicios de mensajería instantánea, y que ofrecen orientación a niños y padres sobre el uso seguro de Internet y de los dispositivos móviles digitales. La iniciativa cuenta también con una línea de asistencia en línea que permite a los usuarios de Internet denunciar entornos que contengan materiales que violen los derechos de los niños a la autodeterminación sexual, así como otros contenidos inapropiados. Desde su puesta en marcha en enero de 2019, el proyecto ha dado prioridad a la cooperación entre diversas partes interesadas en Estonia y en toda Europa, participando activamente en las redes INHOPE e Insafe para reforzar su impacto.

Proyecto deSHAME (2017)

El proyecto deSHAME es un proyecto financiado por la UE cuyo objetivo es prevenir y dar respuesta al acoso sexual en línea. En el proyecto participaron Dinamarca, Hungría y el Reino Unido, y su objetivo era abordar y reducir el acoso sexual en línea entre jóvenes de entre 13 y 17 años. El proyecto pretendía empoderar a las comunidades locales para que colaboraran con el fin de aumentar el número de denuncias entre los jóvenes. Para abordar estas cuestiones, el proyecto deSHAME desarrolló recursos adaptados a educadores, padres y jóvenes. Estos materiales tienen como objetivo sensibilizar, educar sobre los daños del acoso sexual en línea y promover un comportamiento seguro en Internet. El proyecto también elaboró un conjunto de herramientas de adaptación internacional para ayudar a otros países y organizaciones a poner en marcha iniciativas similares para combatir el acoso sexual en línea.

Trabajo con los autores (2015)

Este proyecto ofrece valiosas directrices para abordar la ciberviolencia, con un enfoque centrado en los autores. Un principio clave de estas directrices es que la carga de la protección no debe recaer sobre la víctima, ya que esta tiene el derecho fundamental a la seguridad en los espacios digitales. En lugar de atribuir a las personas la responsabilidad de evitar o mitigar el abuso en línea, el proyecto subraya la necesidad de soluciones sistémicas, entre las que se incluyen marcos jurídicos más sólidos, estrategias de intervención proactivas y medidas de rendición de cuentas para los autores. También destaca el papel crucial de la colaboración entre las plataformas digitales, los responsables políticos y las fuerzas del orden a la hora de prevenir y abordar la ciberviolencia, garantizando que las víctimas no se vean obligadas a soportar el daño en silencio, sino que reciban apoyo a través de protecciones integrales y mecanismos de aplicación de la ley eficaces.



OTRAS MEDIDAS PREVENTIVAS EN LOS PAÍSES DE LOS GRUPOS DE DISCUSIÓN

Al analizar en profundidad los Estados miembros en los que se llevaron a cabo los grupos focales, queda claro que sus autoridades y organizaciones también han puesto en marcha estrategias orientadas a la prevención que tienen como objetivo abordar la ciberviolencia mediante formas de apoyo específicas dirigidas a los niños y jóvenes, a los padres y a las instituciones pertinentes.

La orientación parental desempeña un papel crucial a la hora de proporcionar apoyo emocional y consejos prácticos a las niñas que sufren ciberviolencia. Sin embargo, los padres suelen enfrentarse a importantes dificultades a la hora de comprender cuál es la mejor manera de responder ante este tipo de situaciones. En Alemania e Italia (véase el recuadro 5), se han puesto en marcha campañas de sensibilización y prevención para promover un uso seguro de Internet y ofrecer a los padres orientación sobre cómo apoyar a los niños y jóvenes a la hora de abordar cuestiones relacionadas con la ciberviolencia.

Recuadro 5 | Ejemplos de campañas para entornos en línea más seguros: Alemania e Italia

La campaña **alemana** «klicksafe», cofinanciada por la UE, promueve el uso responsable de Internet entre niños, jóvenes, padres y educadores. Incluye recursos específicos para ayudar a abordar la violencia sexual digital, como el folleto «El primer smartphone: ¿cómo puedo proteger a mi hijo de la violencia sexual en Internet?», elaborado en colaboración con el Ministerio Federal de Educación, Asuntos Familiares, Tercera Edad, Mujeres y Juventud y el Comisionado Independiente para Asuntos de Abuso Sexual Infantil. Otra iniciativa importante es «Activos contra la violencia digital», que apoya a las víctimas de abusos digitales por motivos de género mediante campañas de sensibilización y herramientas prácticas, como parte de la estrategia general de digitalización de Alemania.

En **Italia**, la iniciativa «Scelgo io!» (Yo elijo), puesta en marcha en 2018 por la organización Cuore e Parole en el marco del proyecto «Generazioni Connesse», ofrece formación en línea y conferencias para padres sobre los peligros del sexting para sus hijos y proporciona orientación sobre cómo protegerlos del abuso basado en imágenes y la ciberviolencia.

Fuente: Autores, a partir de los sitios web del programa «klicksafe» y de «Generazioni Connesse».

Otros Estados miembros (véase el recuadro 6) han adoptado prácticas interesantes para hacer frente a la ciberviolencia contra las mujeres jóvenes y las niñas, combinando la educación, la tecnología y los marcos jurídicos con el fin de fomentar un entorno digital más seguro y prevenir futuros incidentes de ciberviolencia.

Recuadro 6 | Ejemplos de diferentes enfoques para combatir la ciberviolencia: Bélgica, Estonia, Irlanda y España

El plan internacional **belga** SafeHaven utiliza Roblox (una popular plataforma de juegos en línea) para enseñar a los jóvenes sobre los comportamientos inapropiados en los mundos virtuales. Recurre a juegos interactivos ambientados en un «e-pabellón» que proporcionan a los jóvenes las herramientas necesarias para romper estereotipos, establecer límites y buscar ayuda. También se les anima a actuar como testigos activos tanto en línea como fuera de línea.

Los «agentes de la web» **de Estonia** representan otra estrategia innovadora; se trata de agentes de policía dedicados a supervisar y responder al abuso en línea, incluidos el discurso de odio y el acoso.

Irlanda ha integrado la prevención de la ciberviolencia en su plan de estudios escolar a través de un curso breve sobre educación social, personal y sanitaria (SPHE). Actualizado en 2023, el programa incluye módulos sobre la comunicación respetuosa en línea, el consentimiento digital y el reconocimiento de comportamientos nocivos en las interacciones en línea. Dota a los jóvenes de los conocimientos y habilidades prácticas necesarios para prevenir y responder al ciberacoso y al abuso basado en imágenes.

España también adoptó un enfoque creativo con el videojuego «Conectado», que sumerge a los jugadores en la experiencia de una víctima de ciberacoso durante cinco días para fomentar la empatía y el diálogo en los entornos educativos.

Fuente: Autores, basándose en la página web de SafeHaven, el plan de estudios de Educación Social, Personal y Sanitaria del ciclo básico, la página web de «Conectado» y la página web sobre los «web constables».

Además de la orientación parental y la integración de medidas centradas en los jóvenes y de aplicación de la ley, algunos Estados miembros han puesto en marcha programas de formación destinados a dotar a los docentes y a los profesionales especializados de las competencias necesarias para prevenir y responder a los riesgos en línea a los que se enfrentan los niños y los jóvenes (véanse ejemplos en el recuadro 7). Estas iniciativas reconocen que los centros educativos y los servicios de apoyo profesional suelen ser los primeros en detectar los indicios de ciberviolencia.

Recuadro 7 | Ejemplos de programas de formación para docentes y profesionales especializados: Polonia y Suecia

En **Polonia**, el Centro de Sensibilización organiza seminarios web, clases y talleres para docentes y otros especialistas centrados en la seguridad digital. Además, la Fundación Empowering Children gestiona una plataforma de aprendizaje en línea que ofrece recursos de acceso libre sobre seguridad en Internet para docentes.

El módulo nacional de formación **sueco** sobre «uso seguro de Internet» ofrece desarrollo profesional estructurado para docentes, bibliotecarios y personal sanitario escolar. Abarca el comportamiento en línea, el ciberacoso, los videojuegos y la seguridad de la información, y promueve el aprendizaje colaborativo y su aplicación práctica en el aula.

Fuente: Autores, basado en la página web del Centro Polaco para un Internet más Seguro y en la página web del módulo de formación «Uso seguro de Internet».

5.2.3. Las percepciones de los jóvenes sobre las respuestas a la ciberviolencia

Aunque las conclusiones aquí presentadas se basan en debates en grupos focales —y, por lo tanto, no pretenden ser generalizables—, constituyen una aportación crucial e innovadora para comprender cómo viven los adolescentes la ciberviolencia y cómo responden a ella. El debate revela una compleja interacción entre las estrategias de afrontamiento individuales, la dinámica entre iguales, las respuestas institucionales y las barreras estructurales más amplias.
Los relatos de los participantes ponen de relieve que los sentimientos de vergüenza, miedo y desconfianza suelen impedir que las víctimas denuncien la violencia o busquen ayuda. Al mismo tiempo, se percibe que los colegios, los padres y los actores institucionales son inconsistentes en sus respuestas o no están preparados.

RESPUESTAS INDIVIDUALES

Las respuestas emocionales inmediatas de las chicas ante la ciberviolencia venían determinadas por la edad, la gravedad percibida y la disponibilidad de apoyo.

A menudo reaccionaban aislándose emocionalmente, guardando silencio o bloqueando a los agresores, impulsadas por el miedo, la vergüenza o el deseo de evitar que la situación se agravara. Estas reacciones eran más comunes entre las chicas más jóvenes (de
13 a 15 años). Otras describieron confrontaciones defensivas, afirmando que desafiaban directamente a los agresores en línea. Sin embargo, incluso estas respuestas activas se enmarcaban a menudo como reacciones de último recurso que se producían ante la ausencia de estructuras de apoyo. Del mismo modo, los chicos señalaron que la vergüenza —especialmente en los casos de abuso basado en imágenes— constituía una barrera importante para que las chicas denunciaran los incidentes. El miedo al juicio de los padres o de las figuras de autoridad también se reveló como una preocupación clave común entre chicas y chicos.

No obstante, para algunas chicas, la orientación de los padres desempeñó un papel formativo a la hora de definir su enfoque respecto a la seguridad en línea, especialmente durante los primeros años de la adolescencia. Los compañeros también desempeñaron con frecuencia un papel importante como primer punto de confidencia, ofreciendo apoyo emocional, consejos y sirviendo de puente hacia redes de apoyo más amplias.

Los testimonios de los chicos revelaron un panorama más variado. Algunos describieron una cooperación positiva entre los padres y los centros educativos, mientras que otros temían ser culpados y que se les malinterpretara.

RESPUESTAS INSTITUCIONALES

Las percepciones sobre el apoyo institucional —incluidos los centros educativos y la policía— variaban considerablemente. En general, se consideraba que los padres eran más fiables y protectores que otros actores, aunque el hecho de contárselo a ellos solía verse obstaculizado por el miedo a la decepción o a que les culparan.

Las chicas de más edad (de entre 16 y 18 años) tendían a mostrarse más escépticas ante las respuestas institucionales. Este escepticismo solía derivarse de experiencias personales negativas o de una mayor conciencia de las barreras estructurales, como los orientadores poco serviciales. La falta generalizada de conocimiento sobre los servicios de apoyo existentes para chicas y chicos también reforzaba la creencia de que «la solución está en nosotros mismos, y no en buscar ayuda».

Los profesores y los orientadores eran vistos tanto como aliados potenciales como fuentes de frustración. Algunos chicos valoraban a los profesores de confianza que les proporcionaban un espacio seguro para abrirse. Otros, sin embargo, expresaron que algunos profesores agravaban los problemas. Las chicas confirmaron estos sentimientos. Afirmaron que, con frecuencia, consideraban que los colegios eran ineficaces o desdeñosos. En muchos casos, la confianza en los profesores era escasa, y varias chicas denunciaron que el personal del colegio restaba importancia o desestimaba sus experiencias.

Algunas chicas describieron sentirse traicionadas cuando los orientadores les prometían confidencialidad, pero posteriormente revelaban información a sus padres sin su consentimiento. Otras relataron experiencias positivas en las que los profesores u orientadores intervinieron de forma decisiva, aunque no siempre estuvieran bien preparados o contaran con la formación suficiente para hacer frente a la ciberviolencia. Esta ambivalencia pone de relieve la variabilidad en las respuestas de los centros educativos, que a menudo dependen de cada miembro del personal más que de enfoques sistémicos.

> **El orientador escolar nunca hizo nada. Solo tomaba notas y cosas así. Luego llamó a mis padres y les contó todo. Y entonces tuve que enfrentarme a mis padres y asumir toda la responsabilidad. Fue aún peor. Y eso no solo ocurrió una vez. Ocurrió más de una vez.**
>
> **(CHICA DE 16 A 18 AÑOS, BÉLGICA)**

Tanto las chicas como los chicos veían a la policía con mayor escepticismo y frustración, a pesar de que hubo casos en los que las autoridades tomaron medidas. Muchos participantes dudaban de la seriedad con la que las autoridades trataban la ciberviolencia, citando largas demoras, inacción o un rechazo rotundo. Los chicos, en particular, se burlaban de la idea de involucrar a la policía.

> **Nadie va a llamar a la policía. ¿Quién es tan cobarde como para llamar a la policía? Muy pocos agentes de policía se tomarían este asunto en serio.**
>
> **(CHICO DE 15 A 18 AÑOS, CHIPRE)**

Las chicas también expresaron su frustración por la ineficacia de las investigaciones y las demoras.

> **Se pusieron en contacto conmigo dos años y medio después... La denuncia no sirvió de mucho.**
>
> **(NIÑA DE 16 A 18 AÑOS, BÉLGICA)**

OPINIONES DE LOS JÓVENES SOBRE EL APOYO DE LOS ADULTOS

Las chicas de todos los Estados miembros y grupos de edad consideraban, en general, que los adultos estaban desconectados de la realidad de la vida digital de los jóvenes. Muchas describían a los adultos —incluidos padres y profesores— como personas que carecían de la concienciación, la sensibilidad y la formación necesarias para responder de manera eficaz a la ciberviolencia. Las participantes
señalaban que los adultos o bien restaban importancia a sus experiencias o bien respondían de formas que les disuadían de contarlas.

> **A veces los padres no nos creen o no les gusta... en general, las personas mayores no nos creen.**
>
> **(NIÑA DE 13 A 15 AÑOS, ESTONIA)**

> **Muchos adultos... de tu entorno tienden a resolver las cosas diciendo que no es tan importante, cuando tú sientes que sí lo es y eso te duele mucho.**
>
> **(NIÑA DE 13 A 15 AÑOS, RUMANÍA)**

Algunas chicas expresaron su reticencia a pedir ayuda a sus padres, por miedo a ser castigadas o a que no las entendieran, en lugar de recibir apoyo. Mientras que algunas se sentían cercanas a sus padres y creían que estos podían ayudarlas, otras destacaron que sus padres carecen de conocimientos sobre el mundo digital. Otras participantes responsabilizaron a los adultos de su exposición precoz y excesiva a la tecnología.

> **Tengo conocidos que recibieron un móvil con conexión a Internet cuando tenían entre 3 y 4 años... Me parece que nada más salir del útero tus padres ya te echaron a perder; solo querían que te callaras, así que te dieron una tableta... Ahora no sabes cómo relacionarte, no tienes habilidades comunicativas y te preguntas: «¿Qué hago aquí?».**
>
> **(NIÑA DE 13-15 AÑOS, RUMANÍA)**

La percepción del papel de los profesores y los psicólogos escolares en la prevención y la intervención fue variada. Las chicas más jóvenes solían confiar en algunos profesores, sobre todo en aquellos que eran amables o con los que se sentían identificadas. También se mencionó que los psicólogos escolares resultaban de ayuda. Sin embargo, muchas participantes consideraban que los centros educativos carecen de mecanismos de apoyo genuinos, ya que los profesores y las instituciones suelen mostrarse indiferentes o no actúan, lo que lleva a las chicas a pensar que «el colegio es el último lugar al que acudir en busca de ayuda».

La disposición de las niñas a buscar el apoyo de los adultos parece verse influida por factores contextuales. En algunos Estados miembros —como Italia, Chipre y Suecia— expresaron una mayor decepción con las respuestas de los adultos, mientras que en otros —como Estonia e Irlanda— las niñas se mostraban más dispuestas a confiar en los adultos, y describían el colegio y la familia como entornos emocionalmente receptivos o que les brindaban apoyo.

La edad también influye en la percepción de la implicación de los adultos. Las chicas más jóvenes (de entre 13 y 15 años) se mostraban, en general, más abiertas
a confiar en adultos de confianza, especialmente en profesores y padres. Las participantes de más edad (de 16 a 18 años) se mostraron más escépticas, citando la distancia emocional, los problemas de comunicación y las diferencias generacionales, especialmente en lo que respecta a la cultura digital, el sexo y las relaciones.

LIMITACIONES Y RECOMENDACIONES DE LOS JÓVENES PARA UNA PREVENCIÓN EFICAZ

En todos los Estados miembros, la mayoría de las chicas coincidieron en que las estrategias de prevención son limitadas, obsoletas o se aplican de forma deficiente. Las iniciativas escolares se describieron a menudo como superficiales, repetitivas y desconectadas de la realidad digital de los jóvenes. Las breves charlas, las campañas repetitivas y las asambleas escolares impartidas por las mismas personas se consideraron en gran medida ineficaces.

Del mismo modo, los chicos señalaron una laguna crítica en la educación temprana y significativa sobre la ciberviolencia, y destacaron que las intervenciones escolares actuales suelen llegar demasiado tarde o carecen de relevancia.

Las chicas también señalaron que los recursos para prevenir o responder a la ciberviolencia son insuficientes, especialmente en lo que respecta a las estructuras de apoyo. Entre los obstáculos para una prevención eficaz se encontraban la falta de confidencialidad en las comunidades pequeñas, los mecanismos de denuncia vagos o ineficaces, una educación insuficiente y adaptada a la edad, y los tabúes culturales que limitan los debates abiertos. Estos retos eran especialmente pronunciados entre las chicas de más edad (de 16 a 18 años).

> **Aunque los centros educativos sensibilicen sobre la ciberviolencia, esto no resulta eficaz porque los adultos no saben cómo llegar a los adolescentes.**
>
> **(CHICA DE 16 A 18 AÑOS, ITALIA)**

Los chicos, por su parte, reclamaron una mayor rendición de cuentas por parte de los agresores, especialmente a la hora de abordar las lagunas legales relacionadas con el abuso basado en imágenes, incluidos los «deepfakes» ([57]). Esta preocupación refleja un tema emergente dentro de la ciberviolencia, ya que el abuso en línea en entornos de realidad virtual y del metaverso plantea retos sin precedentes debido a la debilidad de las regulaciones, la moderación insuficiente y las actitudes sociales que minimizan o descartan el abuso en línea por no considerarlo «real» (Chawki et al., 2024).

Las chicas propusieron recomendaciones prácticas para mejorar los mecanismos de prevención y apoyo, entre ellas:

- un mejor acceso a profesionales de la salud mental;
- opciones de denuncia anónimas y confidenciales;
- servicios de chat y apoyo en línea entre iguales;
- servicios de apoyo que sean visibles, fiables y emocionalmente accesibles;
- debates más abiertos y estructurados en los centros educativos sobre la ciberviolencia;
- una educación interactiva, participativa y basada en la experiencia, utilizando ejemplos de la vida real;
- información clara y fácilmente accesible sobre cómo y dónde denunciar los abusos;
- programas de prevención dirigidos tanto a las víctimas como a los agresores;
- formación integral para el profesorado sobre cómo comunicarse de manera eficaz con los jóvenes sobre temas delicados.

57 En Irlanda, la creación de un «deepfake» no es ilegal en la actualidad, pero su distribución o difusión es ilegal en virtud de la Ley de 2020 sobre acoso, comunicaciones nocivas y delitos relacionados (la «Ley de Coco»), que se analiza en la sección 2.4.

6 Conclusiones

La ciberviolencia contra las mujeres y las niñas es un continuo de violencia generalizado y profundamente marcado por el género —impulsado por relaciones de poder desiguales y reforzado por las normas sociales— que configura y limita las vidas digitales de las niñas y las mujeres jóvenes.

La ciberviolencia es un fenómeno generalizado, complejo y profundamente marcado por el género que afecta tanto al entorno digital como al físico, formando un continuo de abusos. Tiene sus raíces en las normas sociales, los estereotipos de género y las dinámicas de poder desiguales que reproducen en los espacios en línea las jerarquías de género y de control existentes en el mundo real. Estas dinámicas se manifiestan en comportamientos que cosifican, controlan o silencian a las niñas y las jóvenes. Reflejan normas sociales más amplias que premian el dominio masculino y estigmatizan la sexualidad femenina. Entre los chicos, ciertos actos de ciberviolencia suelen tolerarse y considerarse una forma de ganarse la aprobación de los compañeros o de demostrar masculinidad, mientras que a las chicas que sufren abusos se les culpa o se burlan de ellas. Esto crea una cultura digital en la que la agresión
se vincula al poder y la responsabilidad por el daño se traslada a las víctimas.

Las niñas y las jóvenes sufren la ciberviolencia como parte habitual de su vida digital y social, con patrones distintos según la edad: las niñas más jóvenes (de 13 a 15 años) son más propensas a sufrir exclusión, chismes y burlas por su físico, mientras que las más mayores (de 16 a 18 años) son sometidas con mayor frecuencia a formas de violencia sexualizadas, como la coacción y la extorsión sexuales en línea, la captación de menores con fines sexuales y el intercambio de imágenes sin consentimiento. También se ha constatado que los adolescentes varones son blanco específico de la coacción sexual y la extorsión en línea por parte de agresores que operan
en redes delictivas organizadas, siendo el beneficio económico la principal motivación. Los adolescentes más jóvenes también están cada vez más expuestos a formas sexualizadas y coercitivas de abuso en línea, lo que pone de relieve el alcance cada vez mayor y la normalización de la violencia digital.

Los datos de los grupos de discusión ponen aún más de relieve que los incidentes de ciberviolencia suelen tener su origen en entornos fuera de Internet, como colegios, comunidades o grupos de iguales, y se intensifican en línea, propagándose rápidamente a través de múltiples plataformas y ámbitos sociales. Esta escalada de los espacios físicos a los digitales amplifica el daño, difumina los límites y hace que el abuso sea más difícil de contener.

Una amplia variedad de autores, cómplices y espectadores pasivos mantiene y amplifica el ciclo de la ciberviolencia contra las mujeres y las niñas.

La ciberviolencia es perpetrada por una amplia variedad de personas, entre las que se incluyen compañeros, parejas sentimentales y grupos organizados. El anonimato digital facilita y amplifica el abuso, reduciendo la rendición de cuentas y permitiendo la propagación de comportamientos nocivos. Además de los agresores principales, los actores secundarios que comparten y reaccionan ante contenidos abusivos contribuyen de manera significativa a su perpetuación. Los espectadores también desempeñan un papel fundamental: aunque algunos pueden intervenir, muchos permanecen pasivos debido a la presión social y al miedo a las represalias. Las conclusiones de los grupos focales muestran que los chicos, en particular, pueden actuar tanto como agresores como aliados potenciales. Actos como el intercambio de imágenes sin consentimiento o el acoso en grupo suelen discutirse como actuaciones destinadas a impresionar a los demás o a ajustarse a las expectativas de los compañeros. Esta ambivalencia subraya la necesidad de realizar mayores esfuerzos para fomentar la empatía y la responsabilidad entre los espectadores.

Las desigualdades interseccionales aumentan la vulnerabilidad y agravan el impacto de la ciberviolencia en los grupos marginados.

Los resultados subrayan que la ciberviolencia viene determinada por identidades que se entrecruzan y por desigualdades estructurales. Factores como la discapacidad, el origen étnico, la religión, la identidad de género y la situación socioeconómica agravan el riesgo, ya que las niñas y las jóvenes marginadas se enfrentan a una mayor exposición a la ciberviolencia y cuentan con menos vías de apoyo. Las participantes en los grupos focales destacan cómo los espacios en línea suelen reproducir los sistemas de opresión del mundo real —como el sexismo, el racismo y el abuso transfóbico—, lo que hace que ciertos grupos sean más visibles, se conviertan en blanco de ataques y estén menos protegidos. Estas desigualdades no solo aumentan la probabilidad de sufrir ciberviolencia, sino que también intensifican sus consecuencias emocionales y sociales.

La discriminación sistémica y el acceso desigual a la justicia agravan aún más estas vulnerabilidades. Las niñas y las jóvenes marginadas suelen enfrentarse a importantes obstáculos a la hora de buscar protección, entre ellos la desconfianza hacia las instituciones, el desconocimiento de sus derechos legales y el acceso limitado a asistencia jurídica asequible.
Por lo tanto, abordar la ciberviolencia contra las mujeres y las niñas requiere un enfoque interseccional que reconozca cómo las formas superpuestas de desventaja amplifican el daño y perpetúan las desigualdades.

La ciberviolencia tiene consecuencias psicológicas, emocionales y relacionales duraderas que se extienden mucho más allá del ámbito digital, afectando profundamente a la salud mental, la confianza social y el sentido de identidad de las víctimas.

El espectro de la ciberviolencia se extiende más allá del ámbito digital, causando daños psicológicos, emocionales y relacionales duraderos. Las repercusiones psicológicas y sociales de dicha violencia son profundas, y las víctimas suelen referir altos niveles de ansiedad, depresión, trauma y disminución de la autoestima que tienen consecuencias a largo plazo para su salud mental y sus relaciones. Muchos adolescentes describen experiencias de aislamiento social y desconfianza, utilizando en ocasiones términos como «depresión», «suicidio» y «trauma» para expresar su angustia. El miedo al estigma, a que se culpe a la víctima y al daño a la reputación desalienta aún más la denuncia, perpetuando así los ciclos de silencio.

El carácter duradero del abuso en línea —con contenidos nocivos capaces de resurgir mucho tiempo después del suceso inicial— hace que sus efectos emocionales, psicológicos y relacionales permanezcan profundamente arraigados y sean de larga duración. Además, más allá de sus repercusiones en el individuo, la exposición repetida al abuso en línea también contribuye a la normalización de la violencia. Los jóvenes han empezado a considerar el ciberacoso y el hostigamiento como aspectos inevitables de la vida digital, algo que hay que soportar en lugar de combatirlo. Esta normalización no solo magnifica el impacto emocional de la ciberviolencia, sino que también afianza patrones de aceptación y desinterés, lo que refuerza su impacto duradero tanto en el ámbito digital como en el social.

La Directiva de la UE sobre la violencia contra las mujeres ofrece un marco común muy necesario en lo que respecta a las definiciones y los mecanismos de aplicación. Para obtener resultados, debería darse prioridad a su transposición íntegra al Derecho nacional y a su aplicación.

Los esfuerzos para hacer frente a la ciberviolencia contra las mujeres y las niñas se ven obstaculizados actualmente por la gran variedad de definiciones utilizadas en los distintos Estados miembros y jurisdicciones, así como por la rápida evolución de las tecnologías digitales, incluida la inteligencia artificial. Las diversas manifestaciones de la violencia cibernética —que van desde el acoso hasta el abuso basado en imágenes— y el amplio espectro de motivaciones y dinámicas relacionales que conlleva requieren una comprensión matizada e intervenciones sensibles al contexto. Estas también deben tener en cuenta factores culturales, institucionales y sociales más amplios, incluidas las normas de género arraigadas que normalizan la agresión masculina y la culpabilización de las víctimas, las dinámicas entre iguales que premian el comportamiento abusivo y refuerzan los dobles raseros, la influencia de las subculturas en línea y la pornografía en la configuración de actitudes misóginas, y los patrones institucionales que excusan la conducta dañina de los chicos al tiempo que no protegen ni dan crédito a las chicas.

La Directiva sobre la violencia contra las mujeres ofrece definiciones claras que pueden servir de base para el desarrollo de indicadores armonizados, procesos de recopilación de datos y evaluaciones de seguimiento y de políticas. Como tal, tiene el potencial de promover una mayor coherencia y coordinación entre los Estados miembros.

Los actuales sistemas de prevención, educación y apoyo no reflejan las realidades digitales de los jóvenes, lo que conduce al aislamiento y a la falta de confianza, y deja a muchos sin una protección eficaz.

Los resultados revelan una desconexión significativa entre los esfuerzos de prevención existentes y las experiencias vividas por los adolescentes. Durante los grupos de discusión, las niñas expresaron su frustración con las campañas escolares, las respuestas de los adultos y los padres, y los mecanismos institucionales que percibían como obsoletos, superficiales o desconectados de sus vidas digitales.

Las campañas escolares sobre ciberseguridad se consideran ineficaces porque no abordan las plataformas, prácticas y riesgos reales a los que se enfrentan los jóvenes a diario.

Los adolescentes expresaron de forma sistemática que los adultos subestiman la importancia de los espacios en línea y la gravedad del daño que sufren en ellos. En lugar de reconocer y validar estas experiencias, a menudo se percibe que los adultos las minimizan. Esta falta de comprensión agrava los sentimientos de aislamiento e invalidación, especialmente cuando los jóvenes buscan ayuda en instituciones como los colegios o los servicios de asesoramiento. Muchos describieron respuestas institucionales incoherentes o mal coordinadas, incluyendo violaciones de confidencialidad y la minimización de sus experiencias, lo que erosiona la confianza y disuade de seguir revelando lo sucedido.

Esta discrepancia socava la confianza en los mecanismos de prevención y apoyo, lo que desalienta a los jóvenes a denunciar y deja a muchos adolescentes sin la protección adecuada. Las barreras estructurales agravan aún más el problema: los jóvenes suelen carecer de información clara sobre dónde buscar ayuda y, en las comunidades más pequeñas, el miedo a la exposición pública o a los chismes actúa como un poderoso factor disuasorio.

En conjunto, los resultados ponen de relieve tanto los avances como los retos persistentes. La ciberviolencia contra las mujeres y las niñas está firmemente arraigada en el continuo de la violencia de género y no puede abordarse al margen de contextos sociales, culturales e institucionales más amplios. Si bien la política de la UE ha evolucionado hasta reconocer la complejidad y la urgencia del abuso digital, las lagunas en su aplicación y las diferentes respuestas de los Estados miembros siguen limitando su eficacia. De cara al futuro, son esenciales enfoques coordinados, interseccionales y centrados en los jóvenes para garantizar una prevención, una protección y una rendición de cuentas significativas en toda la UE.

7 Recomendaciones políticas

La lucha contra la ciberviolencia contra las mujeres y las niñas en toda la UE requiere estrategias y acciones coordinadas y multinivel en las que participen tanto las instituciones de la UE como los Estados miembros. También requiere la armonización entre las directivas de la UE, la legislación nacional y los marcos de aplicación locales. Las recomendaciones de esta investigación pueden agruparse en cuatro ámbitos interrelacionados: prevención y educación, marcos jurídicos y políticos sobre la ciberviolencia, apoyo y protección a las víctimas, y seguimiento y evaluación.

Prevención y educación

Garantizar una prevención temprana y sensible al género que refleje las realidades digitales de las niñas y los niños.

- Introducir en las escuelas de primaria y secundaria planes de estudios obligatorios de alfabetización digital con perspectiva de género, que abarquen la identidad digital, las huellas digitales, las interacciones en línea y la detección de desinformación (incluidos los «deepfakes» y los contenidos manipulados). Para lograrlo, basarse en ejemplos nacionales cuyo impacto positivo haya quedado demostrado.

- Promover una cultura del autocuidado digital en las instituciones educativas, sensibilizando a los alumnos y al personal docente sobre la seguridad digital (por ejemplo, la configuración de la privacidad, la documentación segura de pruebas y las herramientas de denuncia) mediante «evaluaciones periódicas de seguridad digital» en los centros educativos, en las que los alumnos revisen su presencia en línea y su configuración de privacidad con apoyo guiado.

- Incluir objetivos de aprendizaje específicos para los niños y los jóvenes varones sobre las normas de género masculinas, la presión de grupo, la responsabilidad y el papel de la complicidad en la ciberviolencia.

- Integrar en los planes de estudios escolares, el trabajo con jóvenes y los programas de alfabetización digital una formación sobre la intervención de los testigos basada en datos empíricos, con el fin de enseñar a los jóvenes cómo intervenir, denunciar, impedir o apoyar de forma segura a un compañero que sea objeto de acoso en línea. Para ello, basarse en programas exitosos de intervención de los testigos de servicios de apoyo especializados centrados en la violencia contra las mujeres.

Garantizar que las iniciativas de prevención se diseñen conjuntamente con las niñas y respondan a sus experiencias.

- Colaborar con organizaciones de la sociedad civil dirigidas por jóvenes y de base comunitaria, especialmente aquellas que trabajan con grupos diversos de jóvenes, utilizando una pedagogía participativa para aprovechar la inteligencia colectiva, al tiempo que se reconoce la experiencia de los jóvenes en las prácticas digitales.

- Diseñar conjuntamente con los adolescentes programas de prevención, garantizando que sus materiales educativos aborden la ciberviolencia, incluidos el abuso sexualizado, la violencia basada en imágenes y los discursos que culpan a las víctimas.

- Promover iniciativas de apoyo dirigidas por compañeros y compañeras, en las que niñas y niños formados puedan hablar sobre el acoso, la coacción y las relaciones digitales saludables, creando así espacios seguros para compartir experiencias.

- Garantizar que la participación de niñas y niños en la cocreación no se traduzca en un traspaso de responsabilidad hacia las víctimas. Con este fin, esforzarse por proporcionar un espacio seguro para que se escuchen sus voces y se valoren sus conocimientos, al tiempo que se garantiza que las víctimas reciban apoyo profesional especializado.

- Proporcionar a los padres y cuidadores orientación práctica sobre la crianza en el ámbito digital, incluidas herramientas y recursos que les ayuden a detectar y abordar el abuso en línea de forma temprana.

Cuestionar las normas de género nocivas y abordar los riesgos que se entrecruzan.

- Desarrollar programas específicos para chicos que cuestionen las normas sociales sexistas y ofrezcan alternativas positivas a través de modelos a seguir, tutorías y debates dirigidos por jóvenes sobre el respeto, el consentimiento y las relaciones saludables. Dichos programas pueden basarse en planes de estudios de educación sexual integral e integrarse en ellos.

- Crear iniciativas de divulgación específicas para las niñas que se enfrentan a formas de discriminación que se entrecruzan (por ejemplo, niñas migrantes, niñas con discapacidad, jóvenes LGBTIQ+) con el fin de abordar sus riesgos específicos en línea y las barreras que les impiden acceder al apoyo.

Integrar la prevención en marcos políticos más amplios, tanto a nivel de la UE como nacional.

- Financiar grupos consultivos juveniles estructurados para que aporten información a las estrategias de prevención a nivel nacional y de la UE.
- Financiar campañas a escala de la UE en las que se den voz a las niñas para desestigmatizar la denuncia del abuso de imágenes íntimas y poner de relieve los daños que supone cometer y compartir dicho contenido.
- Garantizar que se aplique la prevención de la violencia de género en línea mediante la plena implementación de la legislación y los marcos políticos de la UE existentes, incluidos el plan de acción de la Comisión Europea contra el ciberacoso ([58]), la Ley de Servicios Digitales (DSA), la estrategia de la UE sobre los derechos del niño, la estrategia de la UE para la juventud y la Directiva sobre la violencia contra las mujeres.

Fomentar y apoyar las innovaciones tecnológicas que mejoren la prevención de la ciberviolencia.

- Promover la incorporación de la responsabilidad en el diseño de las plataformas y los productos para anticipar las formas en que las características técnicas de las plataformas pueden ser objeto de uso indebido con fines de abuso.
- Garantizar que las plataformas de redes sociales inviertan en el desarrollo de soluciones tecnológicas innovadoras para anticipar, detectar y disuadir los actos de ciberviolencia dirigidos específicamente contra las niñas y las mujeres jóvenes.
- Garantizar que las plataformas refuercen la disuasión mediante herramientas de mensajería (por ejemplo, avisos emergentes antes de compartir imágenes no consentidas) y herramientas técnicas (por ejemplo, sistemas de detección basados en imágenes que señalen posibles infracciones). Dichas medidas pueden moldear el comportamiento de los usuarios de forma proactiva y tienen una fuerte función preventiva.
- Exigir la detección y moderación proactivas de las tendencias nocivas, especialmente aquellas dirigidas a las niñas y a los jóvenes LGBTIQ+.

Mejorar la cooperación a escala de la UE en materia de hash de imágenes y bases de datos de imágenes no consentidas.

- Aprovechando las plataformas existentes, como «Stop Non-consensual Intimate Image Abuse», facilitar la colaboración entre la Agencia de Ciberseguridad de la Unión Europea, los centros nacionales de ciberseguridad y las organizaciones de terceros de confianza.
- Apoyar la interoperabilidad y la normalización de las bases de datos de hash de imágenes para permitir la detección y eliminación coherentes de contenidos nocivos en todas las plataformas.
- Garantizar que los mecanismos de denuncia de las víctimas a nivel nacional estén directamente vinculados a estas infraestructuras técnicas, de modo que, una vez que una imagen haya sido sometida a hash y señalada, sea reconocida y bloqueada en múltiples servicios.

58 «Plan de acción contra el ciberacoso: proteger a los niños en Internet» — Comisión Europea.

Marcos jurídicos y normativos sobre la ciberviolencia

Garantizar una regulación y una aplicación sólidas y armonizadas en toda la UE.

- Reafirmar la voluntad política y el compromiso de la UE de hacer cumplir y desarrollar los marcos jurídicos existentes, especialmente la Ley de Servicios Digitales (DSA), la Ley de Inteligencia Artificial (AI Act) y el Reglamento General de Protección de Datos (RGPD). En el contexto de los debates en curso sobre el paquete ómnibus digital, defender las garantías fundamentales.
- Garantizar la plena aplicación de la DSA y la transposición y aplicación íntegras de la Ley de IA y de la Directiva sobre la violencia contra las mujeres, incluidas las obligaciones específicas de género en materia de prevención, denuncia y apoyo a las víctimas.
- Utilizar definiciones comunes y armonizadas de las diferentes formas de violencia cibernética establecidas por la Directiva de la UE sobre la violencia contra las mujeres y el marco de medición de la violencia cibernética contra las mujeres y las niñas elaborado por el EIGE, con el fin de facilitar la recopilación de datos comparables y desglosados por sexo a escala de la UE sobre la violencia de género en línea.
- Fomentar y perseguir una coordinación plena entre las instituciones nacionales y el Consejo Europeo de Servicios Digitales para supervisar y mejorar el cumplimiento de los requisitos de la DSA por parte de las plataformas de redes sociales.
- Difundir y fomentar el cumplimiento de las directrices de la Comisión Europea sobre la protección de los menores en línea, adoptadas en julio de 2025.

Reforzar la sensibilización y los protocolos de ciberseguridad de los Estados miembros para responder mejor a la violencia cibernética.

- Desarrollar vías de derivación claras a escala de la UE para que los servicios de apoyo nacionales puedan acceder a conocimientos técnicos especializados, ya sea a través de centros nacionales de ciberseguridad, equipos de respuesta a incidentes de seguridad informática o unidades de las fuerzas del orden. Dichos conocimientos proporcionarían a los profesionales el apoyo técnico adecuado para responder a los casos de abuso facilitados por la tecnología.
- Aprovechar los conocimientos especializados a nivel de la UE, por ejemplo los de la Agencia de Ciberseguridad de la Unión Europea, para reforzar estos vínculos mediante la promoción de orientaciones técnicas coherentes, la formación y el intercambio transfronterizo de información.
- Desarrollar vías de aprendizaje mutuo e intercambio de información a escala de la UE con el fin de aprovechar las iniciativas nacionales que hayan tenido éxito.
- Elaborar un protocolo de la UE para responder a la ciberviolencia en los centros educativos, en el que se detallen los pasos necesarios para la documentación, la denuncia, la conservación de pruebas y la colaboración entre las partes interesadas.

Exigir una fuerte responsabilidad por parte de las plataformas y la creación de herramientas de denuncia adaptadas a las víctimas.

- Promover la creación de mecanismos sólidos que supervisen el cumplimiento por parte de las plataformas de redes sociales de la Ley de Servicios Digitales (DSA) y de la Directiva de la UE sobre la violencia contra las mujeres, especialmente en lo que respecta a sus prácticas de moderación, la notificación de incidentes y el apoyo a los usuarios. La creación de un organismo de supervisión independiente podría proporcionar una coordinación y un control útiles.
- Aumentar el número y la visibilidad de los denunciantes de confianza y terceros autorizados por la UE para facilitar la notificación rápida y la escalación de los casos relacionados con contenidos ilegales.
- Involucrar a los servicios de apoyo especializados en la violencia contra las mujeres en el desarrollo de mecanismos centrados en el usuario, anónimos y accesibles para denunciar incidentes de ciberviolencia a las plataformas digitales, incluyendo líneas de atención telefónica, aplicaciones móviles y portales en línea.
- Garantizar que los mecanismos de denuncia aborden la dimensión interseccional de la ciberviolencia. En particular, deben tenerse en cuenta las necesidades y los hábitos de denuncia de los usuarios de diferentes grupos de edad, especialmente los más jóvenes, para maximizar la accesibilidad de la denuncia.
- Garantizar que se cumplan las obligaciones de retirada previstas en la DSA, con plazos claros y notificaciones enviadas a las víctimas una vez que se haya eliminado el contenido.
- Incentivar a las plataformas para que adopten y respeten un código de conducta para combatir la ciberviolencia de género, elaborado en colaboración con la sociedad civil y los organismos de igualdad.

Establecer normas más estrictas para un diseño más seguro de las plataformas y una mitigación proactiva de los riesgos.

- Promover la creación de normas más estrictas para las plataformas que tengan en cuenta los perjuicios reales a los que se enfrentan las mujeres y las niñas en Internet e incluyan requisitos para:
- un diseño seguro de los productos y los algoritmos que reduzca la amplificación de contenidos nocivos y evite la revictimización;
- una evaluación de riesgos sólida y estrategias de protección, garantizando que las plataformas identifiquen y aborden de forma activa riesgos como el acoso en línea, los «deepfakes» y el abuso basado en imágenes.
- Exigir que se utilicen principios de diseño que tengan en cuenta el trauma y se centren en la víctima en los procesos de moderación y en el diseño de la interfaz.
- Introducir evaluaciones obligatorias del impacto de género en las evaluaciones de derechos fundamentales exigidas por la Ley de IA, incluidas auditorías de terceros para detectar y corregir los sesgos algorítmicos.
- Armonizar los requisitos de las plataformas en materia de verificación de la edad, diseño y seguridad de los usuarios con las directrices de la Comisión Europea para 2025 y la aplicación prototipo para un espacio en línea más seguro para los niños.
- Garantizar que estas medidas de verificación de la edad se apliquen de manera sensible al género, reconociendo que las niñas se enfrentan a riesgos específicos en entornos en línea.

Reforzar y garantizar la aplicación de la normativa sobre IA y tecnologías emergentes.

- Garantizar la aplicación de la Ley de IA.
- Garantizar que los instrumentos de gobernanza de la IA existentes en la UE —incluidas las directrices éticas para una IA fiable y el Código de prácticas sobre el marcado y el etiquetado de contenidos generados por IA— se apliquen plenamente y se refuercen con mecanismos vinculantes de rendición de cuentas.
- Abogar por que los riesgos relacionados con el género de la IA generativa, como la producción y difusión de «deepnudes», herramientas de «nudificación» y otras imágenes sintéticas no consentidas, se incluyan como «prácticas prohibidas» en virtud del artículo 5 de la Ley de IA.
- Garantizar que las normas técnicas elaboradas para los proveedores de IA incluyan mecanismos eficaces para la presentación de denuncias y su seguimiento, la eliminación de contenidos nocivos y la información a las víctimas de ciberviolencia sobre los servicios de apoyo.
- Garantizar que los organismos de igualdad y las organizaciones de la sociedad civil que trabajan en favor de la igualdad de género y los derechos fundamentales a escala nacional y de la UE cuenten con los recursos y la financiación suficientes para desempeñar su función como órganos consultivos con arreglo al artículo 77 de la Ley de IA.
- Garantizar que las víctimas de la violencia facilitada por la IA tengan acceso a vías de recurso y mecanismos de protección.

Apoyo y protección a las víctimas

Reforzar los servicios de apoyo centrados en las víctimas y los mecanismos de denuncia.

- Garantizar que todos los Estados miembros creen servicios de denuncia y apoyo para las víctimas de la ciberviolencia, de conformidad con las obligaciones vigentes en virtud del Convenio de Estambul (artículos 20 a 22), la Directiva sobre los derechos de las víctimas (2012/29/UE) y la Directiva de la UE sobre la violencia contra las mujeres, en relación con las respuestas rápidas y los servicios de apoyo especializados.
- Garantizar que los servicios de apoyo especializados centrados en la violencia contra las mujeres cuenten con los recursos y la financiación suficientes para prestar un apoyo especializado y adaptado al trauma, incluyendo apoyo técnico, servicios de salud mental y asistencia jurídica.
- Garantizar que el apoyo especializado a las víctimas de la ciberviolencia se adapte a los distintos grupos de edad de mujeres y niñas, en función de sus experiencias y necesidades.
- Desarrollar programas de intervención con los autores adecuados a la edad y adaptados específicamente a los menores, teniendo en cuenta su etapa de desarrollo y los diferentes mecanismos de responsabilidad que puedan aplicarse.

Reforzar la capacidad de los profesionales para responder de forma eficaz.

- Impartir formación obligatoria a los profesionales de primera línea (docentes, trabajadores sociales, policías, personal sanitario) sobre la naturaleza de género de la ciberviolencia y los patrones específicos de cada plataforma.
- Establecer puntos nacionales de asistencia técnica que permitan a los profesionales acceder a conocimientos especializados en ciberseguridad procedentes de instituciones públicas u organizaciones de la sociedad civil especializadas.
- Garantizar una financiación sostenible para las organizaciones de la sociedad civil que llevan a cabo intervenciones en los centros educativos y para las organizaciones especializadas en la sensibilización de los jóvenes sobre temas digitales y de igualdad de género, con el fin de prevenir la ciberviolencia y los deepfakes generados por IA.

Apoyar a las familias, los cuidadores y los educadores en las intervenciones y respuestas tempranas.

- Proporcionar a los padres y cuidadores orientación práctica sobre la crianza en la era digital, incluidas herramientas y recursos que les ayuden a detectar y abordar a tiempo los abusos en línea.
- Exigir a los centros escolares y otras instituciones educativas que establezcan políticas y protocolos claros sobre cómo actuar en casos de abuso facilitado por la tecnología para proteger a las víctimas.
- Exigir a los centros escolares y otras instituciones educativas que definan y comuniquen consecuencias claras para los autores de ciberviolencia (por ejemplo, expedientes disciplinarios, anotaciones en los boletines escolares, expulsión temporal o permanente y las medidas propuestas en estos casos).
- Sensibilizar a los padres y cuidadores sobre las vías legales civiles de que disponen las víctimas para exigir responsabilidades y obtener reparaciones civiles.

Fomentar la colaboración y la innovación entre las distintas partes interesadas.

- Facilitar la cooperación entre los gobiernos, la sociedad civil, los investigadores, las escuelas y otros centros educativos, y las empresas tecnológicas, promoviendo el intercambio de datos y buenas prácticas entre las partes interesadas para mejorar la prevención y la respuesta.
- Introducir protocolos de respuesta a nivel de la UE con la participación de múltiples partes interesadas para centros escolares y entornos juveniles, aclarando las funciones de los educadores, la policía, los servicios sociales, las plataformas y los organismos de ciberseguridad.
- Apoyar el desarrollo de soluciones tecnológicas innovadoras adaptadas a la naturaleza rápidamente cambiante de la ciberviolencia.

Seguimiento y evaluación

Establecer un marco armonizado de seguimiento y rendición de cuentas a escala de la UE.

- Garantizar que los planes de acción nacionales se utilicen para realizar un seguimiento sistemático de la aplicación por parte de los Estados miembros de la Directiva sobre la violencia contra las mujeres, incluidas sus disposiciones en materia de prevención, protección, acceso a la justicia y ciberviolencia.
- Garantizar la evaluación periódica del cumplimiento por parte de los Estados miembros para asegurar normas armonizadas, identificar las deficiencias en la aplicación y respaldar las medidas correctivas cuando no se cumplan las obligaciones derivadas de la Directiva.
- Abogar por que la Comisión Europea publique informes periódicos de seguimiento sobre la violencia cibernética basados en las obligaciones de recopilación de datos de los Estados miembros en virtud de la Directiva sobre la violencia contra las mujeres y la Ley de Servicios Digitales (DSA).

Garantizar que la recopilación de datos refleje la diversidad de las experiencias de las víctimas.

- En colaboración con las instituciones pertinentes a nivel de la UE y nacional, recopilar datos sobre todas las formas de violencia de género, incluida la ciberviolencia, que puedan desglosarse por sexo, edad, origen étnico, discapacidad y situación socioeconómica.
- Garantizar que las experiencias específicas de los grupos que se enfrentan a formas de discriminación que se entrecruzan queden reflejadas en la investigación y durante la recopilación de datos.
- Garantizar que la ciberviolencia y otras formas de violencia contra las mujeres facilitadas por la tecnología se integren en futuras encuestas de victimización a escala de la UE.

Invertir en investigación a largo plazo y basada en datos empíricos sobre los efectos y las tendencias.

- De conformidad con el artículo 44 de la Directiva sobre la violencia contra las mujeres, garantizar una asignación presupuestaria adecuada para la investigación específica sobre la ciberviolencia en el marco financiero plurianual actual y futuro.
- Apoyar la investigación longitudinal para comprender los efectos psicológicos a largo plazo de la ciberviolencia.
- Investigar las consecuencias sociales y económicas de la ciberviolencia a lo largo del tiempo.

Referencias

- Adam, A. (2002), «Cyberstalking and internet pornography: Gender and the gaze», Ethics and Information Technology, vol. 4, n.º 2, pp. 133-142, https://doi.org/10.1023/A:1019967504762.
- Afrouz, R. y Vassos, S. (2024), «Adolescents' experiences of cyber-dating abuse and the pattern of abuse through technology, a scoping review», Trauma, Violence, & Abuse, vol. 25, n.º 4, pp. 2814-2828, https://doi.org/10.1177/15248380241227457.
- Allison, K. R. y Bussey, K. (2016), «La actitud de los espectadores en el ciberacoso en su contexto: una revisión de la literatura sobre las respuestas de los testigos al ciberacoso», Children and Youth Services Review, vol. 65, pp. 183-194, https://doi.org/10.1016/j.childyouth.2016.03.026.
- Asamblea Nacional (2019), Ley n.º 2020-766, de miércoles 24 de junio de 2020, destinada a luchar contra los contenidos que incitan al odio en Internet, https://www.assemblee-nationale.fr/dyn/15/dossiers/lutte_contre_haine_internet.
- Azzarito, L., Simon, M. y Marttinen, R. (2017), «"Up against whiteness": Rethinking race and the body in a global era», Sport, Education and Society, vol. 22, n.º 5, pp. 635-657, https://doi.org/10.1080/13573322.2015.1136612.
- Baas, N., de Jong, M. D. T. y Drossaert, C. H. C. (2013), «Children's perspectives on cyberbullying: Insights based on participatory research», *Cyberpsychology, Behavior, and Social Networking*, vol. 16, n.º 4, pp. 248-253, https://doi.org/10.1089/cyber.2012.0079.
- Backe, E. L., Lilleston, P. y McCleary-Sills, J. (2018), «Individuos conectados en red, violencia de género: una revisión bibliográfica sobre la ciberviolencia», Violence and Gender, vol. 5, n.º 3, pp. 135-146, https://doi.org/10.1089/vio.2017.0056.
- Barlińska, J., Szuster, A. y Winiewski, M. (2013), «Ciberacoso entre adolescentes espectadores: el papel del medio de comunicación, la forma de violencia y la empatía», Journal of Community & Applied Social Psychology, vol. 23, n.º 1, pp. 37-51, https://doi.org/10.1002/casp.2137.
- Chawki, M., Basu, S. y Choi, K. (2024), «Redefiniendo los límites en el metaverso: cómo afrontar los retos del daño virtual y la seguridad de los usuarios», Laws, vol. 13, n.º 3, https://www.mdpi.com/2075-471X/13/3/33.
- Chiang, J., Chang, F. y Lee, K. (2021), «Transiciones en la agresividad entre los niños: efectos del género y la exposición a la violencia en línea», Aggressive Behavior, vol. 47, n.º 3, pp. 310-319, https://doi.org/10.1002/ab.21944.

- Connell, R. W. (2005), Masculinities, 2.ª edición, Polity Press, Cambridge.
- Cosma, A., Molcho, M. y Pickett, W. (2024), «Un enfoque sobre la violencia entre iguales y el acoso escolar en adolescentes en Europa, Asia Central y Canadá – Comportamiento en materia de salud de los niños en edad escolar: Informe internacional de la encuesta 2021/2022», volumen 2, Oficina Regional de la OMS para Europa, Copenhague, https://www.who.int/europe/publications/i/item/9789289060929.
- Consejo de Europa (2001), «Convenio sobre la ciberdelincuencia», Serie de Tratados Europeos, n.º 185, Budapest, 23 de noviembre, https://rm.coe.int/1680081561.
- Consejo de Europa (2007), «Convenio del Consejo de Europa sobre la protección de los niños contra la explotación y el abuso sexuales», Serie de Tratados del Consejo de Europa, n.º 201, 25 de octubre, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201.
- Consejo de Europa (2011), «Convenio del Consejo de Europa sobre la prevención y la lucha contra la violencia contra las mujeres y la violencia doméstica», Serie de Tratados del Consejo de Europa, n.º 210, https://rm.coe.int/168008482e.
- Consejo de Europa (2018), Estudio de análisis sobre la ciberviolencia: con las recomendaciones adoptadas por el T-CY el 9 de julio de 2018, Comité del Convenio sobre la Ciberdelincuencia, Estrasburgo, https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914.
- Consejo de Europa (2020), Manual para responsables políticos sobre los derechos del niño en el entorno digital, Estrasburgo.
- Consejo de Europa (2023), «Riesgos y oportunidades del metaverso».
- Cybersafe (2020), «Ciberviolencia contra las mujeres y las niñas: informe», Universidad de Liubliana.
- DeKeseredy, W. S. y Schwartz, M. D. (2013), «Apoyo entre hombres y violencia contra las mujeres: historia y verificación de una teoría», Northeastern University Press, Boston, MA.
- De Vido, S. (2024), «Los deepfakes como violencia contra las mujeres generada por la IA», ponencia en la Conferencia Mundial sobre IA y Derechos Humanos, Liubliana, 13 y 14 de junio.
- Domínguez-Hernández, F., Bonell, L. y Martínez-González, A. (2018), «Una revisión sistemática de la literatura sobre los factores que moderan las acciones de los testigos en el ciberacoso», *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 12, n.º 4, https://doi.org/10.5817/CP2018-4-1.
- Dunn, S. (2020), «Violencia de género facilitada por la tecnología: una visión general», Supporting a Safer Internet Papers, n.º 1, Centro para la Innovación en Gobernanza Internacional, Waterloo, Canadá, https://www.jstor.org/stable/resrep27513.
- EIGE (2021), «Inteligencia artificial, trabajo en plataformas e igualdad de género», Oficina de Publicaciones de la Unión Europea, Luxemburgo, https://data.europa.eu/doi/10.2839/53252.
- EIGE (2022), «Lucha contra la ciberviolencia contra las mujeres y las niñas», Oficina de Publicaciones de la Unión Europea, Luxemburgo, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf.
- EIGE (2024), Lucha contra la ciberviolencia contra las mujeres y las niñas: el papel de las plataformas digitales, Oficina de Publicaciones de la Unión Europea, Luxemburgo, https://data.europa.eu/doi/10.2839/1955989.
- EIGE (2025), «De la percepción a la política: Desmantelar los estereotipos de género en la Unión Europea», Oficina de Publicaciones de la Unión Europea, Luxemburgo, https://data.europa.eu/doi/10.2839/7052284.

- El Comisionado de eSafety y la Autoridad Australiana de Comunicaciones y Medios de Comunicación (ACMA), 2022. Informe anual 2021-2022, https://www.esafety.gov.au/sites/default/files/2022-10/ACMA%20and%20eSafety%20annual%20report%202021-22.pdf?v=1776941478076
- Parlamento Europeo (2016), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46/CE (DO L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
- Parlamento Europeo (2021a), Resolución del Parlamento Europeo, de 14 de diciembre de 2021, con recomendaciones a la Comisión sobre la lucha contra la violencia de género: ciberviolencia (2020/2035(INL)) (DO C 251, 30.6.2022, p. 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_251_R_0002).
- Parlamento Europeo: Dirección General de Servicios de Investigación Parlamentaria (2024), «Ciberviolencia contra las mujeres en la UE», https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI%282024%29767146_EN.pdf.
- Europol (Agencia de la Unión Europea para la Cooperación Policial) (2017), «La coacción y la extorsión sexuales en línea como forma de delito que afecta a los niños: perspectiva de las fuerzas del orden», La Haya, online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.
- EWL (Lobby Europeo de las Mujeres) (2017), #HerNetHerRights: Análisis de la situación de la violencia en línea contra las mujeres y las niñas en Europa, Bruselas.
- Comisión FEMM (Comisión de Derechos de la Mujer e Igualdad de Género) y van der Wilk, A. (2018), «Ciberviolencia y discurso de odio en línea contra las mujeres».
- Foster, A. (2023). Adolescentes australianos, víctimas de retorsiones sexuales pervertidas. News.com.au. https://www. news.com.au/technology/online/security/australian-teenagers-targeted-by-sick-sextortion-scams/news-story/ae6975b8308917f611b03fa99bd2b0d9
- FRA (Agencia de los Derechos Fundamentales de la Unión Europea) (2015), Violencia contra las mujeres: una encuesta a escala de la UE. Principales resultados, Oficina de Publicaciones de la Unión Europea, Luxemburgo.
- FRA (2017), Segunda encuesta de la Unión Europea sobre minorías y discriminación: los musulmanes. Conclusiones seleccionadas, Oficina de Publicaciones de la Unión Europea, Luxemburgo, https://doi.org/10.2811/072254.
- Freed, D., Consolvo, S., Cosley, D., Kelley, P. G., Ricart, E. et al. (2025), «Estrategias de búsqueda de ayuda y de afrontamiento ante el abuso facilitado por la tecnología que sufren los jóvenes», Proceedings of the ACM on Human–Computer Interaction, vol. 9, n.º 2, pp. 1-25, https://doi.org/10.1145/3710992.
- Gámez-Guadix, M., Sorrel, M. A. y Martínez-Bacaico, J. (2022), «Perpetración y victimización de la violencia sexual facilitada por la tecnología entre adolescentes: un análisis de redes», Sexuality Research and Social Policy, vol. 20, pp. 1000-1012, https://doi.org/10.1007/s13178-022-00775-y.
- Gius, C. (2023), «(Re)pensar el género en la ciberviolencia. Reflexiones a partir de campañas de sensibilización sobre la violencia en línea contra las mujeres y las niñas en Italia», Media Education, vol. 14, n.º 2, pp. 95-106, https://doi.org/10.36253/me-14896.
- Gobierno de Bélgica (2021), Plan de acción nacional de lucha contra la violencia de género
- Gilen, A., Van Damme, E., Walrave, M., Giacometti, M., Ponnet, K. y Hardyns, W. (2025). La violencia digital en el contexto de las citas y las relaciones de pareja en Bélgica. Instituto para la Igualdad entre Mujeres y Hombres, https://igvm-iefh.belgium.be/fr/documentation/la-violencia-digital-en-el-contexto-de-las-citas-y-las-relaciones-entre-parejas
- GREVIO (Grupo de Expertos sobre la Acción contra la Violencia hacia las Mujeres y la Violencia Doméstica) (2021), Recomendación General n.º 1 del GREVIO sobre la dimensión digital de la violencia contra las mujeres – Aprobada

el 20 de octubre de 2021, Consejo de Europa, Estrasburgo, https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

- Gurumurthy, A. y Menon, N. (2009), «Violencia contra las mujeres a través del ciberespacio», Economic and Political Weekly, vol. 44, n.º 40, pp. 19-21, https://www.jstor.org/stable/25663650.
- Hicks, J. (2021), «Datos globales sobre la prevalencia y el impacto de la violencia de género en línea (OGBV)», Instituto de Estudios sobre el Desarrollo, https://doi.org/10.19088/K4D.2021.140.
- Janickyj, M. y Tanczer, L. M. (2025), «Perfiles de abuso tecnológico: análisis de los comportamientos de búsqueda de ayuda y las necesidades de apoyo de las víctimas y supervivientes de abusos facilitados por la tecnología», Actas de los resúmenes ampliados de la Conferencia CHI sobre Factores Humanos en Sistemas Informáticos, 509, pp. 1-11, https://doi.org/10.1145/3706599.3719986.
- Koukopoulos, N., Janickyj, M. y Tanczer, L. M. (2025), «Definición y conceptualización del abuso facilitado por la tecnología («abuso tecnológico»): resultados de un estudio Delphi a escala mundial», Journal of Interpersonal Violence, vol. 41, n.º 1-2, https://doi.org/10.1177/08862605241310465.
- Leonhardt, M. y Overå, S. (2021), «¿Existen diferencias en el uso de videojuegos y redes sociales entre niños y niñas? — Un enfoque de métodos mixtos—», International Journal of Environmental Research and Public Health, vol. 18, n.º 11, https://doi.org/10.3390/ijerph18116085.
- López-Castro, L. y Priegue, D. (2019), «Influencia de las variables familiares en la perpetración y la victimización por ciberacoso: una revisión sistemática de la literatura», Social Sciences, vol. 8, n.º 3, 98, https://doi.org/10.3390/socsci8030098.
- López-Castro, L., Smith, P. K., Robinson, S. y Görzig, A. (2023), «Diferencias de edad en la victimización y la perpetración del acoso: Evidencia de encuestas transculturales», Aggression and Violent Behavior, vol. 73, 101888, https://doi.org/10.1016/j.avb.2023.101888.
- Lu, Y., Van Ouytsel, J. y Temple, J. R. (2021), «Abuso en las relaciones sentimentales presenciales y en línea: una investigación longitudinal», Journal of Social and Personal Relationships, vol. 38, n.º 12, pp. 3713-3731, https://doi.org/10.1177/02654075211065202.
- Machado, B., Caridade, S., Araújo, I. y Lobato Faria, P. (2022), «Mapping the cyber interpersonal violence among young populations: A scoping review», Social Sciences, vol. 11, n.º 5, p. 207, https://doi.org/10.3390/socsci11050207.
- McGraw, D. K. (1995), «El acoso sexual en el ciberespacio: el problema del correo electrónico no deseado», Rutgers Computer and Technology Law Journal, vol. 21, pp. 491-518, https://api.semanticscholar.org/ CorpusID:64276291.
- Mclocklin, G., Kellezi, B., Stevenson, C. y Mackay, J. (2024), «Decisiones de revelación y experiencias en la búsqueda de ayuda entre las víctimas-supervivientes de la distribución no consentida de imágenes íntimas», Victims & Offenders, vol. 20, n.º 7, pp. 1258–1284, https://doi.org/10.1080/15564886.2024.2329107.
- Mukred, M., Mokhtar, U. A., Moafa, F. A., Gumaei, A., Sadiq, A. S. et al. (2024), «Las raíces de la agresión digital: análisis de la ciberviolencia a través de una revisión sistemática de la literatura», International Journal of Information Management Data Insights, vol. 4, n.º 2, 100281, https://doi.org/10.1016/j. jjimei.2024.100281.
- Murphy, C. (2024), «El ciberacoso entre los jóvenes: leyes y políticas en determinados Estados miembros», Informe del Servicio de Investigación del Parlamento Europeo, PE 7662.331, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762331/EPRS_BRI(2024)762331_EN.pdf.
- Academias Nacionales de Ciencias, Ingeniería y Medicina (2024), «La relación entre las redes sociales y la salud», en: Redes sociales y salud de los adolescentes, National Academies Press, Washington, D. C., pp. 91-136.
- Nixon, C. L. (2014) «Perspectivas actuales: el impacto del ciberacoso en la salud de los adolescentes», *Adolescent Health, Medicine and Therapeutics*, 5, pp. 143-158, https://doi.org/10.2147/AHMT.S36456.

- OEA (Organización de los Estados Americanos) (2021), Violencia de género en línea contra las mujeres y las niñas: Guía de conceptos básicos, Departamento de Estado de los Estados Unidos, Washington, D.C.
- Odink, I. (2024), «Lucha contra el abuso sexual infantil: revisión de la Directiva (2011/93/UE) —refundición», Nota informativa del Servicio de Investigación del Parlamento Europeo, PE 762.374, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2024)762374.
- Pichel, R., Foody, M., O'Higgins Norman, J., Feijóo, S., Varela, J. et al. (2021), «Acoso escolar, ciberacoso y su solapamiento: ¿qué tiene que ver la edad con ello?», Sustainability, vol. 13, n.º 15, https://doi.org/10.3390/ su13158527.
- PLAN International (2020), «State of the World's Girls 2020: ¿Libres para estar en línea? Las experiencias de las niñas y las jóvenes con el acoso en línea», Woking.
- Powell, A. y Henry, N. (2017), La violencia sexual en la era digital, Palgrave Macmillan, Londres.
- Proyecto deSHAME (Explotación digital y acoso sexual entre menores en Europa) (2017), Experiencias de los jóvenes con el acoso sexual en línea: un informe transnacional, Londres.
- Ratajczak, M. y Galzignato, E. (2019), «Niños migrantes y ciberviolencia. El problema del discurso de odio en Italia y Polonia», Peace Human Rights Governance, vol. 3, n.º 3, pp. 365-388.
- Ray, A. y Henry, N. (2024), «Sextorsión: una revisión exploratoria», *Trauma, Violence, & Abuse*, vol. 26, n.º 1, https://doi.org/10.1177/15248380241277271.
- Rudnicki, K., Vandebosch, H., Voué, P. y Poels, K. (2023), «Revisión sistemática de los determinantes y las consecuencias de las intervenciones de los testigos en el odio en línea y el ciberacoso entre adultos», Behaviour & Information Technology, vol. 42, n.º 5, pp. 527-544, https://doi.org/10.1080/0144929X.2022.2027013.
- Sala, A., Porcaro, L. y Gómez, E. (2024), «Uso de las redes sociales y salud mental y bienestar de los adolescentes: una revisión global», Computers in Human Behavior Reports, vol. 14, https://doi.org/10.1016/j.chbr.2024.100404.
- Salazar, M., Raj, A., Silverman, J. G., Rusch, M. L. A. y Reed, E. (2023), «Acoso sexual en Internet entre las adolescentes: un análisis cualitativo», *Adolescents*, vol. 3, n.º 1, pp. 84-91, https://doi.org/10.3390/adolescents3010007.
- Schittenhelm, C., Kops, M., Moosburner, M., Fischer, M. S. y Wachs, S. (2024), «La victimización por ciberacoso sexual entre los jóvenes: una revisión sistemática de las tasas de prevalencia, los factores de riesgo y las consecuencias», Adolescent Research Review, vol. 10, pp. 169-200, https://doi.org/10.1007/s40894-024-00248-w.
- Sciacca, B., Mazzone, A., Loftsson, M., O'Higgins Norman, J. y Foody, M. (2023), «Difusión no consentida de imágenes sexuales entre adolescentes: asociaciones con la depresión y la autoestima», Journal of Interpersonal Violence, vol. 38, núm. 15-16, pp. 9438-9464, https://doi.org/10.1177/08862605231165777.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E. et al. (2020), «EU Kids Online 2020: Resultados de la encuesta realizada en 19 países», EU Kids Online, https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf.
- Smith, D. (2023), «El papel del engaño en las citas en línea y las aplicaciones de citas», Canadian Journal of Family and Youth, vol. 15, n.º 2, pp. 23-32, https://doi.org/10.29173/cjfy29869.
- Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T. et al. (2010) «Factores de riesgo psicosociales asociados al ciberacoso entre adolescentes: un estudio poblacional», Archives of General Psychiatry, vol. 67, n.º 7, pp. 720-728, https://doi.org/10.1001/archgenpsychiatry.2010.79.
- Šulc, A., Vehovar, V., Brečko, B., Rucman, A. B. y Krainer, A. (2024), «Diferencias en la victimización y la perpetración del ciberacoso según la edad y la localidad en Eslovenia», Revija za kriminalistiko in kriminologijo, vol. 72, n.º 4, pp. 337-349, http://www.dlib.si/?URN=URN:NBN:SI:doc-F7LDTW5D.

- Sutton, S. y Finkelhor, D. (2023), «La identidad de los autores de delitos en línea contra menores: un metaanálisis», *Trauma, Violence, & Abuse*, vol. 25, n.º 3, pp. 1756-1768, https://doi.org/10.1177/15248380231194072.
- Thorn. (2024). Nueva investigación de Thorn: Aumento de la sextorsión financiera dirigida a adolescentes varones. https://www.thorn.org/blog/new-research-from-thorn-financial-sextortion-on-the-rise-targetting-teen-boys/
- ONU Mujeres y la OMS (Organización Mundial de la Salud) (2023), «Violencia contra las mujeres facilitada por la tecnología: balance de las pruebas y recopilación de datos», https://www.unwomen.org/en/digital-library/publications/2023/04/violencia-facilitada-por-la-tecnología-contra-las-mujeres-balance-de-las-pruebas-y-la-recopilación-de-datos.
- ONU Mujeres (2024b), Guía para jóvenes para poner fin a la violencia de género en línea, versión 3.
- Naciones Unidas (2018), A/HRC/38/47: Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, relativo a la violencia en línea contra las mujeres y las niñas desde una perspectiva de derechos humanos, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Ginebra, 18 de junio, https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and.
- USAID (Agencia de los Estados Unidos para el Desarrollo Internacional) (2023), DRG Learning Digest – Lucha contra la violencia de género facilitada por la tecnología en la política, marzo, https://content.govdelivery.com/accounts/USAIDHQ/bulletins/34c7e57.
- Van Ouytsel, J., Ponnet, K. y Walrave, M. (2020), «Abuso en las citas por Internet: investigación de los comportamientos de vigilancia digital entre adolescentes desde una perspectiva de aprendizaje social», Journal of Interpersonal Violence, vol. 35, n.º 23-24, pp. 5157-5178, https://doi.org/10.1177/0886260517719538.
- Vogels, E. A. (2022), «Los adolescentes y el ciberacoso en 2022», Pew Research Center, 15 de diciembre, https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.
- Vogler, S., Kappel, R. y Mumford, E. (2023), «Experiencias de abuso facilitado por la tecnología entre las minorías sexuales y de género», Journal of Interpersonal Violence, vol. 38, n.º 19-20, 11290-11313, https://doi.org/10.1177/08862605231179724.
- Wajcman, J. (2004), TechnoFeminism, Polity Press, Cambridge.
- Wajcman, J. (2010), «Teorías feministas de la tecnología», Cambridge Journal of Economics, vol. 34, n.º 1, pp. 143–152, https://doi.org/10.1093/cje/ben057.
- Wajcman, J. (2015), «Pressed for Time: The acceleration of life in digital capitalism», University of Chicago Press, Chicago.
- Wallace, A., Langevin, R. y Hébert, M. (2023), «An analysis of risk and protective factors associated with cyber-dating violence victimization of adolescent girls: An ecological perspective», Journal of Child & Adolescent Trauma, vol. 16, n.º 4, pp. 1017–1029, https://doi.org/10.1007/s40653-023-00558-6.
- WeProtect Global Alliance (2016), «Prevención y lucha contra la explotación y el abuso sexuales infantiles: un modelo de respuesta nacional», Londres.
- WeProtect Global Alliance (2021), «Material sexual "autogenerado" por menores en Internet: perspectivas de los niños y jóvenes», Londres.
- WeProtect Global Alliance (2024), «Primera estimación mundial de la magnitud de la explotación y el abuso sexual infantil en línea», disponible en: https://www.weprotect.org/blog/worlds-first-estimate-of-the-scale-ofonline-child-sexual-exploitation-and-abuse/
- Zweig, J. M., Lachman, P., Yahner, J. y Dank, M. (2014), «Correlatos del abuso en las relaciones sentimentales en línea entre adolescentes», Journal of Youth and Adolescence, vol. 43, n.º 8, pp. 1306-1321, https://doi.org/10.1007/ s10964-013-0047-x.

- Oficina del Gobierno de la República Checa (2021), Estrategia de Igualdad de Género para 2021-2030: Versión actualizada, Praga, https://vlada.gov.cz/assets/ppov/rovne-prilezitosti-zen-a-muzu/dokumenty/ Updated-Gender-Equality-Strategy-2021-2030---Condensed-Version.pdf.
- Olenik-Shemesh, D., Heiman, T. y Eden, S. (2017), «El comportamiento de los espectadores en episodios de ciberacoso: patrones activos y pasivos en el contexto de factores personales y socioemocionales», Journal of Interpersonal Violence, vol. 32, n.º 1, pp. 23-48, https://doi.org/10.1177/0886260515585531.
- Penado-Abilleira, M. y Rodicio-García, M. L. (2018), «Desarrollo y validación de una escala de violencia de género en adolescentes (ESVIGA)», Anuario de Psicología Jurídica, vol. 28, n.º 1, pp. 49-57, https://doi.org/10.5093/apj2018a10.
- Pichel, R., Foody, M., O'Higgins Norman, J., Feijóo, S., Varela, J. et al. (2021), «Acoso escolar, ciberacoso y su solapamiento: ¿qué tiene que ver la edad con ello?», Sustainability, vol. 13, n.º 15, https://doi.org/10.3390/su13158527.
- Pietkiewicz, M. y Treder, M. (2018), «Ciberaquizamiento en las redes sociales: la perspectiva polaca», Journal of Modern Science, vol. 38, pp. 29-40, https://doi.org/10.13166/jms/99217.
- PLAN International (2020), «State of the World's Girls 2020: ¿Libres para estar en línea? Las experiencias de las niñas y las jóvenes con el acoso en línea», Woking.
- Posetti, J., Shabbir, N., Maynard, D., Bontcheva, K. y Aboulez, N. (2021), «The Chilling: Tendencias globales en la violencia en línea contra las mujeres periodistas», UNESCO, París.
- Powell, A. y Henry, N. (2017), La violencia sexual en la era digital, Palgrave Macmillan, Londres.
- Pozza, V. D. (2024), Informe sobre la ciberviolencia contra las mujeres: panorama general de las políticas y recomendaciones, Lobby Europeo de las Mujeres, Bruselas.
- Proyecto deSHAME (Explotación digital y acoso sexual entre menores en Europa) (2017), Experiencias de los jóvenes con el acoso sexual en línea: un informe transnacional, Londres.
- Ratajczak, M. y Galzignato, E. (2019), «Niños migrantes y ciberviolencia. El problema del discurso de odio en Italia y Polonia», *Peace Human Rights Governance*, vol. 3, n.º 3, pp. 365-388.
- Ray, A. y Henry, N. (2024), «Sextorsión: una revisión exploratoria», *Trauma, Violence, & Abuse*, vol. 26, n.º 1, https://doi.org/10.1177/15248380241277271.
- Rigotti, C. y Malgieri, G. (2024), «Violencia sexual y acoso en el metaverso: una nueva manifestación de los daños de género», Alliance for Universal Digital Rights, Equality Now y Vulnera (Observatorio Internacional sobre las Personas Vulnerables en la Protección de Datos).
- Rodríguez Ramos, M. S. y Zarzalejos, J. (2024) «Revisión del acervo en materia de derechos de las víctimas», https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-revision-of-the-victims-rights-acquis.
- Rudnicki, K., Vandebosch, H., Voué, P. y Poels, K. (2023), «Revisión sistemática de los factores determinantes y las consecuencias de las intervenciones de terceros ante el odio en línea y el ciberacoso entre adultos», Behaviour & Information Technology, vol. 42, n.º 5, pp. 527-544, https://doi.org/10.1080/0144929X.2022.2027013.
- Centro para una Internet más segura de Lituania (2019), Centro para una Internet más segura de Lituania: Informe público, enero de 2019–diciembre de 2020, Agencia Nacional de Educación, Vilna, https://www.draugiskasinternetas.lt/wp-content/uploads/2021/03/English_2019-2020.pdf.
- Sala, A., Porcaro, L. y Gómez, E. (2024), «Uso de las redes sociales y salud mental y bienestar de los adolescentes: una revisión global», Computers in Human Behavior Reports, vol. 14, https://doi.org/10.1016/j.chbr.2024.100404.

- Salazar, M., Raj, A., Silverman, J. G., Rusch, M. L. A. y Reed, E. (2023), «Acoso sexual en línea entre las adolescentes: un análisis cualitativo», *Adolescents*, vol. 3, n.º 1, pp. 84-91, https://doi.org/10.3390/adolescents3010007.
- Sales, N. J. (2024), «Una niña habría sido violada en el metaverso. ¿Es este el comienzo de un nuevo y oscuro futuro?», The Guardian, 5 de enero, https://www.theguardian.com/commentisfree/2024/jan/05/ metaverse-sexual-assault-vr-game-online-safety-meta.
- Sánchez-Jiménez, V., Rodríguez-de-Arriba, M. y Muñoz-Fernández, N. (2022), «¿Es agresiva esta conversación de WhatsApp? La percepción de los adolescentes sobre la agresión en las citas online», Journal of Interpersonal Violence, vol. 37, n.º 19-20, pp. NP17369-NP17393, https://doi.org/10.1177/08862605211028011.
- Schittenhelm, C., Kops, M., Moosburner, M., Fischer, M. S. y Wachs, S. (2024), «La victimización por ciberacoso sexual entre los jóvenes: una revisión sistemática de las tasas de prevalencia, los factores de riesgo y los resultados», Adolescent Research Review, vol. 10, pp. 169–200, https://doi.org/10.1007/s40894-024-00248-w.
- Sciacca, B., Mazzone, A., Loftsson, M., O'Higgins Norman, J. y Foody, M. (2023), «Difusión no consentida de imágenes sexuales entre adolescentes: asociaciones con la depresión y la autoestima», Journal of Interpersonal Violence, vol. 38, núm. 15-16, pp. 9438-9464, https://doi.org/10.1177/08862605231165777.
- Scott, A., Semmens, L. y Willoughby, L. (2001), «Las mujeres e Internet: la historia natural de un proyecto de investigación», en: Adam, A. y Green, E. (eds.), Virtual Gender: Technology, consumption and identity matters, Routledge, Abingdon.
- Secretaría del Comité de Lanzarote (2018), Directrices para la implementación de la participación infantil, https://rm.coe.int/guidelines-for-implementation-of-child-participation/1680790571.
- Singh, P., Smith, M. V., Raba, C. M. y Keller, J. (2016), «Violencia de pareja en el ámbito digital y consecuencias para la salud mental en una muestra de alumnas de secundaria», MedCrave Online Journal of Public Health, vol. 4, n.º 3, pp. 67-70, https://doi.org/10.15406/mojph.2016.04.00078.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E. et al. (2020), «EU Kids Online 2020: Resultados de la encuesta realizada en 19 países», EU Kids Online, https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf.
- Smith, A. (2024), «La violación en la realidad virtual: cómo vigilar el metaverso», página web de Context, 24 de enero, https://www.context.news/digital-rights/las-denuncias-de-agresiones-sexuales-y-la-delincuencia-aumentan-el-temor-a-un-nuevo-«oeste-salvaje-virtual».
- Smith, D. (2023), «Cómo influye el engaño en las citas online y las aplicaciones de citas», Canadian Journal of Family and Youth, vol. 15, n.º 2, pp. 23-32, https://doi.org/10.29173/cjfy29869.
- Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T. et al. (2010) «Factores de riesgo psicosociales asociados al ciberacoso entre adolescentes: un estudio poblacional», Archives of General Psychiatry, vol. 67, n.º 7, pp. 720-728, https://doi.org/10.1001/archgenpsychiatry.2010.79.
- Steinvik, H. R., Duffy, A. L. y Zimmer-Gembeck, M. J. (2023), «Respuestas de los testigos ante el ciberacoso: el papel de la angustia empática, la ira empática y la compasión», International Journal of Bullying Prevention, vol. 6, pp. 399–410, https://doi.org/10.1007/s42380-023-00164-y.
- Šulc, A., Vehovar, V., Brečko, B., Rucman, A. B. y Krainer, A. (2024), «Diferencias en la victimización y la perpetración del ciberacoso según la edad y la localidad en Eslovenia», Revija za kriminalistiko in kriminologijo, vol. 72, n.º 4, pp. 337-349, http://www.dlib.si/?URN=URN:NBN:SI:doc-F7LDTW5D.
- Sutton, S. y Finkelhor, D. (2023), «La identidad de los autores de delitos en línea contra menores: un metaanálisis», *Trauma, Violence, & Abuse*, vol. 25, n.º 3, pp. 1756-1768, https://doi.org/10.1177/15248380231194072.

- Torek, B. (2025), «Las nuevas políticas de Meta: cómo ponen en peligro a las comunidades LGBTQ+ y nuestros consejos para mantenerse a salvo en Internet», sitio web de Human Rights Campaign, 15 de enero, https://www.hrc.org/news/metas-new-policies-how-they-endanger-lgbtq-communities-and-our-tips-for-staying-safe-online.
- ONU Mujeres (Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres) (2021), Guía para mujeres y niñas sobre cómo prevenir y responder a la ciberviolencia.
- ONU Mujeres (2022), «Acelerar los esfuerzos para combatir la violencia contra las mujeres y las niñas (VAWG) facilitada por Internet y la tecnología», documento de políticas de ONU Mujeres.
- ONU Mujeres y OMS (Organización Mundial de la Salud) (2023), «Violencia contra las mujeres facilitada por la tecnología: balance de las pruebas y recopilación de datos», https://www.unwomen.org/en/digital-library/publications/2023/04technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection.
- ONU Mujeres (2024a), «Violencia de género facilitada por la tecnología: desarrollo de una agenda de investigación compartida», https://www.unwomen.org/en/digital-library/publications/2024/09/violencia-de-género-facilitada-por-la-tecnología-elaboración-de-una-agenda-de-investigación-compartida.
- ONU Mujeres (2024b), Guía para jóvenes para acabar con la violencia de género en línea, versión 3.
- UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura) (2023), «Tu opinión no importa, de todos modos»: Denuncia de la violencia de género facilitada por la tecnología en la era de la IA generativa, París.
- Naciones Unidas (2018), A/HRC/38/47: Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, relativo a la violencia en línea contra las mujeres y las niñas desde una perspectiva de derechos humanos, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Ginebra, 18 de junio, https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and.
- Naciones Unidas (2024), «Ciberviolencia contra las mujeres y las niñas: la creciente amenaza de la era digital», sitio web del Centro Regional de Información de las Naciones Unidas para Europa Occidental, 5 de diciembre, https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/.
- USAID (Agencia de los Estados Unidos para el Desarrollo Internacional) (2023), «DRG Learning Digest – Lucha contra la violencia de género facilitada por la tecnología en la política», marzo, https://content.govdelivery.com/accounts/USAIDHQ/bulletins/34c7e57.
- Vallance, C. (2024), «La policía investiga una agresión sexual virtual contra el avatar de una niña», sitio web de BBC News, 2 de enero, https://www.bbc.com/news/technology-67865327.
- Van Ouytsel, J., Ponnet, K. y Walrave, M. (2020), «Abuso en las citas online: investigación de los comportamientos de vigilancia digital entre adolescentes desde una perspectiva de aprendizaje social», Journal of Interpersonal Violence, vol. 35, n.º 23-24, pp. 5157-5178, https://doi.org/10.1177/0886260517719538.
- Vogels, E. A. (2022), «Los adolescentes y el ciberacoso en 2022», Pew Research Center, 15 de diciembre, https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.
- Vogler, S., Kappel, R. y Mumford, E. (2023), «Experiencias de abuso facilitado por la tecnología entre las minorías sexuales y de género», Journal of Interpersonal Violence, vol. 38, n.º 19-20, 11290-11313, https://doi.org/10.1177/08862605231179724.
- Waasdorp, T. E. y Bradshaw, C. P. (2014), «El solapamiento entre el ciberacoso y el acoso tradicional», Journal of Adolescent Health, vol. 56, n.º 5, pp. 483–488, https://doi.org/10.1016/j.jadohealth.2014.12.00.
- Wajcman, J. (2004), TechnoFeminism, Polity Press, Cambridge.
- Wajcman, J. (2010), «Teorías feministas de la tecnología», Cambridge Journal of Economics, vol. 34, n.º 1, pp. 143–152, https://doi.org/10.1093/cje/ben057.

- Wajcman, J. (2015), «Pressed for Time: The acceleration of life in digital capitalism», University of Chicago Press, Chicago.
- Wallace, A., Langevin, R. y Hébert, M. (2023), «Análisis de los factores de riesgo y de protección asociados a la victimización por violencia en las relaciones sentimentales en línea entre las adolescentes: una perspectiva ecológica», Journal of Child & Adolescent Trauma, vol. 16, n.º 4, pp. 1017-1029, https://doi.org/10.1007/s40653-023-00558-6.
- WeProtect Global Alliance (2016), «Prevención y lucha contra la explotación y el abuso sexuales infantiles: un modelo de respuesta nacional», Londres.
- WeProtect Global Alliance (2021), Material sexual «autogenerado» por menores en Internet: perspectivas de los niños y jóvenes, Londres.
- WWWF (World Wide Web Foundation) (2024), «Autores de violencia de género en línea: hoja de ruta para las investigaciones», Washington, D. C.
- WWWF y Asociación Mundial de Guías y Scouts (2020), Encuesta: la experiencia de los jóvenes con el acoso en línea, Washington D. C., https://ureport.in/opinion/3983/.
- Wright, M. F. (2017), «Percepciones de los adolescentes sobre los comportamientos, las características y las relaciones motivadas por la popularidad en el ciberespacio y la ciberagresión: el papel del género», Cyberpsychology, Behavior and Social Networking, vol. 20, n.º 6, pp. 355-361, https://doi.org/10.1089/cyber.2016.0693.
- Wright, M. F. (2020), «El papel de las tecnologías, los comportamientos, el género y los rasgos de estereotipos de género en la ciberagresión de los adolescentes», Journal of Interpersonal Violence, vol. 35, n.º 7-8, pp. 1719-1738, https://doi.org/10.1177/0886260517696858.
- Wright, M. F. y Wachs, S. (2020), «La cibervictimización de los adolescentes: la influencia de las tecnologías, el género y los rasgos de estereotipos de género», International Journal of Environmental Research and Public Health, vol. 17, n.º 4, 1293, https://doi.org/10.3390/ijerph17041293.
- Xu, Y. y Trzaskawka, P. (2021), «Hacia una descripción adecuada del ciberacoso: estudios interdisciplinares sobre las características, los casos y las cuestiones legislativas del ciberacoso», International Journal for the Semiotics of Law, vol. 34, n.º 4, pp. 929-943, https://doi.org/10.1007/s11196-021-09856-4.
- Yoon, J. (2022), «¿Podemos hacer algo contra los delitos sexuales en el metaverso?», sitio web de Inside Compliance, 6 de octubre, https://blogs.luc.edu/compliance/?p=4849.
- Zamfir, I. y Murphy, C. (2024), «Ciberviolencia contra las mujeres en la UE», Informe del Servicio de Investigación del Parlamento Europeo, PE 7677.146, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI%282024%29767146_EN.pdf.
- Zweig, J. M., Lachman, P., Yahner, J. y Dank, M. (2014), «Correlatos del abuso en las relaciones sentimentales por Internet entre adolescentes», Journal of Youth and Adolescence, vol. 43, n.º 8, pp. 1306-1321, https://doi.org/10.1007/ s10964-013-0047-x.

Anexo

Recuadros

Recuadro 8: Detalles del enfoque metodológico utilizado para el estudio

Investigación documental y revisión bibliográfica

La primera fase del estudio consistió en una investigación documental sistemática y una revisión bibliográfica, que proporcionaron la base conceptual y empírica del estudio. Se identificaron estudios clave y documentos de política mediante bases de datos como Google Scholar y Semantic Scholar. Mientras que Google Scholar se utilizó para una selección inicial amplia, Semantic Scholar permitió una búsqueda más específica gracias a sus recomendaciones basadas en inteligencia artificial y al análisis de citas. La fecha de publicación (dando prioridad al periodo 2019-2024) y la relevancia para los objetivos del estudio fueron los criterios clave de inclusión. Se incluyeron trabajos anteriores cuando fue necesario para seguir la evolución de los debates o para aportar una perspectiva histórica.

La revisión abarcó una amplia gama de fuentes: artículos revisados por pares, libros académicos, informes elaborados por instituciones internacionales y europeas (por ejemplo, el EIGE, la ONU o el Banco Mundial), estudios de ONG y organizaciones de defensa de los derechos de las mujeres a escala de la UE (por ejemplo, el Lobby Europeo de las Mujeres o WAVE), así como informes, documentos y otros resultados de investigaciones financiadas por la UE. También se incorporó la literatura gris, incluidos documentos de asociaciones, revistas especializadas y artículos de prensa, para captar los debates en curso y las preocupaciones emergentes. Se utilizó el software Zotero para gestionar las referencias y clasificar la bibliografía según palabras clave y temas. Las etiquetas nos permitieron agrupar los estudios por preguntas de investigación específicas o enfoques metodológicos, lo que garantizó una base empírica bien estructurada y fácilmente consultable.

Mapeo de medidas políticas y disposiciones legales

Partiendo de la revisión bibliográfica, el estudio llevó a cabo un mapeo sistemático de los marcos políticos y las disposiciones legales pertinentes a nivel internacional, europeo y nacional. Este mapeo tenía por objeto identificar la arquitectura normativa que aborda la ciberviolencia y poner de relieve las convergencias y divergencias entre los Estados miembros. El proceso se basó en una amplia gama de fuentes oficiales, entre ellas la base de datos del Tribunal Europeo de Derechos Humanos (HUDOC), GREVIO

, la biblioteca en línea del Consejo de Europa, el repositorio de definiciones jurídicas del EIGE y el Foro Europeo de Boletines Oficiales.

Las técnicas de «bola de nieve» garantizaron además que, además de la muestra inicial de documentos, se incluyeran las leyes nacionales y las nuevas medidas políticas. Este enfoque proporcionó una visión global del panorama normativo y jurídico de la UE, poniendo de relieve tanto las tendencias comunes como los enfoques nacionales específicos.

Análisis de datos estadísticos

El análisis cuantitativo ayudó a contextualizar la investigación mediante el examen de la prevalencia y la dinámica de la ciberviolencia en los distintos Estados miembros. A nivel de la UE, el análisis se basó en estadísticas de la Encuesta de la UE sobre la violencia de género, la Encuesta de la FRA y el EIGE sobre la violencia de género en la UE y la Encuesta HBSC.

También se examinaron encuestas nacionales y datos recopilados por ONG y organizaciones coordinadoras. Las encuestas comparativas internacionales (por ejemplo, de Plan International y del Pew Research Center) aportaron perspectivas adicionales, mientras que proyectos financiados por la UE, como «EU Kids Online», proporcionaron información detallada sobre los comportamientos en línea de los niños y adolescentes. La triangulación de estas fuentes permitió al estudio cuantificar las tendencias y situar sus hallazgos cualitativos dentro de una dinámica estructural más amplia.

Grupos focales y diseño cualitativo

El segundo pilar de la metodología fue el trabajo de campo cualitativo, diseñado para captar las experiencias vividas por los adolescentes en sus propias palabras. Se llevaron a cabo un total de 37 grupos focales en 10 Estados miembros (Bélgica, Alemania, Estonia, Irlanda, España, Italia, Chipre, Polonia, Rumanía y Suecia), en los que participaron 133 chicas de entre 13 y 18 años y 38 chicos de entre 15 y 18 años. La decisión de utilizar grupos focales se basó en principios feministas y participativos: no se trató a los participantes meramente como informantes, sino como portadores de conocimiento capaces de articular las formas en que las relaciones de poder de género y las normas sociales configuran sus experiencias de daños en línea.

Los debates en grupo se estructuraron en torno a guías de debate específicas adaptadas a los distintos grupos de edad. Para las participantes más jóvenes (de 13 a 15 años), las guías de debate incluían actividades interactivas (por ejemplo, nubes de palabras o juegos como Kahoot) y una viñeta sobre un personaje ficticio que sufría ciberacoso, con el fin de fomentar la reflexión sin exigir la revelación de datos personales. Para los adolescentes de más edad (de 16 a 18 años), las guías de debate incluían escenarios más complejos, como la presión para compartir imágenes íntimas y el consiguiente acoso en línea, lo que permitía un análisis más profundo de los temas del consentimiento digital y el daño a la reputación. Los grupos focales con chicos se centraron en las normas sociales, la masculinidad, el comportamiento de los espectadores y la empatía. En consonancia con la política de ética y protección del proyecto, los debates con chicas y chicos también abordaron los posibles mecanismos de apoyo disponibles tras sufrir experiencias de ciberviolencia. Las estrategias de selección de participantes garantizaron la diversidad en cuanto a origen socioeconómico, origen étnico y entornos educativos, al tiempo que se priorizó la seguridad psicológica. Los grupos focales se celebraron en lugares accesibles y adaptados a los jóvenes, como colegios, centros comunitarios y bibliotecas. En todos los casos se obtuvo el consentimiento informado de los padres y el asentimiento de los participantes.

Análisis de datos y medidas de protección

El análisis de los datos se llevó a cabo mediante un enfoque combinado temático y de síntesis. Las discusiones de los grupos focales se transcribieron, codificaron y analizaron utilizando el software NVivo. Las categorías de codificación incluyeron formas de ciberviolencia, causas percibidas, repercusiones, estrategias de afrontamiento, barreras para la denuncia y respuestas institucionales. La codificación fue inductiva, lo que permitió que surgieran nuevos temas

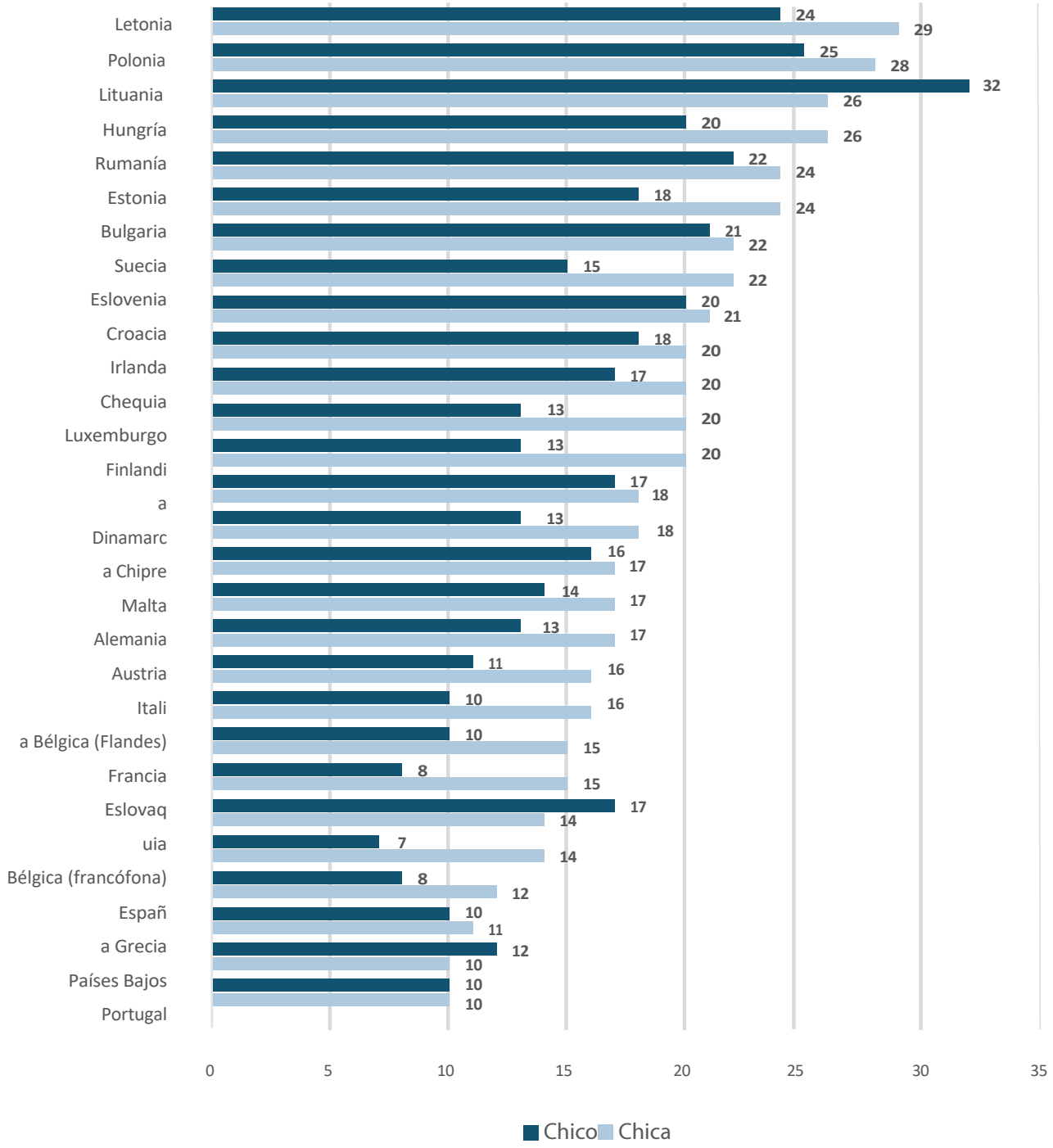
directamente a partir de los datos, y deductivo, guiado por preguntas de investigación predefinidas y el marco teórico del estudio.

El análisis temático se complementó con un análisis de síntesis para comparar los resultados entre los distintos grupos de edad y Estados miembros, lo que permitió identificar patrones comunes y variaciones contextuales. La triangulación con datos cuantitativos y conclusiones sobre políticas reforzó aún más la solidez del análisis. Este marco multifacético garantizó que los relatos subjetivos de los adolescentes se interpretaran en el contexto de la evidencia estructural.

Dada la naturaleza sensible de la investigación y la participación de menores, se aplicaron estrictas garantías éticas. El estudio se llevó a cabo de conformidad con las directrices de la OMS y los marcos institucionales de protección de la infancia. Los procedimientos de consentimiento informado y de asentimiento fueron fundamentales para el diseño: los tutores recibieron información detallada sobre los objetivos y procedimientos del estudio, mientras que a los adolescentes se les concedió la autonomía para dar su asentimiento o retirarse en cualquier momento. Las medidas de protección incluyeron facilitadores cualificados, garantías de confidencialidad y el seguimiento continuo del bienestar de los participantes antes, durante y después de las sesiones.

Figuras

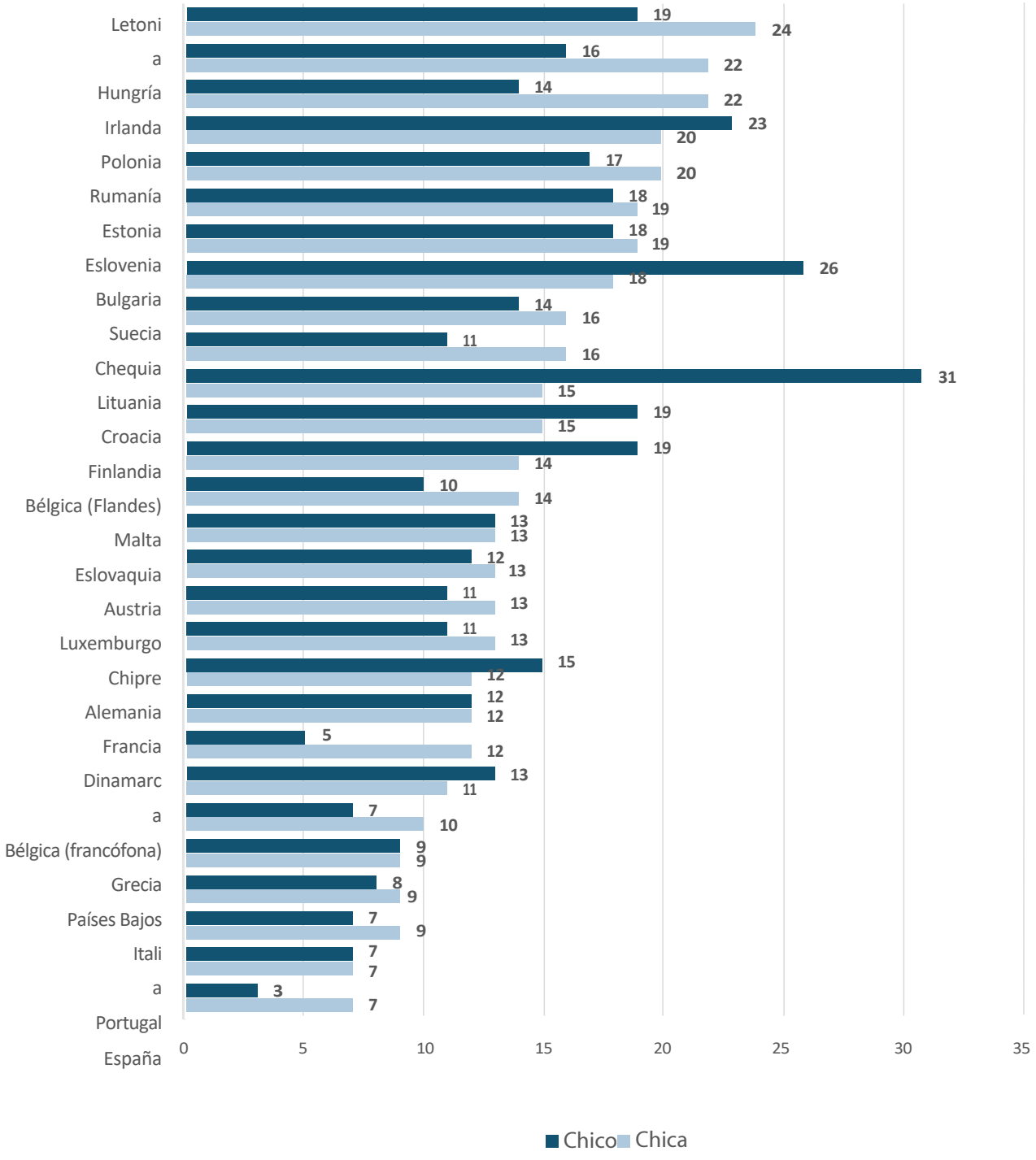
FIGURA A1 | Menores de 13 años que han sufrido ciberacoso al menos una vez en los últimos dos meses, por sexo y Estado miembro (%, 2021-2022)



Nota: Se preguntó a los jóvenes con qué frecuencia habían sufrido ciberacoso (por ejemplo, que alguien les enviara mensajes instantáneos, publicaciones en el muro o correos electrónicos ofensivos, o que alguien publicara o compartiera fotos o vídeos en Internet sin su permiso). Las opciones de respuesta iban desde «No he sufrido ciberacoso en los últimos dos meses» hasta «Varias veces a la semana». Los resultados que aquí se presentan muestran el porcentaje de jóvenes que habían sufrido ciberacoso al menos una vez en los últimos dos meses.

Fuente: Explorador de datos del estudio HBSC (resultados de la encuesta HBSC 2021-2022) – https://data-browser.hbsc.org.

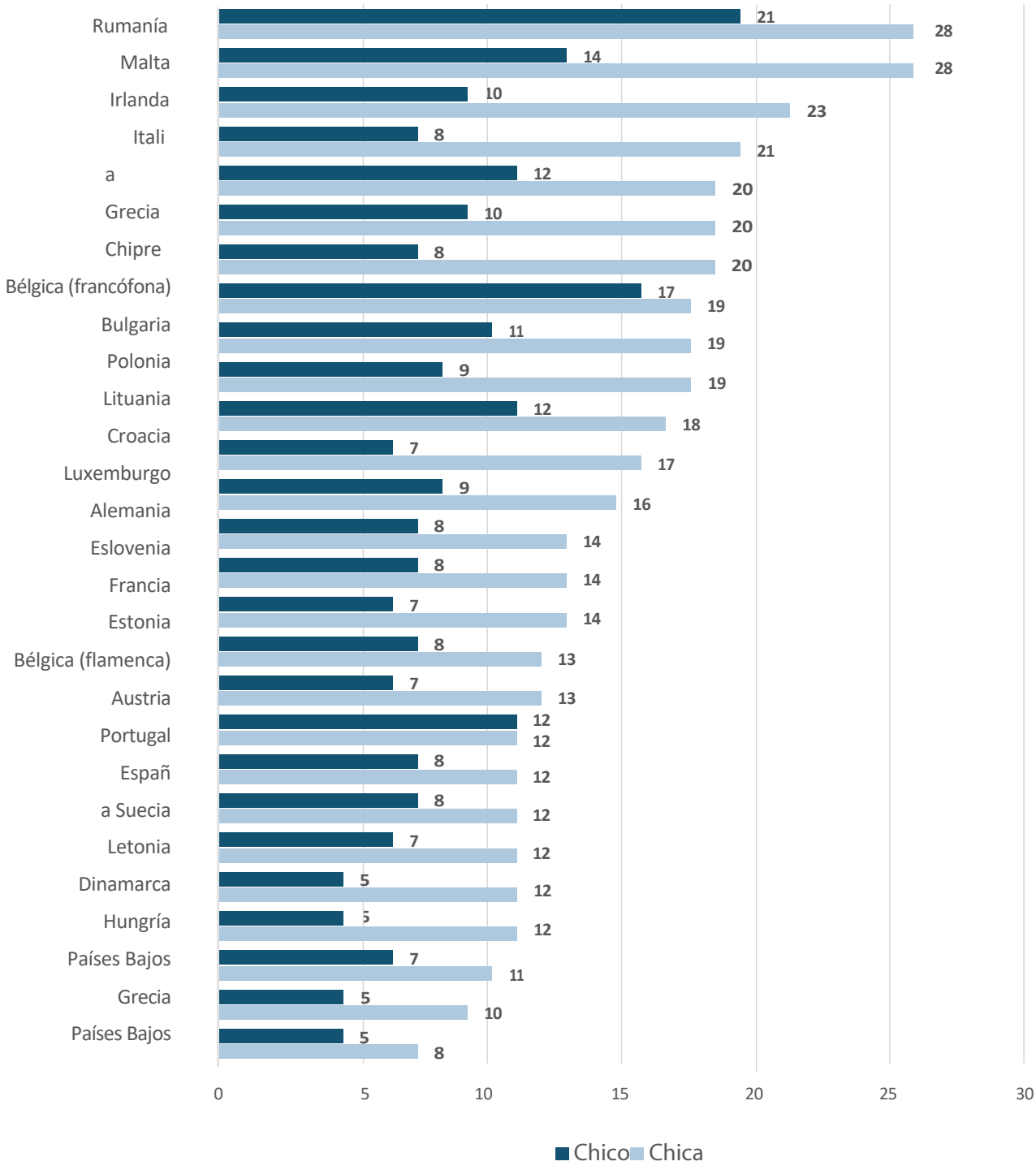
FIGURA A2 | Jóvenes de quince años que han sufrido ciberacoso al menos una vez en los últimos dos meses, por sexo y Estado miembro (%, 2021-2022)



Nota: Se preguntó a los jóvenes con qué frecuencia habían sufrido ciberacoso (por ejemplo, que alguien les enviara mensajes instantáneos, publicaciones en el muro o correos electrónicos ofensivos, o que alguien publicara o compartiera fotos o vídeos en línea sin su permiso). Las opciones de respuesta iban desde «No he sufrido ciberacoso en los últimos dos meses» hasta «Varias veces a la semana». Los resultados que aquí se presentan muestran el porcentaje de jóvenes que habían sufrido ciberacoso al menos una vez en los últimos dos meses.

Fuente: Explorador de datos del estudio HBSC (resultados de la encuesta HBSC 2021-2022) – https://data-browser.hbsc.org.

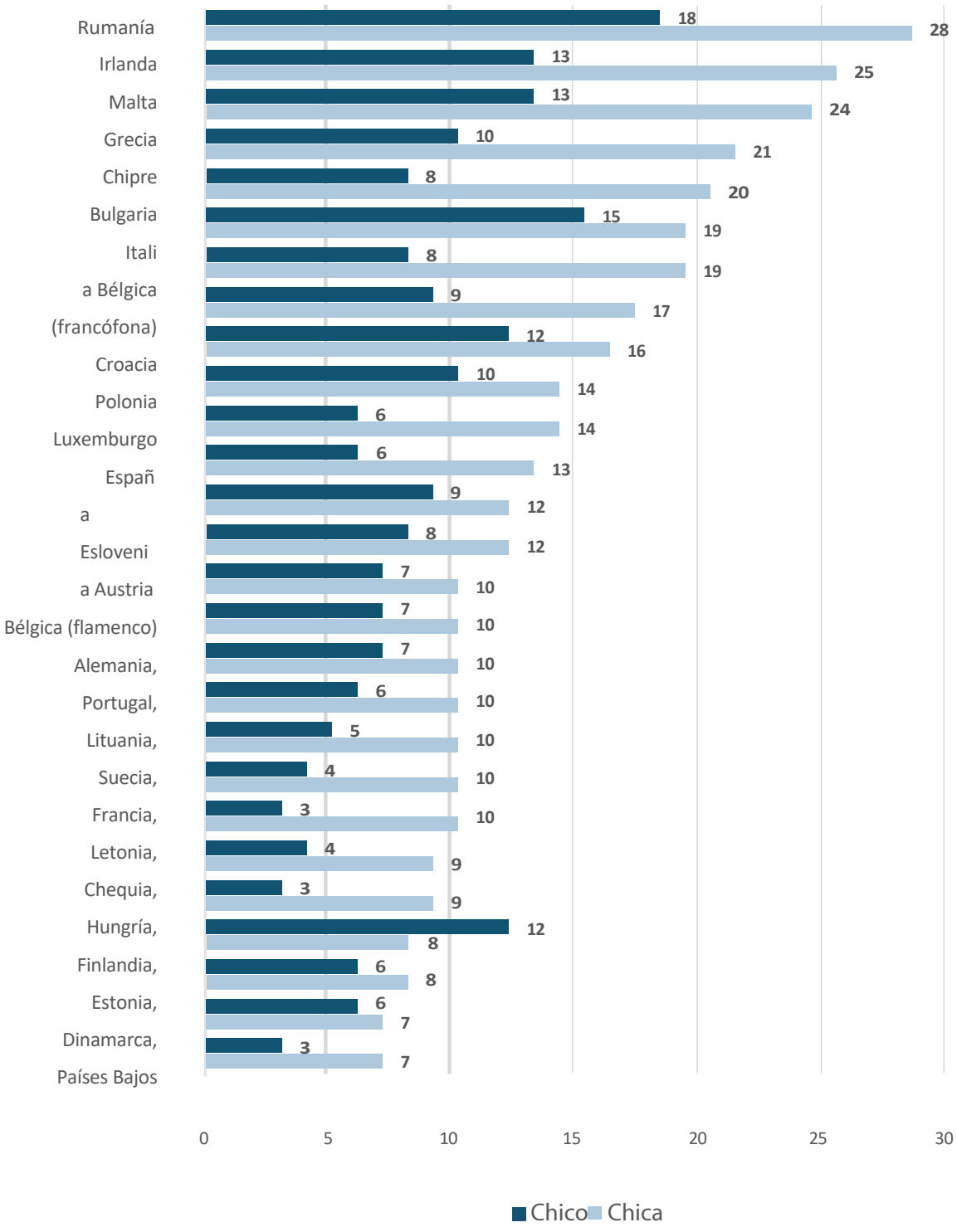
FIGURA A3 | Jóvenes de trece años que declaran un uso problemático de las redes sociales, por sexo y Estado miembro (% 2021-2022)



Nota: Se pidió a los jóvenes que informaran de los síntomas de un uso problemático (similar a una adicción) de las redes sociales mediante la Escala de Trastorno de las Redes Sociales, una escala de nueve ítems en la que los encuestados respondían a cada pregunta con un «sí» o un «no». Los resultados que aquí se presentan muestran el porcentaje de jóvenes que respondieron «sí» a seis o más preguntas y que, por lo tanto, fueron clasificados como usuarios problemáticos de las redes sociales.

Fuente: Explorador de datos del estudio HBSC (resultados de la encuesta HBSC 2021-2022) – https://data-browser.hbsc.org.

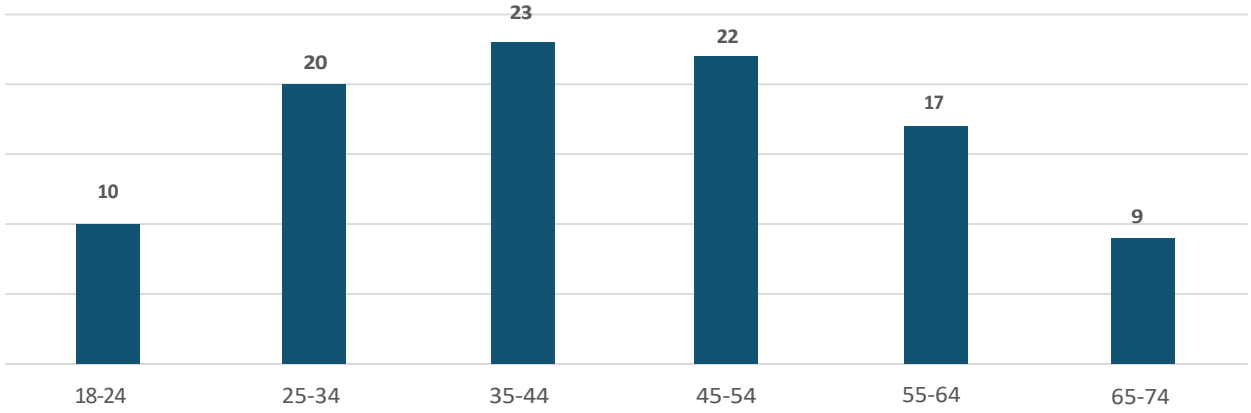
FIGURA A4 | Jóvenes de quince años que declaran un uso problemático de las redes sociales, por sexo y Estado miembro (% 2021-2022)



Nota: Se pidió a los jóvenes que informaran sobre los síntomas de un uso problemático (similar a una adicción) de las redes sociales mediante la Escala de Trastorno de las Redes Sociales, una escala de nueve ítems en la que los encuestados respondían a cada pregunta con un «sí» o un «no». Los resultados que aquí se presentan muestran el porcentaje de jóvenes que respondieron «sí» a seis o más preguntas y que, por lo tanto, fueron clasificados como usuarios problemáticos de las redes sociales.

Fuente: Explorador de datos del estudio HBSC (resultados de la encuesta HBSC 2021-2022) – https://data-browser.hbsc.org.

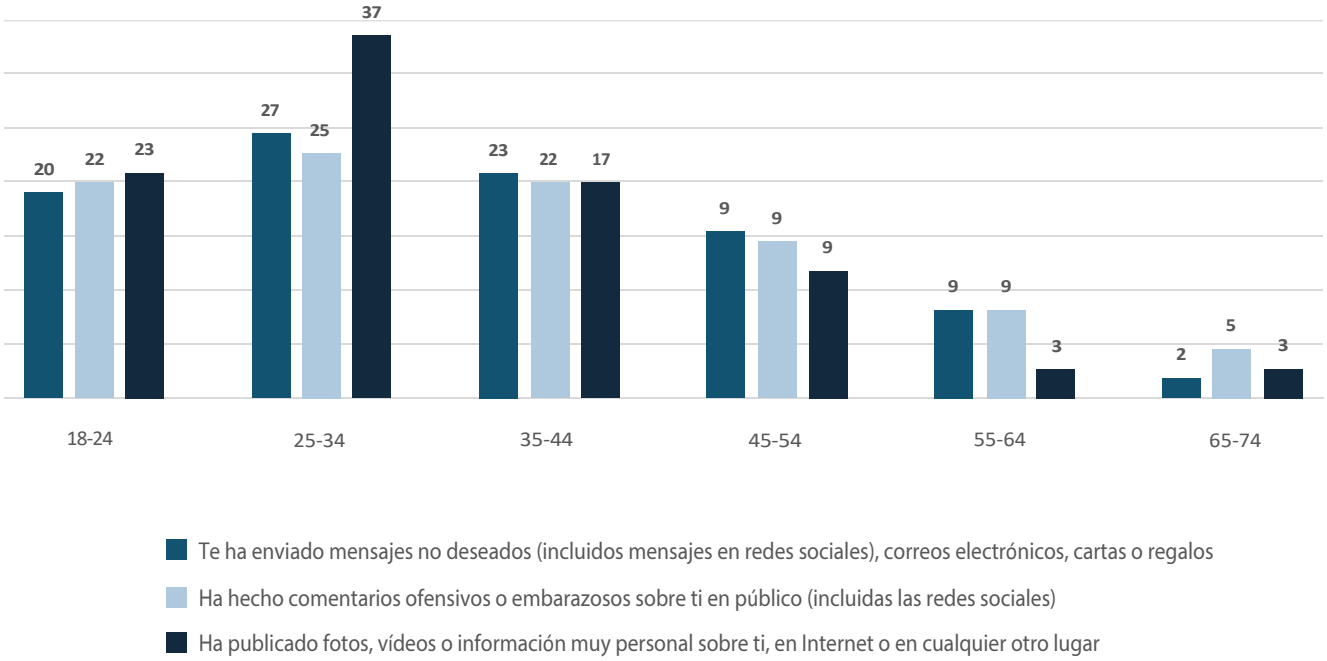
FIGURA A5 | Mujeres que han sufrido comportamientos controladores por parte de sus parejas, que insisten en saber su paradero, por grupo de edad (%, de 18 a 74 años, UE, 2021)



Nota: Se preguntó a los encuestados si alguna de sus parejas actuales o anteriores había insistido alguna vez en saber dónde se encontraban de forma controladora o en rastrearlos mediante GPS, teléfono, redes sociales, etc. (Pregunta F1 de la Encuesta de la UE sobre la violencia de género). Los resultados que aquí se presentan muestran la proporción de encuestados que declararon haber vivido este tipo de experiencias, desglosada por edades. Estos datos se basan en la estimación de la población derivada de la muestra y han sido debidamente ponderados. La población objetivo de la Encuesta de la UE sobre la Violencia de Género se define como las personas de entre 18 y 74 años que viven en hogares privados, con especial atención a las mujeres.

Fuente: Autores, a partir de datos de la Encuesta de la UE sobre la violencia de género (ola de 2021).

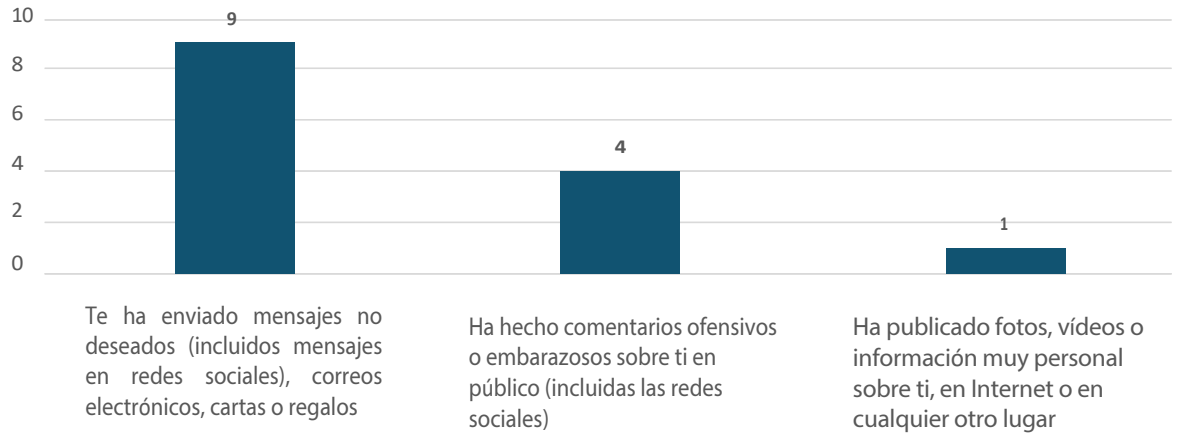
FIGURA A6 | Mujeres que han sufrido ciberviolencia, por tipo de violencia y grupo de edad (%, personas de entre 18 y 74 años, UE, 2021)



Nota: Se preguntó a los encuestados si, a lo largo de su vida, la misma persona había llevado a cabo repetidamente (más de una vez) una o varias de las siguientes acciones de tal forma que les causara miedo, alarma o angustia. Los elementos considerados están relacionados con cuestiones vinculadas (aunque no limitadas a) a diferentes tipos de ciberviolencia, concretamente: «Te ha enviado mensajes no deseados (incluidos mensajes en redes sociales), correos electrónicos, cartas o regalos»; «Ha hecho comentarios ofensivos o embarazosos sobre ti en público (incluidas las redes sociales)»; y «Ha publicado fotos, vídeos o información muy personal sobre ti, en Internet o en cualquier otro lugar». (Pregunta n.º 1 de la Encuesta de la UE sobre la violencia de género. Variables de la encuesta: ST_GIFTS, ST_COMMENT, ST_PUBLISH.) Los resultados que aquí se presentan muestran la proporción de encuestados que declararon haber sufrido este tipo de experiencias, desglosada por edades. Estos datos se basan en la estimación de la población derivada de la muestra y han sido debidamente ponderados. La población objetivo de la Encuesta de la UE sobre la violencia de género se define como las personas de entre 18 y 74 años que viven en hogares privados, con especial atención a las mujeres.

Fuente: Autores, a partir de datos de la Encuesta de la UE sobre la violencia de género (ola de 2021).

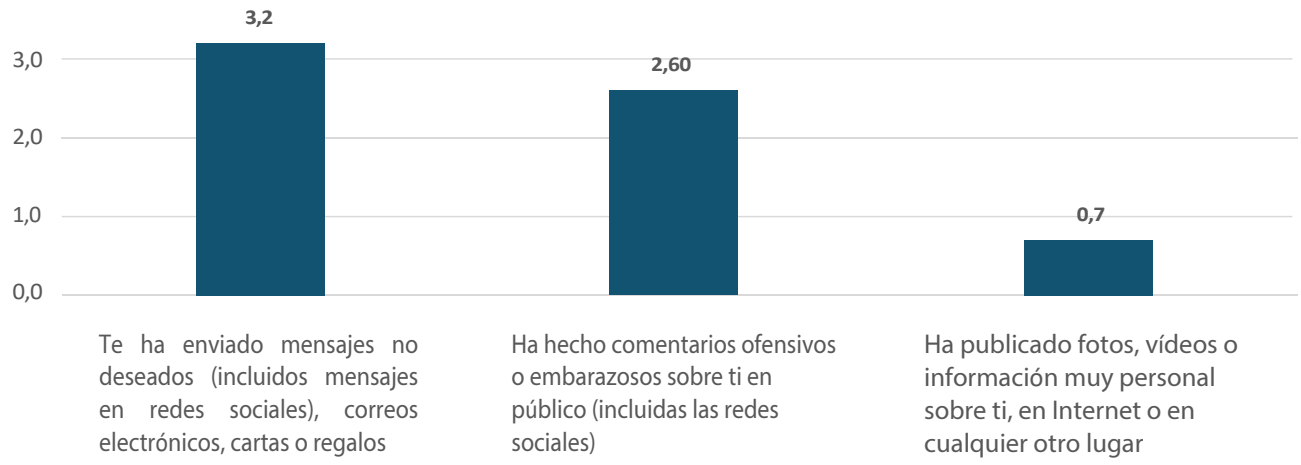
FIGURA A7 | Mujeres que han sufrido ciberviolencia, por tipo de violencia (%, UE, personas de entre 18 y 74 años, 2021)



Nota: Se preguntó a los encuestados si, a lo largo de su vida, la misma persona había llevado a cabo repetidamente (más de una vez) una o varias de las siguientes acciones de tal forma que les causara miedo, alarma o angustia. Los elementos considerados están relacionados con cuestiones vinculadas (aunque no limitadas a) a diferentes tipos de ciberviolencia, concretamente: «Te ha enviado mensajes no deseados (incluidos mensajes en redes sociales), correos electrónicos, cartas o regalos»; «Ha hecho comentarios ofensivos o embarazosos sobre ti en público (incluidas las redes sociales)»; y «Ha publicado fotos, vídeos o información muy personal sobre ti, en Internet o en cualquier otro lugar». (Pregunta n.º 1 de la Encuesta de la UE sobre la violencia de género. Variables de la encuesta: ST_GIFTS, ST_COMMENT, ST_PUBLISH.) Los resultados que aquí se presentan muestran la proporción de encuestados que declararon haber sufrido este tipo de experiencias. Estos datos se basan en la estimación de la población derivada de la muestra y han sido debidamente ponderados. La población objetivo de la Encuesta de la UE sobre la violencia de género se define como las personas de entre 18 y 74 años que viven en hogares privados, con especial atención a las mujeres

Fuente: Autores, a partir de datos de la Encuesta de la UE sobre la violencia de género (ola de 2021).

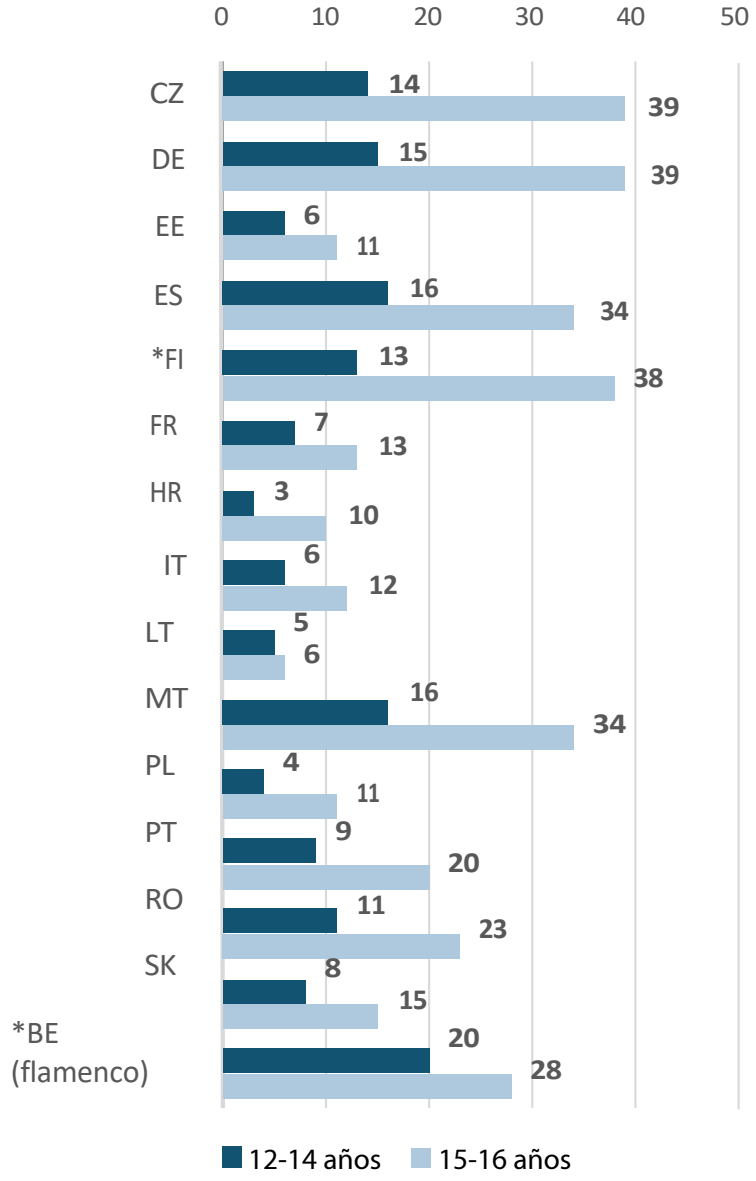
FIGURA A8 | Mujeres cuyas experiencias de ciberviolencia tuvieron lugar antes de los 15 años (%, UE, personas de entre 18 y 74 años, 2021)



Nota: Se preguntó a las personas encuestadas si el episodio de violencia que habían sufrido había tenido lugar antes de los 15 años. Los resultados que aquí se presentan corresponden a aquellas personas encuestadas que —de entre las que afirmaron haber sufrido ciberviolencia en respuesta a la pregunta N1— respondieron que, de las situaciones que habían indicado haber sufrido en la pregunta N1, «todas ellas» ocurrieron antes de los 15 años (pregunta N6 de la Encuesta de la UE sobre la violencia de género). Los resultados presentados se basan en la estimación de la población derivada de la muestra y se han ponderado adecuadamente. La población objetivo de la Encuesta de la UE sobre la violencia de género se define como las personas de entre 18 y 74 años que viven en hogares privados, con especial atención a las mujeres.

Fuente: Autores, a partir de datos de la encuesta de la UE sobre la violencia de género (ola de 2021).

FIGURA A9 | Adolescentes que han recibido propuestas sexuales no deseadas, por grupo de edad y Estado miembro (%, jóvenes de 12 a 16 años, 2020)

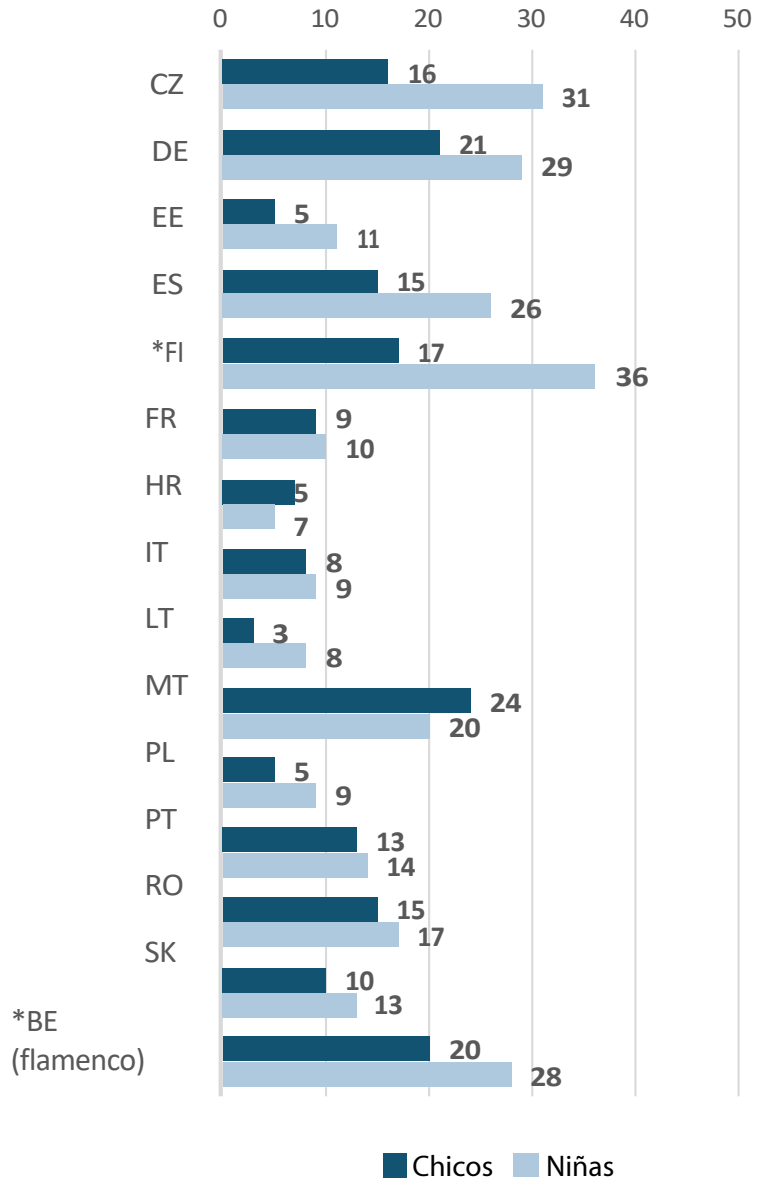


(*) datos no ponderados

Nota: Basado en la siguiente pregunta de una encuesta realizada en el marco del proyecto «EU Kids Online» (QF47). «En el ÚLTIMO AÑO, ¿con qué frecuencia, si es que alguna vez, te ha pedido alguien por Internet información de carácter sexual (palabras, imágenes o vídeos) sobre ti cuando no querías responder a esas preguntas?». Porcentaje de niños que respondieron «unas cuantas veces», «al menos una vez al mes» o «a diario o casi a diario».

Fuente: Smahel et al., 2020.

FIGURA A10 | Adolescentes que han recibido solicitudes sexuales no deseadas, por sexo y Estado miembro (%, de 12 a 16 años, 2020)

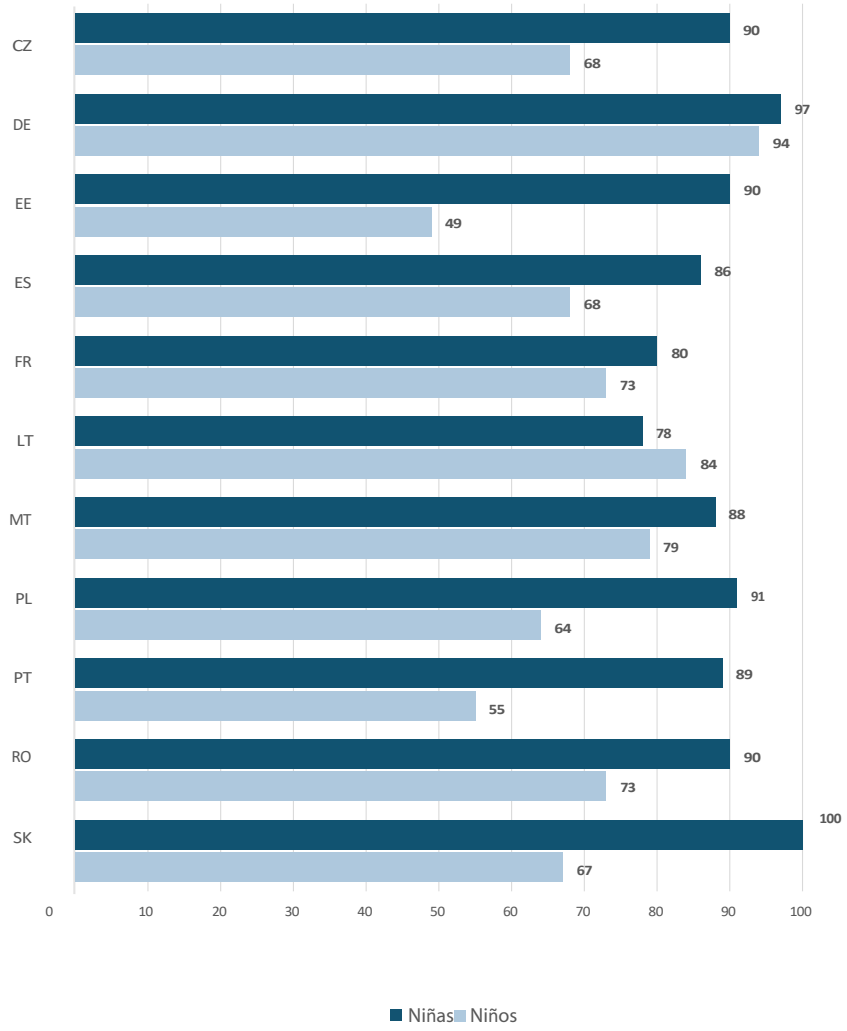


(*) datos no ponderados

Nota: Basado en la siguiente pregunta de la encuesta del proyecto «EU Kids Online» (QF47). «En el ÚLTIMO AÑO, ¿con qué frecuencia, si es que alguna vez, te ha pedido alguien por Internet información de carácter sexual (palabras, imágenes o vídeos) sobre ti cuando no querías responder a esas preguntas?». Porcentaje de niños que respondieron «unas cuantas veces», «al menos una vez al mes» o «a diario o casi a diario» del total de niños de entre 9 y 16 años que utilizan Internet.

Fuente: Smahel et al., 2020.

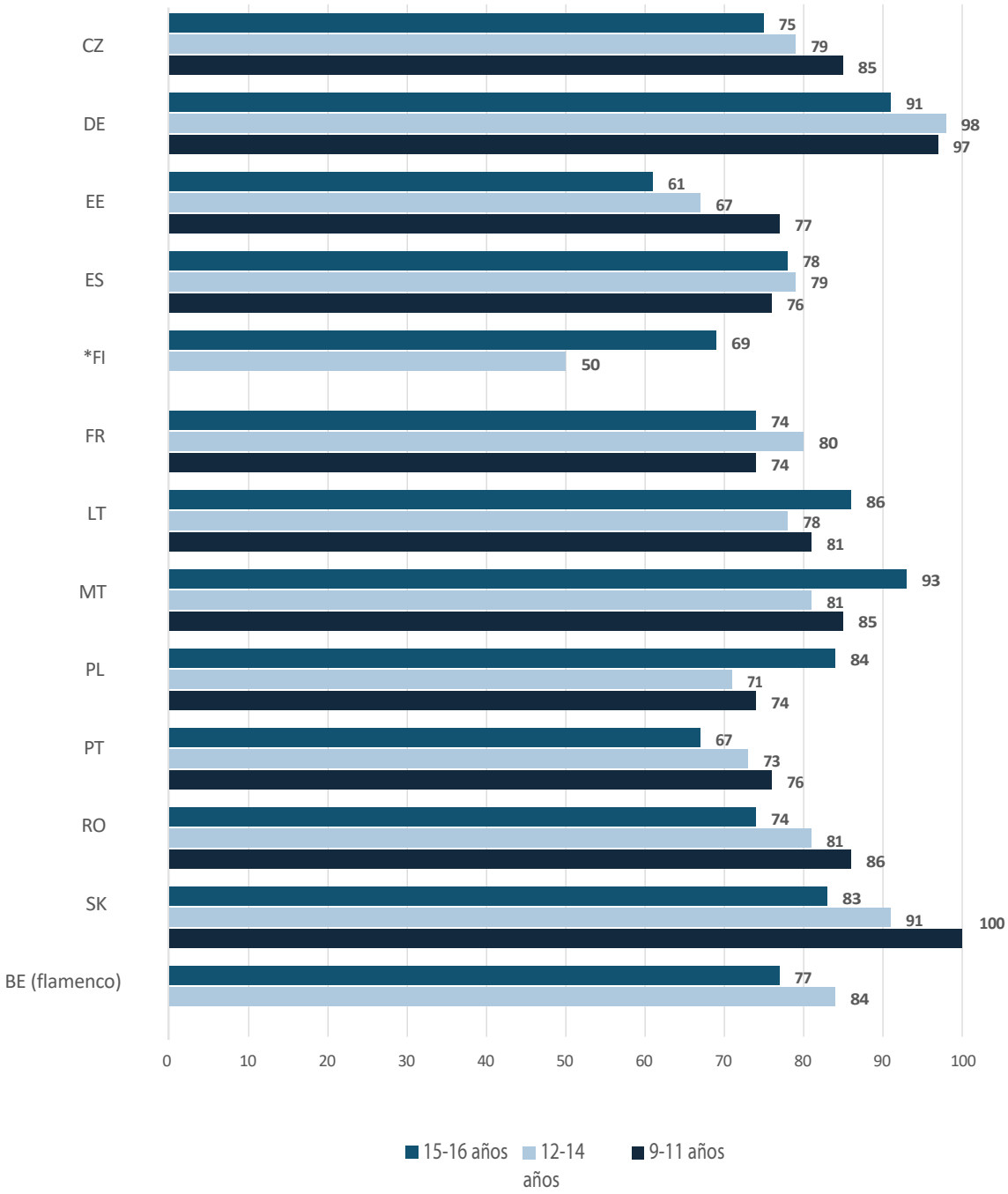
FIGURA A11 | Niños que han sufrido daños como consecuencia de la victimización en línea (hasta el punto de sentirse al menos un poco molestos), por sexo y Estado miembro (%, niños de 9 a 16 años, 2020)



Nota: En la Región Flamenca de Bélgica y en Finlandia no se disponía del rango de edades completo; en Hungría e Italia no se formuló la pregunta. La pregunta (QF24) era la siguiente: «Pensando en la ÚLTIMA VEZ que alguien te trató de forma hiriente o desagradable EN INTERNET, ¿cómo te sentiste?». Los resultados incluyen el porcentaje de niños que respondieron «Me sentí un poco molesto», «Me sentí bastante molesto» o «Me sentí muy molesto» de entre todos los niños de entre 9 y 16 años que utilizan Internet y que declararon haber sido víctimas de acoso en línea al menos en algunas ocasiones.

Fuente: Smahel et al., 2020.

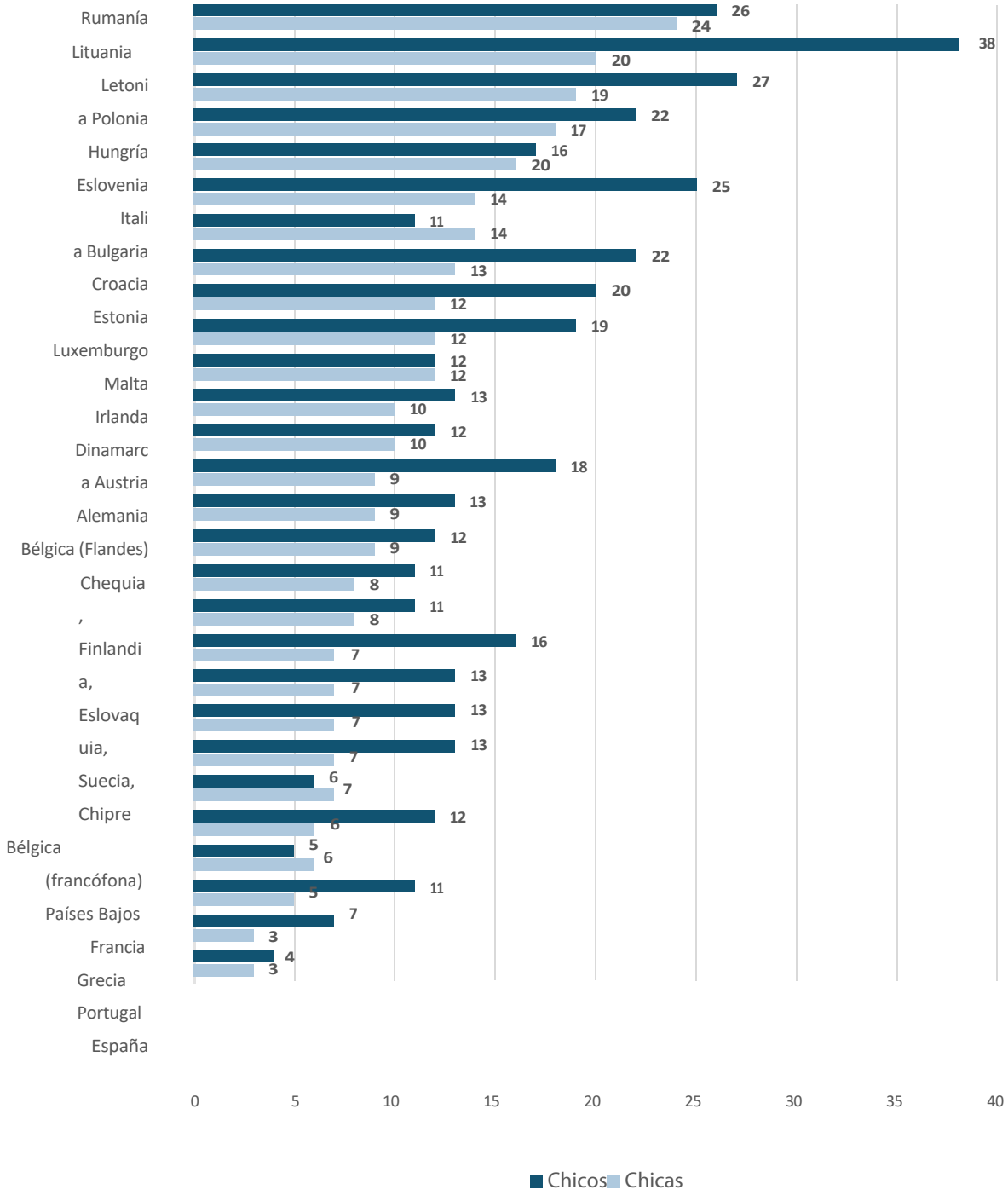
FIGURA A12 | Niños que declaran haber sufrido daños por acoso en línea (al menos un poco molesto), por grupo de edad y Estado miembro (%, niños de 9 a 16 años, 2020)



Nota: En la Región Flamenca de Bélgica y en Finlandia no se disponía del rango de edades completo; en Hungría e Italia no se formuló la pregunta. La pregunta (QF24) era la siguiente: «Pensando en la ÚLTIMA VEZ que alguien te trató de forma hiriente o desagradable EN INTERNET, ¿cómo te sentiste?». Los resultados incluyen el porcentaje de niños que respondieron «Me sentí un poco molesto», «Me sentí bastante molesto» o «Me sentí muy molesto» de entre todos los niños de 9 a 16 años que utilizan Internet y que declararon haber sido víctimas de acoso en línea al menos en algunas ocasiones.

Fuente: Smahel et al., 2020.

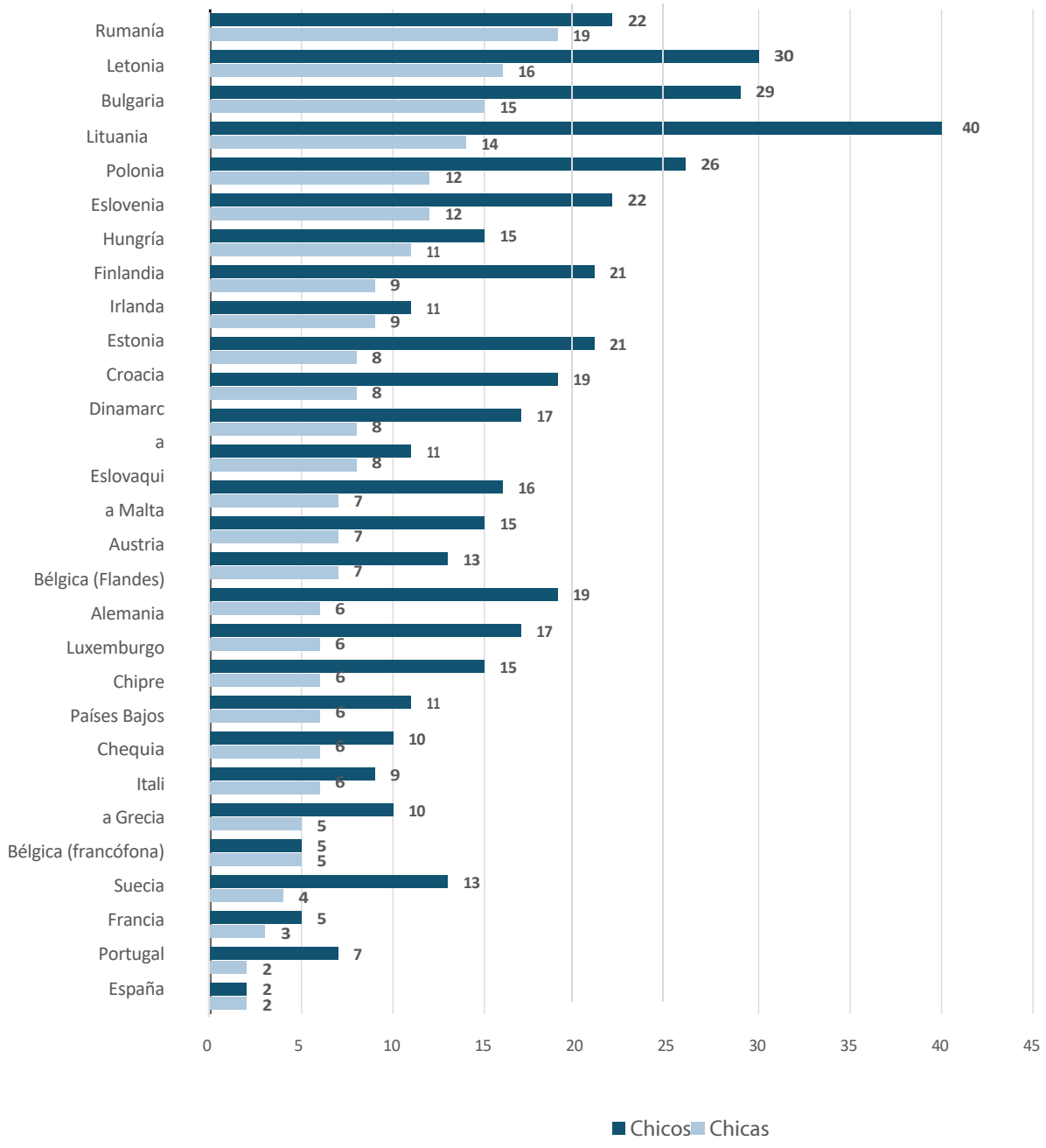
Figura A13 | Jóvenes de 13 años que han acosado a otras personas por Internet al menos una vez en los últimos dos meses, por sexo y Estado miembro (%, 2021-2022)



Nota: Se preguntó a los jóvenes si habían participado en actos de ciberacoso (por ejemplo, enviar mensajes instantáneos, publicaciones en el muro o correos electrónicos ofensivos, o publicar o compartir fotos o vídeos en línea sin permiso). Las opciones de respuesta iban desde «No he acosado a otra persona por Internet en los últimos dos meses» hasta «Varias veces a la semana». Los resultados que aquí se presentan muestran el porcentaje de jóvenes que habían acosado a otras personas por Internet al menos una vez en los últimos dos meses.

Fuente: Explorador de datos del estudio HBSC (resultados de la encuesta HBSC 2021-2022) – https://data-browser.hbsc.org.

Figura A14 | Jóvenes de quince años que han acosado a otras personas en Internet al menos una vez en los últimos dos meses, por sexo y Estado miembro (%, 2021-2022)



Nota: Se preguntó a los jóvenes si habían participado en actos de ciberacoso (por ejemplo, enviar mensajes instantáneos, publicaciones en el muro o correos electrónicos ofensivos, o publicar o compartir fotos o vídeos en línea sin permiso). Las opciones de respuesta iban desde «No he acosado a otra persona por Internet en los últimos dos meses» hasta «Varias veces a la semana». Los resultados que aquí se presentan muestran el porcentaje de jóvenes que habían acosado a otras personas por Internet al menos una vez en los últimos dos meses.

Fuente: Explorador de datos del estudio HBSC (resultados de la encuesta HBSC 2021-2022) – https://data-browser.hbsc.org.

Tablas

Tabla A1: Ejemplos de documentos normativos y jurídicos internacionales que abordan la ciberviolencia

Instrumento	Año y organismo	Ámbito de aplicación y disposiciones principales	Dimensión de la ciberviolencia	Relevancia para la acción de la UE
Documento de investigación de ONU Mujeres y la OMS sobre la violencia contra las mujeres facilitada por la tecnología	2023, ONU y la OMS	Pone de relieve las lagunas en la recopilación de datos; ofrece metodologías para obtener mejores datos empíricos.	Aboga por la inclusión de experiencias diversas en la elaboración de políticas.	Apoya el énfasis de la UE en la formulación de políticas basada en datos y en los enfoques interseccionales.
Recomendación general n.º 1 de GREVIO sobre la dimensión digital de la violencia contra las mujeres	2021, Consejo de Europa	Ofrece orientación sobre la aplicación del Convenio de Estambul en el contexto digital.	Hace hincapié en los planes de acción nacionales, la alfabetización digital y la formación de las fuerzas del orden.	Sirve de base para las recomendaciones de la UE sobre formación, prevención y alfabetización digital.
Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, relativo a la violencia en línea contra las mujeres y las niñas desde una perspectiva de derechos humanos	2018, ONU	Identifica formas de ciberviolencia, como el ciberacoso, el hostigamiento y difusión de imágenes sin consentimiento; recomienda una reforma legal y un cambio sistémico.	Hace especial hincapié en las soluciones centradas en las víctimas y en la educación para la alfabetización digital.	Proporciona el marco de derechos humanos utilizado en los debates y documentos del Parlamento Europeo.
Convenio sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica (Convenio de Estambul)	2011, Consejo de Europa	Es un tratado integral contra la violencia contra las mujeres; exige a los Estados que tipifiquen como delito múltiples formas de abuso.	Incluye explícitamente el abuso en línea (acoso cibernético, hostigamiento, imágenes no consentidas).	Base sobre la que la UE insta a los Estados miembros a ratificar y aplicar la legislación contra la violencia contra las mujeres; en consonancia con la Directiva (UE) 2024/1385.

Instrumento	Año y organismo	Ámbito de aplicación y disposiciones principales	Dimensión de la ciberviolencia	Relevancia para la acción de la UE
Convenio de Lanzarote sobre la protección de los niños contra la explotación y el abuso sexuales	2007, Consejo de Europa	Protege a los menores de la explotación y el abuso sexuales.	Incluye la explotación digital; las directrices del Comité de Lanzarote (2017, 2022) hacen hincapié en la importancia de educar a los niños sobre la seguridad digital, promover una moderación de contenidos adecuada a la edad, garantizar la responsabilidad de las plataformas y mejorar la colaboración intersectorial entre gobiernos, empresas tecnológicas, ONG y fuerzas del orden.	Refuerza las estrategias de la UE en materia de protección de la infancia (por ejemplo, el Reglamento (UE) 2021/1232; la estrategia «Un Internet mejor para los niños»).
Convenio de Budapest sobre la Ciberdelincuencia y su Segundo Protocolo Adicional	2001–2022, Consejo de Europa	Primer tratado internacional vinculante sobre la ciberdelincuencia; establece la cooperación transfronteriza y la responsabilidad de las plataformas.	Abarca el acoso cibernético, la captación de menores con fines sexuales, las imágenes no consentidas y la explotación en línea.	Proporciona herramientas jurídicas y operativas a los Estados miembros para perseguir los delitos cibernéticos transfronterizos.

Tabla A2: Ejemplos de novedades normativas de la UE sobre la violencia (cibernética) de género

	Instrumento	Año	Ámbito de aplicación y disposiciones principales	Dimensión de la violencia cibernética	Relevancia/Valor añadido
Fortalecimiento de las protecciones jurídicas ante los nuevos retos	Directiva de la UE sobre la violencia contra las mujeres	2024	Supone un importante compromiso legislativo para combatir la ciberviolencia contra las mujeres y las niñas, ya que obliga a los Estados miembros a actuar contra formas específicas de ciberviolencia.	Establece definiciones comunes para las cuatro formas principales de violencia cibernética. Fija normas mínimas para la tipificación como delito y exige la recopilación de datos.	Aborda los problemas de larga data relacionados con la diversidad y multiplicidad de definiciones y con un enfoque fragmentado de la tipificación penal. Establece un marco para la recopilación armonizada de datos que probablemente mejorará la investigación y el seguimiento.
	Ley de la UE sobre la IA (Reglamento 2024/1689)	2024	Primera ley del mundo sobre IA; establece obligaciones para la IA de alto riesgo y la transparencia de los contenidos.	Exige el etiquetado de los contenidos «deepfake» generados por IA.	Supone una respuesta directa a los «deepnudes» y a las imágenes íntimas sintéticas no consentidas; refuerza la transparencia y la rendición de cuentas.
	DSA	2022	Impone normas estrictas de moderación de contenidos a las grandes plataformas en línea.	Exige la moderación proactiva de contenidos ilegales y nocivos, incluido el material de abuso sexual infantil y las imágenes íntimas no consentidas.	Es la herramienta clave para garantizar la rendición de cuentas de las plataformas. La Directiva (UE) 2024/1385 se ajusta a los mecanismos de aplicación de la DSA.
	Directiva sobre servicios de medios audiovisuales (2018/1808)	2018	Regula los servicios de medios de comunicación en todos los Estados miembros.	Incluye disposiciones contra el discurso de odio en línea y los contenidos nocivos.	Amplía la protección a las plataformas en línea; permite un enfoque interseccional respecto a los grupos vulnerables.
	RGPD	2018	Refuerza los derechos sobre los datos personales; establece garantías contra el uso indebido.	Permite la eliminación de contenidos personales nocivos o no consentidos en Internet.	Ofrece una protección basada en la privacidad que suelen utilizar las víctimas de la ciberviolencia.

	Instrumento	Año	Ámbito de aplicación y disposiciones principales	Dimensión de la ciberviolencia	Relevancia/Valor añadido
Ampliación de los sistemas de apoyo a las víctimas	Directiva sobre los derechos de las víctimas (2012/29/UE, revisión propuesta en 2023)	2012 / revisión en curso	Establece normas mínimas en materia de derechos y apoyo a las víctimas.	Facilita el acceso al asesoramiento, a la denuncia y a la asistencia jurídica; entre sus propuestas se incluyen mayores protecciones digitales para los grupos vulnerables.	Constituye una piedra angular del enfoque de la UE centrado en las víctimas; está en consonancia con la Directiva (UE) 2024/1385, que mejora el apoyo a las víctimas mediante la introducción de mecanismos de denuncia anónima en línea, servicios especializados de asesoramiento y salud mental e iniciativas de prevención (por ejemplo, el artículo 34.5 de la Directiva (UE) 2024/1385 apoya la creación de medidas preventivas para los hombres).
Seguimiento y evaluación mediante la colaboración	Código de conducta de la UE para la lucha contra el discurso de odio ilegal en línea	2016 (integrado en la DSA en 2025)	Promueve la colaboración con las principales plataformas para eliminar el discurso de odio.	Aborda el discurso de odio en línea; ahora reforzado mediante las disposiciones de la DSA.	Es un instrumento de cooperación entre el sector público y el privado; garantiza una eliminación más rápida de los contenidos y la rendición de cuentas en línea.
Medidas para proteger a los menores y abordar los riesgos específicos de género	Reglamento (UE) 2021/1232	2021	Permite la detección y la retirada de material de abuso sexual infantil, al tiempo que garantiza el cumplimiento de las garantías de la UE en materia de privacidad y protección de datos.	Protege a los menores de la explotación sexual en línea, incluidas las niñas.	Refuerza el cumplimiento de las normas de privacidad al tiempo que combate el material de abuso sexual infantil.
	Estrategia «Una Internet mejor para los niños»	2022	Promueve la alfabetización digital y la seguridad en línea en todos los Estados miembros.	Aborda explícitamente la ciberviolencia a través del ciberacoso, los contenidos nocivos, el acoso, la exposición a contenidos de abuso sexual, los contenidos violentos, los riesgos de autolesión, etc. También tiene como objetivo prevenir y responder a las conductas nocivas entre los menores en línea.	Proporciona un marco integral y centrado en la infancia que vincula las medidas legales y normativas (como la DSA) con la sensibilización, la educación y la participación directa de los niños.
	Estrategias de la UE: estrategia de igualdad de género 2020-2025; estrategia sobre los derechos de las víctimas 2020-2025; estrategia 2020-2025 para una lucha más eficaz contra el abuso sexual infantil	2020-2025	Presentar hojas de ruta políticas para la igualdad, la protección de las víctimas y la seguridad infantil.	Hacer hincapié en la prevención de la violencia de género en línea, la alfabetización digital, la responsabilidad de las plataformas y la protección de la infancia.	Proporcionar orientaciones significativas sobre la violencia de género que se ajusten a las directivas vinculantes.

Tabla A3: Ejemplos de jurisprudencia específica relacionada con la violencia cibernética

Estado miembro	N.º de sentencia	Descripción
Italia	Sentencia del Tribunal Supremo n.º 3989/2019 ([59])	En este caso, el acusado fue condenado por acoso a través de mensajes de WhatsApp. El acusado alegó que los mensajes privados entre dos usuarios no debían considerarse un medio electrónico a efectos de la ley. Sin embargo, el Tribunal Supremo italiano rechazó este argumento, afirmando que la comunicación a través de WhatsApp constituye el uso de medios electrónicos o telemáticos, lo que agrava el delito de acoso. El tribunal dictaminó que el acusado debía cumplir una pena de seis meses de prisión, al considerar que dichas plataformas de mensajería entran en el ámbito de aplicación del artículo 612-bis.
	Sentencia del Tribunal Supremo n.º 33230/2024 ([60])	Esta sentencia abordó la distinción entre el acoso (artículo 612-bis) y la difusión ilícita de imágenes sexualmente explícitas (artículo 612-ter, conocido como «porno vengativo»). El acusado fue condenado por ambos delitos tras enviar mensajes ofensivos y difundir imágenes íntimas de su expareja a través de medios electrónicos. El Tribunal Supremo italiano destacó que el intercambio no autorizado de imágenes explícitas constituye un delito distinto del acoso, subrayando el reconocimiento por parte del ordenamiento jurídico de una serie de conductas relacionadas con las TIC como actos delictivos.
Rumanía	Sentencia del Tribunal Europeo de Derechos Humanos n.º 56867/15 (Buturugă contra Rumanía) ([61])	En este caso, el Tribunal Europeo de Derechos Humanos determinó que las autoridades rumanas no investigaron adecuadamente ni las denuncias de violencia doméstica ni las de ciberacoso. La demandante denunció el comportamiento violento de su exmarido y alegó que este había accedido a sus cuentas electrónicas privadas sin su consentimiento. Sin embargo, los tribunales desestimaron sus denuncias, argumentando que las violaciones de la privacidad en línea no guardaban relación con el caso. El tribunal dictaminó que las violaciones cibernéticas, incluido el acceso no autorizado a la correspondencia electrónica, constituyen una forma de violencia doméstica y requieren un examen exhaustivo. Se determinó que Rumanía había violado los artículos 3 y 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, y se concedió a la demandante una indemnización de 10 000 euros por daños morales.
	Tribunal Europeo de Derechos Humanos, n.º 28935/21 (M. Ş. D. contra Rumanía) ([62])	El caso se refiere a la gestión por parte de las autoridades nacionales de la denuncia de la demandante sobre un presunto acoso en línea por parte de su expareja, supuestamente motivado por venganza, que incluía la difusión pública no consentida de fotografías íntimas de la demandante. El Tribunal determinó que Rumanía había vulnerado el derecho de una mujer a la intimidad y a la vida familiar al no proporcionar protección contra la ciberviolencia.

Fuente: Autores.

59 «Acoso a través de WhatsApp» – VGS Family Lawyers.
60 «Sentencia del Tribunal Supremo: La frontera entre el acoso y el porno vengativo» – Studio Legale Bianucci.
61 Sentencia del Tribunal Europeo de Derechos Humanos de 28 de marzo de 2024, Buturugă c. Rumanía, n.º 56867/15, ECLI:CE:ECHR:2020:0211JUD005686715.
62 Sentencia del Tribunal Europeo de Derechos Humanos, M. Ş. D. contra Rumanía, n.º 28935/21, ECLI:CE:ECHR:2024:1203JUD002893521.

Tabla A4: Experiencias de ciberviolencia entre los jóvenes, por edad y sexo (%)

	Insultos ofensivos	Difusión de rumores falsos sobre ellos	Recibir imágenes explícitas que no han solicitado	Que alguien que no sea uno de sus padres les pregunte constantemente dónde están, qué están haciendo o con quién están	Amenazas físicas	Que se compartan imágenes explícitas de ellos sin su consentimiento	Cualquier tipo de ciberacoso
Chicos	31	16	15	13	10	5	43
Chicas	32	29	19	17	10	8	49
Blanco	35	24	16	14	10	6	48
Negro	29	17	21	9	11	10	40
Hispanos	29	21	19	21	10	7	47
De 13 a 14 años	29	20	11	12	10	4	42
De 15 a 17 años	34	24	22	17	10	8	49
Chicos de 13 a 14 años	31	15	11	12	10	3	41
Chicos de entre 15 y 17 años	32	16	18	13	10	7	44
Niñas de entre 13 y 14 años	25	24	10	12	9	5	41
Chicas de entre 15 y 17 años	36	33	25	20	10	9	54

Nota: Las cifras correspondientes a los jóvenes blancos y negros se refieren a aquellos que declararon pertenecer a una sola raza (y no ser hispanos). Los jóvenes hispanos son aquellos de cualquier otra raza. No se incluyen aquellos que no respondieron a esta pregunta. A los jóvenes se les planteó la siguiente pregunta: «Pensando en tus experiencias en Internet o con tu móvil, ¿cuál de las siguientes situaciones, si es que hay alguna, te ha ocurrido personalmente alguna vez?».

Fuente: Vogels, 2022; encuesta realizada del 14 de abril al 4 de mayo de 2022.

Tabla A5: Tipos de ciberviolencia sufridos o presenciados por las participantes de los grupos focales (de 13 a 18 años, grupos focales realizados entre marzo de 2025 y junio de 2025)

Tipo de ciberviolencia	Descripción	Relación con las formas de ciberviolencia contempladas en la Directiva (UE) 2024/1385	Ejemplos de citas
Ciberviolencia o acoso (sexual)	Incluye mensajes o imágenes de carácter sexual no solicitados, captación de menores con fines sexuales, coacción para obtener desnudos, pornografía de venganza, deepfakes y amenazas sexuales.	Ciberacoso (incluido el ciberacoso escolar)	«Y hay una aplicación llamada Snapchat. Y en esta aplicación, una amiga mía en concreto aceptaba a todo el mundo que la invitaba. Y era como que, cuando abrías los mensajes, todos eran simplemente de un pene desnudo». (Polonia, 13-15) «Ya estaba en Omegle con mis amigas en una fiesta de pijamas [fiesta de pijamas en casa de una amiga]. Esto es típico en las fiestas de pijamas. Me conecté con un chico así. Le digo: "Hola", "¿De dónde eres?", una conversación, y de repente estoy [como] "espera, ¿qué estás haciendo?", y pensé: "¡Qué asco!", me enseñó sus [genitales]. ¡Pasa todo el rato! ¡Hola, hola, saltar, saltar, saltar! Y luego, tras unos tres saltos más, volvía a ser lo mismo.» (Polonia, 13-15) «Más adelante empecé a unirme a otros servidores y entonces me llovieron, literalmente, mensajes de gente que me escribía, y en algún momento me hice amiga de un chico. Me dijo que tenía más o menos mi misma edad y cosas así, y estuvimos escribiéndonos durante mucho tiempo hasta que empezamos a «salir» [es decir, a ser una «pareja»]. Obviamente, era algo así como, ya sabes, yo con nueve años y un chico en Discord. Y luego me enteré, mucho tiempo después, porque solía decirme cosas como «bueno, si no me respondes, ¿me voy a suicidar?», y es que él estaba en una zona horaria diferente, así que a menudo me quedaba despierta toda la noche para hablar con él, porque no quería que se suicidara. Y al cabo de un tiempo, simplemente… hubo una conversación del tipo: «Tengo que contarte algo». «Bueno, ¿qué tienes que contarme?», «En realidad tengo 19 años». No solo tenía 19 años, sino que no era una sola persona, sino tres personas que compartían una cuenta y escribían a menores en Discord haciéndose pasar por un personaje que se habían inventado. Y además estafaban a estos chicos con «fotos desnudas», «imágenes subidas de tono» y cosas por el estilo». (Polonia, 13–15) En algunos países, TikTok ofrece ahora la posibilidad de publicar fotos directamente en la sección de comentarios, y hay gente que, literalmente, publica porno allí, GIF de algún tipo, cosas así. Puede ser una foto, puede ser un GIF de unos segundos y, muy a menudo, puede ser porno. Puede ser incluso cualquier cosa, quizá una broma, algo gracioso; quizá recibas comentarios como este: «¡Qué [pene] más grande!», y hasta se mueve». (Polonia, 13-15)

Tipos de ciberviolencia	Descripción	Relación con las formas de ciberviolencia contempladas en la Directiva (UE) 2024/1385	Ejemplos de citas
			Había una persona que, por su perfil, parecía un hombre mayor que le enviaba mensajes porque esta chica tenía un perfil de Instagram y él no paraba de enviarle diversos mensajes provocativos, pidiéndole que le enviara fotos de ella en ropa interior o incluso sin [ropa interior], quizá en ciertas posturas, no precisamente las más apropiadas. Y cada vez que ella lo bloqueaba, él creaba otros perfiles y seguía escribiéndole, así que no aceptaba el rechazo». (Italia, 13-15)
			Sí, o una cuenta llamada «Cachondo en [ciudad]» te añadía. Eso tampoco es raro. O «enviando desnudos»; tampoco es raro. Tíos cachondos de [ciudad], hay un montón. Incluso ahora puedo entrar en mi Snap[chat] y hay varios de ellos que dicen cosas como «cachondo, buscando una chica guapa». (Suecia, 13-15)
			«Estaba en un grupo con un chico muy inmaduro. Me envió un mensaje privado una vez y luego siguió… Al menos cada tres meses, digamos… y me escribía, digamos —cómo decirlo— [para ver] si quería enviarle un mensaje, si quería que él me enviara un mensaje, si quería tener sexo, esto y lo otro». (Chipre, 16-18)

Tipo de ciberviolencia	Descripción	Relación con las formas de ciberviolencia contempladas en la Directiva (UE) 2024/1385	Citas de ejemplo
Ciberacoso	Contacto persistente no deseado, seguimiento a través de cuentas falsas, manipulación emocional (p. ej., amenazas de suicidio) y control en las relaciones.	Acoso cibernético	«Da la sensación de que lo primero que te pregunta un chico… cuando lo añades en Snap[chat] es sobre ti, pero luego siempre envía una foto. Siempre son fotos…» (Suecia, 16-18)
			«Este chico haría cualquier cosa por recuperarla: la acosaba, le enviaba mensajes e intentaba privarla de todo… pero ella solo era una niña; no creo que tuviera ni siquiera quince años». (Italia, 16-18)
			«Al cabo de un tiempo se volvió un poco posesivo y, cuando ella rompió con él, intentó localizarla a través de otras cuentas y de sus amigos, llegando incluso a recurrir al chantaje, diciendo que se suicidaría o cosas por el estilo». (Italia, 16-18)
			«Pero también está el caso de una chica de mi clase… un chico de mi clase está obsesionado con ella. Llevamos mucho tiempo intentando que los profesores y demás lo entiendan, pero él sigue enviando fotos en las que se ve cómo se pone cuchillos en los brazos y dice: “Si no te quedas conmigo, me suicidaré”». (Suecia, 13–15)
			«Fue un chico que le escribió algo, y ella le respondió… entonces él empezó a ponerse un poco raro. Ella lo bloqueó, pero él seguía abriendo nuevas cuentas y escribiéndole. Por mucho que ella lo bloqueara, él seguía insistiendo —y ella no podía saber que [él haría algo así]». «Nunca se sabe». (Suecia, 16–18)
			«Eran amigos por Internet. Y al cabo de unos meses, dijimos: “Ya que nos llevamos tan bien, enseñémonos la cara”. Vale, nos enseñamos la cara, y como yo tenía 12 años por entonces y estaba un poco gordito, empezaron a burlarse de mí y me echaron del grupo». (Chipre, 16–18)

Tipo de ciberviolencia	Descripción	Relación con las formas de ciberviolencia contempladas en la Directiva (UE) 2024/1385	Citas de ejemplo
Ciberacoso (incluido el ciberbullying)	Mensajes de odio, chats grupales dirigidos a personas concretas, exclusión, difusión de rumores, burlas, ataques verbales, humillaciones, difusión de noticias falsas y humillación pública coordinada que afectan al bienestar mental.	Ciberacoso; incitación cibernética al odio o a la violencia	«Creo que todos nos hemos fijado, ya sea en TikTok o en Instagram, en una chica que publicó unas fotos y ahora hay mensajes que se pueden escribir a alguien cuando publica una historia, que son anónimos, y lo que la gente le escribe en esos mensajes es muy desagradable y tiene un contenido repugnante». (Chipre, 16-18 años)
			«Empezó a difundir rumores sobre mí, como para vengarse, y llegamos a un punto en el que tenía a toda la clase en mi contra. Como mi colegio era pequeño, los rumores se extendieron rápidamente a las otras secciones y a varias clases, y no pude soportarlo… pasar ocho horas en el colegio con todo el mundo mirándote y susurrando bromas a tus espaldas». (Italia, 13-15)
			«Algunas personas de mi antiguo colegio habían creado un grupo en Messenger. Estaba ahí literalmente solo para menospreciarnos a mí y a mis dos amigos. Era una tontería porque no publicaban nada, sino que [reenviaban algunas fotos de] diferentes cuentas de Instagram y luego se las comentaban entre ellos. O también estaba el hecho de que empezaron a generar historias con IA». (Polonia, 13-15)
			«Pues sí, ya te habrás dado cuenta de que en los cursos inferiores se trata principalmente de enviar fotos de desnudos y difundir rumores y cosas así. Sin duda hubo uno o dos casos en los cursos inferiores. Creo que todo el mundo se dio cuenta de eso también. Y eso sin duda también ocurre aquí, en nuestro colegio». (Alemania, 16-18)
			«Me enteré por una chica de que tenían un grupo en el que se enviaban fotos mías y de un amigo nuestro juntos en ciertos sitios, como cuando íbamos a una [tienda] de té de burbujas, por ejemplo, y había una foto nuestra tomada desde atrás. O cuando estábamos en el colegio y él me estaba ayudando porque yo no entendía algo de matemáticas y los dos estábamos inclinados sobre el cuaderno así. También había fotos como esas por todas partes. Y no paraba, no paraba, ni siquiera cuando dejé el colegio». (Polonia, 13–15)

Tipo de ciberviolencia	Descripción	Relación con las formas de ciberviolencia contempladas en la Directiva (UE) 2024/1385	Ejemplos de citas
			Decidieron que, de repente, iban a empezar a insultarla en su cuenta pública de Instagram. Y empezaron a escribir cosas realmente crueles sobre ella. Y ahora hay hilos en Instagram. Y allí empezaron a escribir su nombre y a decir que es estúpida, por ejemplo, o «que le den». Y han creado algo parecido a una imagen de un pene… con coches, y la han subido a la cuenta; han creado fotos de ella junto a esa imagen, comparándola con ese coche del vídeo, y cosas por el estilo… […] Pero recuerdo que lo peor es que esas chicas lo hacían sin motivo alguno. No había pasado nada antes, antes se habían portado muy bien con ella. Y, de repente, pasaron de esa amistad a situaciones muy extrañas y, aun así, fue horrible». (Polonia, 16-18)
			«Hay juegos como Valorant… en los que hay una opción para entrar en un chat de voz. Y puedo decir… que no hay un solo día en el que no ocurra… Digo "hola", oyen que es una voz femenina y empiezan a gritar. Se oyen mucho esos comentarios del tipo «vete a la cocina». Si juego mal, dicen que juego mal porque soy mujer. Si juego bien, empiezan a discutir aún más.» (Polonia, 13-15)
			A mí también me ha pasado, sí, me enteré de esto, de una persona a la que no conozco directamente, de la que oí hablar, y que le envió vídeos a su novio, y esos vídeos se difundieron por todo el colegio y todo eso.» (Italia, 13-15)

Tipo de ciberviolencia	Descripción	Relación con las formas de ciberviolencia contempladas en la Directiva (UE) 2024/1385	Ejemplos de citas
Ciberviolencia basada en imágenes	Tomar o manipular imágenes o vídeos de forma secreta, compartirlos sin consentimiento o crear deepfakes de carácter sexual.	Difusión no consentida de imágenes íntimas	«En mi clase, en los primeros cursos de secundaria, hubo un periodo en el que los padres y los profesores tuvieron que intervenir porque unos chicos fotografiaron las partes íntimas de otra compañera y difundieron las fotos por el instituto y la clase, y el asunto salió a la luz». (Italia, 13-15)
			«Ella no quería salir con él, ni tener una relación, y él, literalmente, creó un deepfake de ella y empezó a difundirlo por todo el instituto. Luego hackeó su cuenta y la de su hermana en Facebook, y empezó a enviar esos deepfakes desde la cuenta de una amiga mía a, literalmente, todos los contactos que ambas tenían». (Polonia, 13-15)
			«Estaba con un chico del que luego descubrí que me había hecho una foto mientras teníamos relaciones sexuales. No la ha compartido, pero sigo pensando: "que se la quede, que se la quede". Da miedo saber que está ahí, porque aunque la haya borrado, podría seguir teniéndola en su móvil». (Suecia, 13-15)
			«Entonces probablemente empezó a enviar mis vídeos, nuestros vídeos —grabábamos vídeos juntos—. Enviaba nuestros vídeos y mis fotos y luego… Y sé que está mal, pero me da pena porque le confié mi cuerpo así sin más. Y luego se lo envía a todo el mundo.» (Alemania, 13–15)
			«Porque, por ejemplo, tengo mi perfil de Instagram, donde quizá solo acepto a ciertas personas. Comparto fotos, incluidas algunas en las que se ven mi cara y mi cuerpo. Quiero decir, sí, mi perfil es privado, así que solo las personas que me siguen pueden ver mis fotos, pero aun así… el mero hecho de saber que en cualquier momento a alguien se le podría ocurrir de repente hacerme una foto y hacer lo que quiera con ella, sinceramente, me da escalofríos. Me hace pensar: espera, quizá debería borrarla» (Italia, 13-15)

Tabla A6: Niños y niñas que han sufrido ciberacoso al menos una vez en los últimos dos meses, por Estado miembro, sexo y nivel de riqueza familiar (%, de 11 a 18 años, 2021-2022)

		Puntuación FAS baja	Puntuación alta en el FAS
Lituania	Chicas	22	23
	Chicos	32	31
Letonia	Chicas	28	24
	Chicos	23	21
Polonia	Chicas	23	20
	Chicos	23	29
Estonia	Niñas	27	21
	Chicos	22	16
Irlanda	Chicas	25	21
	Chicos	21	15
Suecia	Chicas	22	29
	Chicos	13	18
Eslovenia	Chicas	20	18
	Chicos	24	19
Hungría	Chicas	24	18
	Chicos	20	17

		Puntuación baja en la escala FAS	Puntuación alta en la escala FAS
Bulgaria	Niñas	22	16
	Chicos	19	23
Rumanía	Chicas	21	20
	Chicos	28	18
Finlandia	Chicas	17	19
	Chicos	17	20
Croacia	Chicas	18	18
	Chicos	18	16
Chequia	Chicas	19	20
	Chicos	15	13
Dinamarca	Chicas	19	20
	Chicos	14	12
Chipre	Chicas	15	16
	Chicos	15	15
Eslovaquia	Chicas	19	13
	Chicos	16	14

		Puntuación baja en la escala FAS	Puntuación alta en la escala FAS
Luxemburgo	Niñas	19	14
	Chicos	12	13
Bélgica (Región de Flandes)	Chicas	21	15
	Chicos	12	10
Malta	Chicas	16	17
	Chicos	13	12
Alemania	Chicas	16	13
	Chicos	15	10
Italia	Chicas	19	15
	Chicos	11	8
Austria	Chicas	16	13
	Chicos	13	8
Francia	Chicas	15	15
	Chicos	9	11
Bélgica (Región Valona)	Chicas	15	11
	Chicos	10	7

		Puntuación baja en la escala FAS	Puntuación alta en la escala FAS
Grecia	Niñas	11	10
	Chicos	10	11
Portugal	Chicas	10	8
	Chicos	9	9
España	Chicas	11	6
	Chicos	5	4

Nota: FAS – Escala de Riqueza Familiar. El texto en negrita indica una diferencia significativa en la prevalencia entre los grupos de riqueza (con $p < 0,05$). Los grupos de baja y alta riqueza representan el 20 % con menores ingresos y el 20 % con mayores ingresos de cada Estado miembro o región. Los países se ordenan por orden descendente de prevalencia.

Se preguntó a los jóvenes si habían sufrido ciberacoso (por ejemplo, si alguien les había enviado mensajes instantáneos, publicaciones en el muro o correos electrónicos desagradables, o si alguien había publicado o compartido fotos o vídeos en Internet sin su permiso). Las opciones de respuesta iban desde «No he sufrido ciberacoso en los últimos dos meses» hasta «Varias veces a la semana». Los resultados que aquí se presentan muestran el porcentaje de jóvenes que habían sufrido ciberacoso al menos una vez en los últimos dos meses.

Fuente: Explorador de datos del estudio HBSC (resultados de la encuesta HBSC 2021-2022), https://data-browser.hbsc.org.

Tabla A7: Prevalencia del uso problemático de las redes sociales entre los niños, por Estado miembro, sexo y nivel de riqueza familiar

		Puntuación FAS baja	Puntuación FAS alta
Rumanía	Niñas	26	28
	Chicos	16	18
Malta	Chicas	21	25
	Chicos	14	16
Irlanda	Chicas	23	17
	Chicos	11	13
Italia	Chicas	24	16
	Chicos	10	10
Bulgaria	Chicas	19	14
	Chicos	12	13
Bélgica (Región Valona)	Chicas	10	16
	Chicos	10	20
Chipre	Chicas	17	17
	Chicos	11	9
Grecia	Chicas	17	17
	Chicos	7	11

		Puntuación baja en la escala FAS	Puntuación alta en la escala FAS
Lituania	Niñas	18	14
	Chicos	9	12
Croacia	Chicas	11	14
	Chicos	11	16
Polonia	Chicas	13	14
	Chicos	9	9
Luxemburgo	Chicas	17	13
	Chicos	7	7
Germania	Chicas	16	11
	Chicos	8	8
Francia	Chicas	14	13
	Chicos	6	8
Eslovenia	Chicas	12	11
	Chicos	9	9
Bélgica (Región de Flandes)	Chicas	14	9
	Chicos	8	9

		Puntuación baja en la escala FAS	Puntuación FAS alta
Austria	Niñas	12	7
	Chicos	11	9
España	Chicas	16	11
	Chicos	5	6
Portugal	Chicas	10	10
	Chicos	8	8
Estonia	Niñas	14	9
	Chicos	7	6
Chequia	Chicas	11	11
	Chicos	6	7
Finlandia	Chicas	7	7
	Chicos	9	11
Suecia	Chicas	11	12
	Chicos	3	7
Dinamarca	Chicas	12	8
	Chicos	8	6

		Puntuación FAS baja	Puntuación FAS alta
Letonia	Niñas	11	8
	Chicos	4	6
Hungría	Chicas	8	8
	Chicos	7	5

Nota: FAS: Escala de Riqueza Familiar. El texto en negrita indica una diferencia significativa en la prevalencia según el grupo de riqueza familiar (con $p < 0,05$). Los grupos de baja y alta riqueza representan el 20 % con menores ingresos y el 20 % con mayores ingresos de cada Estado miembro o región. Los países se ordenan por orden descendente de prevalencia. Se pidió a los jóvenes que informaran de los síntomas de un uso problemático (similar a una adicción) de las redes sociales utilizando la Escala de Trastorno de las Redes Sociales, una escala de nueve ítems en la que los encuestados respondían a cada pregunta con un «sí» o un «no». Los resultados aquí presentados muestran el porcentaje de jóvenes que respondieron «sí» a seis o más preguntas y que, por lo tanto, fueron clasificados como usuarios problemáticos de las redes sociales.

Fuente: Explorador de datos del estudio HBSC (resultados de la encuesta HBSC 2021-2022), https://data-browser.hbsc.org.

Tabla A8: Tipos habituales de autores de ciberviolencia

Tipo de agresor	Táctica	Medios utilizados
El troll / el acosador sexual en Internet	Ataca a las mujeres que expresan sus opiniones en Internet	Secciones de comentarios, foros, salas de chat
El «creepshotter» / el voyeur digital	Fotografía a mujeres y niñas sin su consentimiento y publica las fotos en Internet	Lugares públicos fuera de Internet, Reddit, páginas web especializadas, redes sociales
El autor de «porno de venganza» / el violador digital	Publica fotos o vídeos privados de carácter sexual para avergonzar y humillar a la víctima: una extensión de la violencia de pareja	Redes sociales
El captador en línea / el abusador sexual de menores	Establece una relación con un menor a través de Internet para abusar sexualmente de él o traficar con él	Redes sociales, foros
El acosador cibernético / el maltratador obsesivo	Espía, se obsesiona y recopila información sobre mujeres en Internet para asustarlas y chantajearlas	Redes sociales
El masculinista / el misógino	Niega y perpetúa el sexismo sistémico «defendiendo los derechos de los hombres»	Páginas web especializadas, páginas web de colectivos de mujeres, redes sociales
El ciberacosador / el humillador	Envía repetidamente mensajes hirientes y difunde rumores para avergonzar y humillar	Redes sociales, aplicaciones de comunicación
El manipulador de las páginas de citas / el depredador sexual	Busca poder y control sobre su víctima seduciéndola en línea y atrayéndola hacia una situación peligrosa	Páginas web de citas, redes sociales, salas de chat, aplicaciones de comunicación
El reclutador / el traficante de víctimas de violación, también conocido como traficante	Utiliza las nuevas tecnologías para atraer a las víctimas con el fin de traficar con ellas y explotarlas sexualmente	Sitios web de venta, plataformas especializadas, redes sociales, aplicaciones de comunicación
El «doxxer» / el ladrón de datos y el difamador	Investiga y publica información privada en Internet para exponer públicamente, desenmascarar y humillar a las víctimas	Perfiles de las víctimas en redes sociales, búsquedas en Google
El difusor malintencionado / el difamador peligroso	Utiliza nuevas tecnologías y herramientas de propaganda para promover la violencia contra las mujeres o contra los grupos defensores de los derechos de las mujeres	Redes sociales
El hacker / el intruso	Intercepta información y comunicaciones privadas (p. ej., cámaras web)	Puede estar en cualquier lugar

Fuente: Autores, basado en la clasificación propuesta por el Lobby Europeo de las Mujeres.

Tabla A9: Factores que influyen en el comportamiento de los jóvenes espectadores (menores de 20 años) que presencian la ciberviolencia

Categoría	Factor	Resumen
Contextuales	Amistad	La amistad influye tanto positiva como negativamente en el comportamiento de los testigos; las relaciones positivas con las víctimas fomentan la ayuda, mientras que los vínculos fuertes con los agresores inhiben la intervención.
	Entorno social	Las normas sociales y los sistemas de apoyo influyen en el comportamiento tanto de forma positiva como negativa. Los entornos positivos fomentan la intervención, mientras que las normas que respaldan el acoso o el rechazo la desalientan.
	Efecto espectador	La probabilidad de intervención disminuye a medida que aumenta el número de espectadores (debido a la difusión de la responsabilidad). La percepción de las acciones de los demás espectadores también influye.
	Gravedad del incidente	Los incidentes graves y la angustia visible de las víctimas motivan a los espectadores a intervenir.
	Actuación de otros espectadores	Las acciones de los demás espectadores influyen en el comportamiento; si apoyan al acosador, esto desalienta la intervención, pero si defienden a la víctima, esto fomenta el apoyo.
	Solicitud de ayuda	Las peticiones directas de ayuda motivan a los testigos a intervenir, ya que ponen de relieve la gravedad de la situación.
	Evaluación de la situación	El desconocimiento de la situación o unas circunstancias poco claras dificultan la intervención, mientras que la percepción de injusticia la motiva.
	Conocimiento de estrategias	Conocer estrategias de intervención eficaces y recursos de apoyo fomenta las intervenciones positivas.
	Entornos virtuales	La desinhibición y el anonimato en línea pueden fomentar comportamientos negativos, mientras que los canales de comunicación públicos pueden reducirlos.
	Miedo a las represalias	El miedo a las represalias puede disuadir de actuar, aunque las amistades sólidas con las víctimas pueden mitigar este miedo.
Aspectos personales	Empatía	Unos niveles elevados de empatía, especialmente la empatía cognitiva, fomentan comportamientos que apoyan a las víctimas, mientras que una empatía baja puede conducir a acciones pasivas o negativas.
	Desvinculación moral	Un alto nivel de desvinculación moral conduce a un comportamiento negativo por parte de los espectadores, mientras que un bajo nivel de desvinculación suele dar lugar a acciones de ayuda.
	Determinantes conductuales	Factores como la autoeficacia, una actitud positiva y las tendencias prosociales facilitan la intervención, mientras que la impulsividad y la ansiedad social actúan como barreras para intervenir.
	Experiencia previa	Las víctimas en el pasado son más propensas a ayudar, mientras que quienes han sido acosadores anteriormente son más propensos a mostrar comportamientos negativos como espectadores.
	Datos demográficos	En algunos casos, las chicas y las personas más jóvenes son más propensas a intervenir.

Fuente: Los autores, basándose en las conclusiones sobre los factores de Domínguez-Hernández et al. (2018).

European Institute for
Gender Equality

Publications Office
of the European Union
| | Publications

eige.europa.eu

European Institute for
Gender Equality

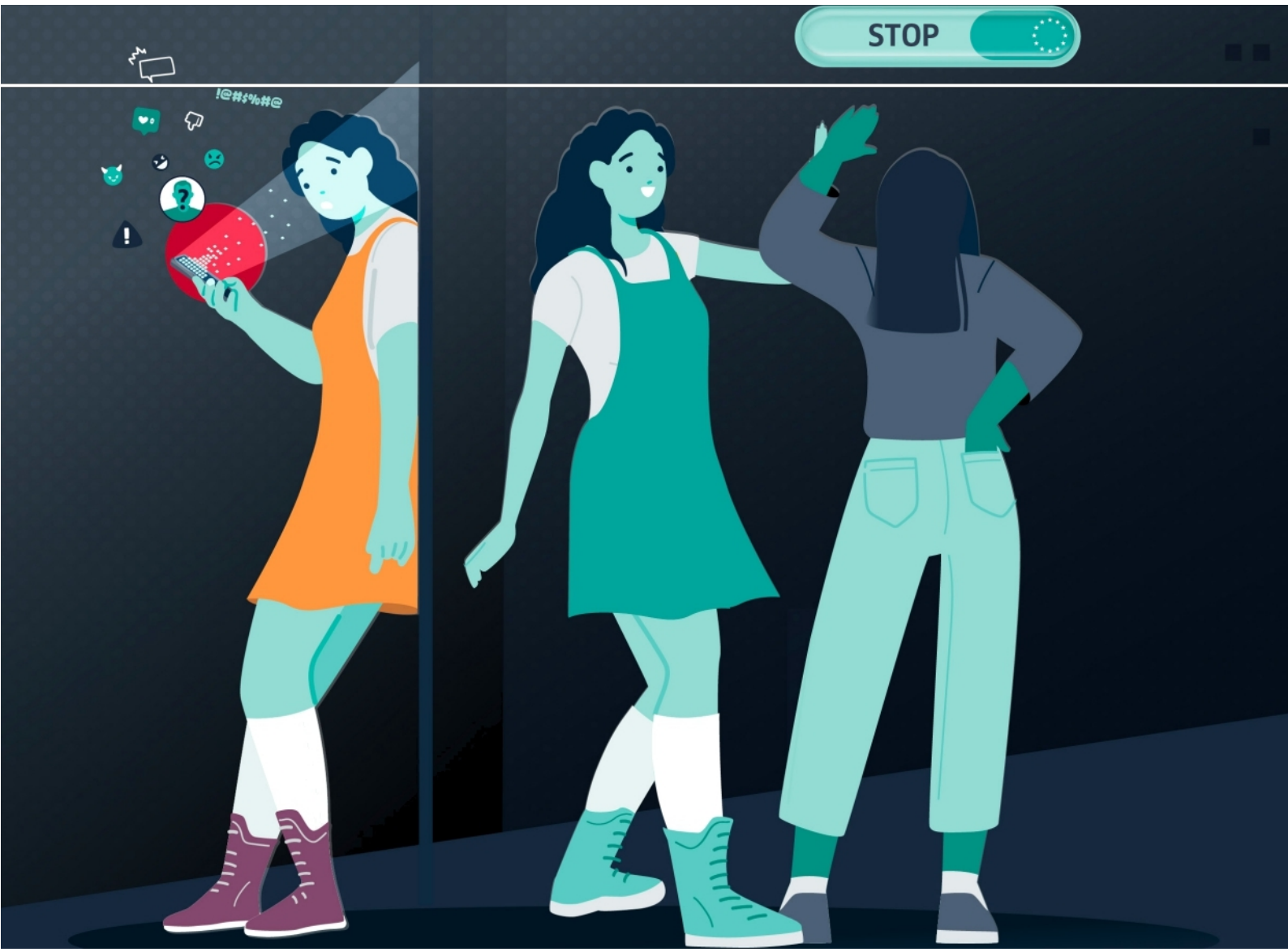
ISBN 978-92-9486-350-8 doi:10.2839/5514733

eige.europa.eu

Instituto Europeo para la Igualdad de Género

DE LA REALIDAD VIVIDA A LA ACCIÓN POLÍTICA:

Combating cyber violence against girls in the EU ...



Una agencia de la UE