REDES QUE ATRAPAN

Save the Children

Colabora:

Asociación Europea para la Transición Digital

La explotación sexual de la infancia y la adolescencia en entornos digitales

Esta publicación ha sido elaborada con la colaboración de la Asociación Europea para la Transición Digital. El estudio se basa en la investigación previa realizada por el equipo de MEDUSA Derechos Humanos, compuesto por Paloma Torres, Isabel Díez y Maribel Rodríguez, y el análisis de datos obtenidos a través de la encuesta realizada por el equipo del Grupo de Investigación en Victimización Infantil y Adolescente (GReVIA) de la Universitat de Barcelona, integrado por Laura Pascual, Alba Águila y Noemí Pereda.

Save the Children

Autoría: ***Clara Burriel.*** Coordinación del proyecto: ***Carmela del Moral.*** Dirección del Departamento de Influencia y Desarrollo Territorial: ***Catalina Perazzo.*** Coordinación gráfica: ***Óscar Naranjo.*** Edición: ***Clara Burriel y Miguel Borque.*** Arte y maquetación: ***Alba Lajarín.*** Fotografía de portada: ***Alba Lajarín.***

Edita:

Save the Children España
Julio 2025

Contenidos

Introducción

Apenas unos meses antes de la publicación de este informe, los medios de comunicación de nuestro país se hacían eco del caso de un hombre que, durante años, explotó sexualmente a una niña de 12 años. El hombre, de 45 años, contactó con ella y se ganó su confianza a través de videollamadas y conversaciones por redes sociales, para después agredirla sexualmente y grabar vídeos y fotografías de estas agresiones. Intercambiaba después este material por Internet con otros pedófilos, y llegó a ofrecer a la niña a través de aplicaciones de citas e Instagram para que otros adultos la violaran y seguir generando imágenes de estas agresiones. Cuando se le detuvo, se encontraron más de 10.000 archivos de «pornografía infantil», cientos de ellos elaborados por él.

Este caso ilustra con crudeza un fenómeno de gran preocupación: el impacto del entorno digital en las dinámicas asociadas a la explotación sexual de la infancia y la adolescencia. Vemos cómo Internet, las redes sociales y las tecnologías no solo facilitan la captación, sino que también pueden ser el medio en el que se cometen estas violencias, y permiten su perpetuación. También evidencia la interrelación de las distintas violencias que forman parte de las dinámicas explotadoras: el contacto y la manipulación a través de las tecnologías (*grooming*) aprovechando las vulnerabilidades, agresiones sexuales físicas, la generación de imágenes de abuso sexual infantil a través de ese abuso, el intercambio posterior de este material y la explotación de la niña para agresiones por terceros, empleando de nuevo los canales digitales para contactar a los agresores. Estas dinámicas (contacto, agresión, difusión, intercambio) ocurren de manera conjunta, siendo difíciles de delimitar, lo que dificulta el entendimiento de qué constituye en realidad la explotación sexual de la infancia y la adolescencia en los entornos digitales.

De hecho, más allá de noticias puntuales, ¿qué sabemos realmente de la explotación sexual de la infancia y la adolescencia en entornos digitales? ¿Hasta qué punto somos conscientes de la prevalencia de estas formas de violencia, de las conductas que abarca, o de cómo puede afectar a los niños, niñas y adolescentes? Y, sobre todo, ¿en qué medida hemos llegado a normalizar como sociedad algunas de las manifestaciones de esta violencia hacia la infancia o los riesgos que conducen a ella?

Con este informe, se pretende arrojar algo de luz sobre un fenómeno especialmente complejo y todavía difícil de delimitar, en parte por la falta de una definición única y por la ausencia de datos que revelen su prevalencia real, pero también en parte por la normalización de determinadas conductas que contribuyen a ocultar su gravedad. Para ello, se ha preguntado a profesionales y personas expertas en la materia, provenientes de diversos ámbitos: jurídico, ciberseguridad y delitos informáticos, psicología, criminología, academia e investigación, y del ámbito de la protección y

los derechos de la infancia. Además, se quiere conocer qué riesgos asociados a la explotación sexual digital identifica, asume y naturaliza la adolescencia en el entorno digital. Para ello, se ha realizado una encuesta a 1.008 jóvenes de entre 18 y 21 años, en la que se les ha preguntado por sus percepciones y conductas *online* durante la adolescencia, con especial foco en los conocimientos, creencias y experiencias relacionadas con la explotación sexual en línea.[1] También se organizaron dos talleres presenciales con adolescentes de entre 15 y 18 años, para profundizar en las preocupaciones y riesgos que identifican en su uso de Internet, así como en cómo perciben y distribuyen la responsabilidad frente a la exposición a estos riesgos.

A partir de este análisis, se busca formular recomendaciones que fortalezcan la protección de niños, niñas y adolescentes frente a esta forma de violencia, también a través de los procesos legislativos actualmente en marcha, para que puedan ejercer de forma segura todos sus derechos en el entorno digital. Y se hace desde un enfoque de infancia, entendiendo que la tecnología y el mundo digital forman parte de la esfera en la que los niños, niñas y adolescentes se desarrollan, y que lo tecnológico está intrínsecamente ligado a su socialización, y también a cómo descubren y exploran su sexualidad, lo que implica riesgos específicos. Pero entendiendo también que estos riesgos no se originan en el vacío, sino que el ecosistema digital proporciona el caldo de cultivo que facilita y condiciona estas dinámicas.

1. Violencias sexuales hacia la infancia y adolescencia en entornos digitales

La era digital ha amplificado riesgos ya existentes para la infancia y adolescencia, generando al mismo tiempo nuevas formas de violencia y nuevas particularidades para formas de violencia ya existentes. Entre ellas, las violencias sexuales destacan por su gravedad y por las dinámicas que adoptan en este entorno.

Las violencias sexuales digitales que afectan a la infancia y la adolescencia comprenden un amplio abanico de situaciones que vulneran la libertad, la integridad y el desarrollo sexual de niños y niñas, entre las que se incluyen, entre otras: el abuso sexual digital, *grooming* o ciberembaucamiento por parte de personas adultas con fines sexuales; el *sexting* sin consentimiento o la difusión no autorizada de contenido íntimo; y formas de abuso y explotación sexual *online*, incluyendo el consumo, producción y la difusión de material de abuso sexual infantil. Entre las tendencias

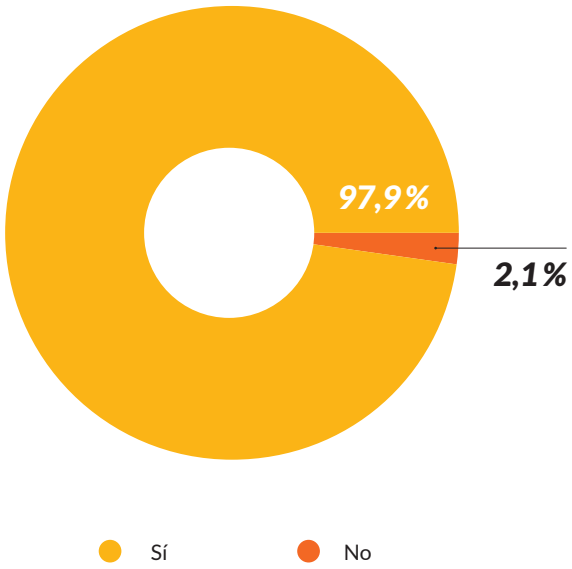
1 Para más información, véase la nota metodológica.

emergentes dentro de este tipo de violencia también destaca el incremento de casos de sextorsión, en los que niños, niñas y adolescentes son coaccionados, chantajeados o amenazados para enviar material íntimo o sexual, y el uso de herramientas de inteligencia artificial generativa para crear digitalmente este tipo de contenido. Es común que estas formas de victimización se interrelacionen, no siempre quedando clara la diferencia o los límites entre ellas, como se verá a lo largo de este estudio.

Según los últimos datos oficiales proporcionados por el Ministerio del Interior, en 2023 se registraron en España 4.896 denuncias por delitos cibernéticos contra niños, niñas y adolescentes, de los cuales 1.068 correspondían a delitos sexuales. Los datos oficiales, sin embargo, tan solo representan la punta del iceberg: la mayoría de casos de violencia contra la infancia y adolescencia no llegan a conocerse, en parte por la ausencia de denuncia y en parte por las dificultades en la detección, que incrementan significativamente cuando estos hechos tienen lugar en el entorno *online*, por las características en cuanto a anonimato, inmediatez y la volatilidad de los contenidos, así como por una menor percepción sobre su gravedad.

Esta brecha entre la realidad y las cifras oficiales queda reflejada también en los datos de la encuesta que hemos realizado en el marco de este informe, dirigida a chicos y chicas de entre 18 y 21 años, en la que les hemos preguntado por las experiencias vividas durante su infancia y adolescencia: así, casi la totalidad de los chicos y chicas encuestadas afirmó haber sufrido algún tipo de victimización sexual en entornos digitales cuando eran menores de edad.

Figura 1. ***Victimizaciones sexuales en el entorno digital antes de los 18 años.***



Estos datos[2] evidencian el enorme riesgo que enfrentan los niños, niñas y adolescentes de encontrarse con alguna forma de violencia sexual en el entorno digital.

2. La explotación sexual de la infancia y la adolescencia en entornos digitales

La explotación sexual de la infancia y la adolescencia en línea (a menudo referida como ESIA digital u *online*, por sus siglas) constituye una de las formas más graves de violencia sexual digital. A pesar de ello, su definición sigue siendo difusa, tanto a nivel jurídico como académico, y a menudo resulta complejo diferenciarla de otras formas de violencia, en especial el abuso sexual.

Limitaciones en la definición de conceptos

Actualmente no existe una definición clara, unánime o consolidada, ni a nivel normativo ni académico, de lo que se entiende por explotación sexual digital de la infancia y la adolescencia. En muchos contextos, incluido el legislativo y el académico, se utilizan a menudo de forma intercambiable los términos «abuso sexual infantil» y «explotación sexual infantil», lo que tiende a diluir las diferencias entre ambos conceptos.

Esta confusión terminológica se traduce también en una falta de delimitación precisa de las conductas que forman parte de cada forma de violencia, siendo frecuente que las referencias al abuso o a la explotación sexual infantil digital abarquen generalmente diferentes y múltiples manifestaciones, como el *grooming*, la sextorsión, la transmisión en directo de abusos sexuales, el consumo o intercambio de material de abuso sexual infantil (CSAM), sin discriminar entre aquellas que constituirían propiamente explotación, aquellas que serían abuso, y aquellas que, podrían ser facilitadoras, sin encajar en las categorías penales de abuso o explotación.

2 En la encuesta se incluyeron distintas formas de victimización sexual digital sufridas durante la infancia y la adolescencia, como el acceso involuntario a contenido sexual, el *grooming*, sextorsión, *sexting* sin consentimiento, creación y difusión de imágenes con inteligencia artificial, explotación sexual. Este dato no incluye las conductas asociadas al *sexting* con consentimiento entre personas menores de edad.

A su vez, esta imprecisión no es neutra: supone una distorsión entre el marco jurídico vigente y los términos utilizados en el debate social y académico, y puede obstaculizar tanto la recogida de datos como el desarrollo de políticas públicas específicas. Como consecuencia, resulta difícil dimensionar de forma adecuada el alcance real de la explotación sexual infantil digital, lo que debilita la respuesta institucional y la capacidad de protección efectiva.

Una de las claves distintivas de la explotación sexual frente a otras formas de violencia sexual infantil radica en la presencia de un intercambio o beneficio, que transforma a niños, niñas y adolescentes en objetos de transacción. Este beneficio puede suponer un lucro económico, y de hecho este suele ser el foco en muchas normativas penales, pero también puede adoptar otras formas más emocionales, simbólicas, afectivas, sociales o relacionales, bastando con que el niño o niña sea instrumentalizado, directa o indirectamente, para la obtención de alguna forma de gratificación por parte del agresor. Así, mientras que el abuso sexual se centraría en la agresión sexual directa (entendida como el ataque a su integridad sexual, tanto en el plano físico como en el digital), la explotación hace referencia a ese componente de instrumentalización, beneficio o lucro, en el que la víctima no es solo un fin en sí misma sino que también es convertida en un medio para obtener un beneficio, que puede ser económico, reputacional o simbólico, o sexual.

«Se entiende que el abuso/agresión es el hecho sobre el cuerpo del NNA (offline u online) y la explotación se vincula al negocio y la generación de material de abuso y poner a circular ese material». —Profesional del ámbito de la justicia

De este modo, en el marco de este informe, se entiende la explotación sexual infantil y adolescente en entornos digitales como una forma de violencia sexual digital caracterizada por la existencia de un intercambio, beneficio o retribución, ya sea para un tercero o para el propio niño, niña o adolescente. Este tipo de violencia implica además el uso de las tecnologías de la información y la comunicación en alguna de sus fases, ya sea como facilitadoras o como contexto en el que tiene lugar. Se incluyen así conductas que van desde la captación digital hasta la difusión del material generado, abarcando también los casos en los que la explotación se docu-

menta y difunde en el entorno digital, con independencia de si el abuso se produce exclusivamente en línea o también en espacios *offline*.

Esta definición va en la línea de las Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales del Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes, conocidas como «Directrices de Luxemburgo»,[3] que incluyen dentro de la explotación sexual digital cualquier uso de las tecnologías que dé lugar a la creación, posesión o difusión de imágenes o materiales que documenten dicha explotación.

> ***«La explotación supone la producción, uso y difusión de imágenes. El grooming o la sextorsión, e incluso el streaming, serían prácticas para la obtención de este tipo de imágenes. Pero todo eso forma parte de la explotación sexual online».*** —Experta en explotación sexual

3. Modalidades de explotación sexual de la infancia y la adolescencia en entornos digitales

En este apartado se abordan las diversas modalidades que, tomando como base la definición propuesta y las aportaciones de personas expertas, se consideran formas de explotación sexual digital de la infancia y la adolescencia. Entre ellas se incluyen la distribución y el consumo de material de abuso sexual infantil y la explotación sexual de niños, niñas y adolescentes en contextos vinculados a la prostitución o a espectáculos pornográficos. Aunque también hemos considerado determinadas prácticas asociadas a la autoexposición por parte de menores de edad como formas de explotación, estas se abordarán de manera detallada en un estudio aparte.

Es importante señalar que las distintas formas de explotación que se analizan a continuación no constituyen fenómenos aislados: en muchos casos, están conectadas entre sí, forman parte de un mismo proceso o se dan al mismo tiempo. Por eso, en la práctica, no siempre será fácil trazar una línea clara que delimite entre unas conductas y otras.

3 Grupo de Trabajo Interinstitucional sobre Explotación Sexual de Niñas, Niños y Adolescentes (2025). Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales (2.ª ed. rev.). ECPAT International (Primera edición publicada en 2016).

3.1. Material visual y representaciones digitales

Las imágenes juegan un papel central en muchas formas de explotación sexual de niñas, niños y adolescentes en entornos digitales. El contenido generado puede ser reutilizado múltiples veces, perpetuando la victimización incluso años después del abuso original.

- **Materiales de abuso sexual infantil**

Una de las manifestaciones más extendidas de esta violencia es la producción, posesión, distribución y consumo de material que representa abuso o explotación sexual de niños, niñas y adolescentes, también conocido como CSAM, por sus siglas en inglés (*Child Sexual Abuse Material*). Este material se define en los distintos instrumentos normativos como aquel que muestra actos de agresiones sexuales a la infancia y la adolescencia o que se centra en la exposición de sus genitales con fines sexuales.

CSAM (Child Sexual Abuse Material)

El CSAM hace referencia a lo que tradicionalmente (e incorrectamente) se conoce como «pornografía infantil». Desde Save the Children, junto a otras organizaciones y personas expertas, venimos desaconsejando el uso de esta expresión,[4] ya que vincula la noción de pornografía con la infancia, minimizando la gravedad de estos actos e incluso contribuyendo a su normalización o legitimación, pues utiliza un lenguaje asociado al consentimiento que corre el riesgo de ser interpretado como que los niños y niñas realizan estos actos de forma voluntaria, cuando en realidad son víctimas de delitos sexuales. Así, mientras que el término «pornografía» se usa principalmente para las representaciones sexuales entre personas adultas que participan en actos consensuados, cuando se involucra a personas menores de edad siempre son actos de abuso sexual. Por ello, hablar de «pornografía infantil» invisibiliza esta realidad. De hecho, este término ya está siendo superado por muchas normativas y directrices, tanto internacionales como europeas.

4 Save the Children (2019) Violencia Viral: Análisis de la violencia contra la infancia y la adolescencia en el entorno digital.

Las imágenes o videos pueden generarse a partir abusos cometidos en entornos físicos, a través de coerción o manipulación, o bien directamente en el entorno digital mediante manipulación, engaños, amenazas o extorsión, que inducen a la víctima menor de edad a producir imágenes de contenido sexual. Por otro lado, este material también puede ser autogenerado por los propios niñas y niños sin que medie una coacción explícita, por ejemplo, a través de conductas normalizadas entre adolescentes como el *sexting*, y luego ser difundido.

En relación con este material como forma de explotación, las Directrices de Luxemburgo han destacado que: «la noción de 'intercambio' se encuentra presente frecuentemente en el marco de material de abuso sexual de niñas, niños y adolescentes (...), ya que dicho material (fotos, videos, etc.) suele ser intercambiado por otro material de abuso sexual o para obtener un beneficio económico y, por lo tanto, también equivale a explotación sexual de niñas, niños y adolescentes».

Aunque la detección de este material todavía presenta grandes desafíos para las autoridades, algunas cifras globales pueden mostrar una idea de la magnitud de este problema: en 2024, la CyberTipline del Centro Nacional para Niños Desaparecidos y Explotados (NCMEC, la organización estadounidense que lidera los esfuerzos para prevenir la explotación sexual infantil, localizar a niños y niñas desaparecidos y reducir la circulación de material de abuso sexual infantil en línea en todo el mundo)[5] registró más de 19,8 millones de denuncias relacionadas con este tipo de material, que contenían 62,9 millones de archivos. Cabe subrayar que casi la totalidad de este contenido fue localizado en canales abiertos y espacios accesibles al público general, no ocultos en la *dark web*. Por otro lado, la Base de Datos Internacional de Interpol (ICSE),[6] especializada en imágenes y vídeos de explotación sexual infantil, registró hasta julio de 2024 más de 4,9 millones de archivos, con más de 42.000 víctimas identificadas y más de 18.000 delincuentes reconocidos. Se ha documentado además que gran parte de este material se origina en países europeos: en 2022, el 68 % de las denuncias realizadas por proveedores de servicios electrónicos a través de la CyberTipline procedían de servicios de mensajería, chat o correo electrónico radicados en la Unión Europea. Además, la Internet Watch Foundation (IWF) informó que el 66 % de todo el CSAM identificado ese año se originó en algún país europeo.[7]

5 National Center for Missing & Exploited Children (NCMEC) (s.f.). CyberTipline Data.

6 INTERPOL. Base de Datos Internacional sobre Explotación Sexual de Niños.

7 Internet Watch Foundation (IWF) (2022). Geographical hosting of URLs. Annual report 2022.

- **Materiales de explotación sexual infantil**

También referido como CSEM (*Child Sexual Exploitation Material*), este material engloba un espectro más amplio que el CSAM, incluyendo representaciones sexualizadas de niñas y niños, que incluyen imágenes o representaciones de NNA en actitudes sexualizadas o situaciones de desnudez parcial o total que, aunque no muestran actos sexuales explícitos, presentan a la infancia desde una mirada sexualizada. A este material también se le denomina como «material de abuso no extremo», «erótica infantil» o representaciones de la «zona gris», términos que le restan gravedad y al no reconocer su naturaleza explotadora, cuando en realidad contribuyen a banalizar las representaciones sexualizadas y la cosificación de la infancia, que alimentan las dinámicas de explotación.

Estos materiales suelen originar controversias, ya que pueden no alcanzar los umbrales legales para ser considerados como CSAM en algunas jurisdicciones, pero plantean igualmente serias preocupaciones por su potencial para normalizar o trivializar la sexualización y la explotación de niños y niñas. También pueden ser utilizados por personas agresoras como material de excitación o para facilitar la captación o el *grooming*. En muchos casos, pueden ser fotografías de la vida cotidiana sin intención sexual, como imágenes en la playa o en actividades deportivas, que son manipuladas o recontextualizadas con fines de explotación o gratificación sexual por parte de adultos.

Este tipo de material presenta un importante desafío para las autoridades, ya que la presencia de CSEM no garantiza la ausencia de abuso, y puede coexistir con material de abuso sexual infantil más explícito. Según datos de Save the Children Europa,[8] muchas de las imágenes recuperadas en páginas de modelaje infantil contenían CSAM, y varias de las víctimas identificadas habían sufrido abusos sexuales. Además, muchos de estos conjuntos de imágenes ilegales incluían también material clasificado como CSEM. Estas páginas, que suelen presentarse como espacios «artísticos» o «profesionales», publican fotografías de niñas y niños en poses «sugerentes» o vestimenta inadecuada para su edad, y son utilizadas con frecuencia como tapadera para la distribución y el consumo de CSAM.

- **Materiales generados digitalmente**

El CSAM y el CSEM también pueden ser generados digitalmente. Estos materiales se componen por representaciones creadas mediante herramientas digitales que simulan a niñas, niños y adolescentes en contextos sexuales o sexualizados. Bajo esta categoría se incluyen imágenes generadas por ordenador, *deepfakes* o ultra

8 Save the Children International (2005). Position paper regarding online images of sexual abuse and other Internet-related sexual exploitation of children.

falsificaciones elaboradas a partir de imágenes reales, así como dibujos o animaciones hiperrealistas, que pueden difundirse de forma masiva y a gran velocidad.

Este tipo de contenido puede originarse a partir de material ya existente de abuso sexual para crear un nuevo material, o transformando mediante inteligencia artificial imágenes publicadas en redes sociales. Aun cuando la creación de este material no implica necesariamente la participación directa de un niño o niña real o la existencia de un abuso sexual previo, estos contenidos constituyen por sí solos una forma de violencia, debido al daño que suponen para la dignidad, el bienestar y la seguridad de las niñas y niños afectados. Además, contribuyen a normalizar de la sexualización infantil, lo que a su vez reduce la percepción de gravedad de estos delitos, y también alimenta la demanda de contenido de abuso, pudiendo aumentar el riesgo de que se produzcan futuras agresiones.[9]

Por otro lado, muchas de estas imágenes resultan «visualmente indistinguibles» de las imágenes reales de abuso sexual infantil, incluso para analistas especializados, lo que plantea enormes retos para la detección, investigación y persecución de estos delitos, ya que dificulta la distinción entre lo real y lo manipulado, complicando a su vez la identificación de víctimas y agresores.

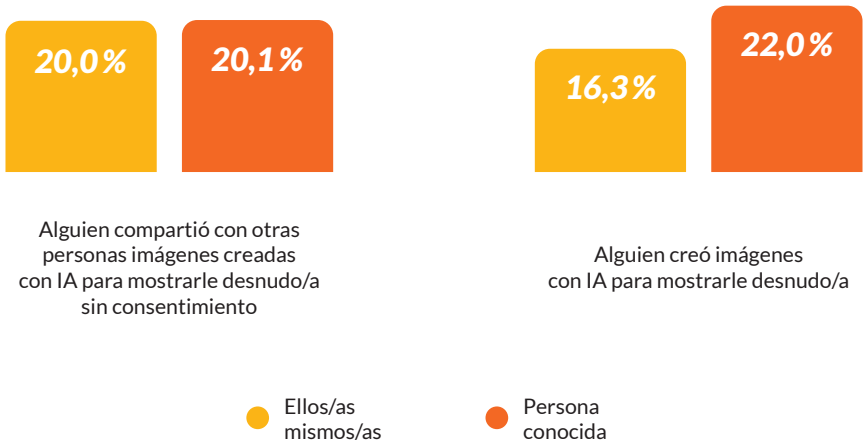
Se trata un fenómeno en crecimiento: en 2024, CyberTipline del NCMEC recibió 67.000 denuncias relacionadas con CSAM generado por IA, lo que supone un aumento del 1325 % respecto al año anterior, en el que se recibieron 4700 denuncias.

Al preguntarle a los chicos y chicas que han participado en este estudio, un 20 % reveló que alguien había compartido con otras personas imágenes creadas con IA para mostrarle desnudo, siendo menor de edad, y sin consentimiento, aproximadamente el mismo número reportaron conocer a alguien de su entorno a quien también le había sucedido. Las chicas experimentaron esta forma de victimización en mayor medida que los chicos: cerca del 21 % frente al 18 %.

Estos datos reflejan cómo la inteligencia artificial se está incorporando a dinámicas ya existentes de violencia sexual digital que afectan a la infancia y a la adolescencia. En contraste, resulta llamativo que cerca del 70 % de los y las jóvenes no señalara como un riesgo percibido durante su infancia la manipulación de fotos o vídeos mediante inteligencia artificial, lo que puede apuntar a la necesidad de seguir concienciando sobre este riesgo y sus consecuencias. Por otro lado, en los talleres con adolescentes, al abordar los riesgos y preocupaciones en el entorno digital, las chicas manifestaron una mayor preocupación por ver su imagen sexualizada mediante la inteligencia artificial, incluso si el contenido original no era sexual.

9 Internet Watch Foundation (2023). How AI is being abused to create child sexual abuse imagery.

Figura 2. ***Creación y difusión de imágenes creadas con IA.***



«Puede que utilicen mi cara con IA para cualquier cosa».

—Chica adolescente

El riesgo del sharenting

Cada vez más familias comparten en redes sociales imágenes de sus hijos e hijas desde edades muy tempranas, en muchos casos sin imaginar los riesgos en los que puede derivar. Esta práctica, conocida como *sharenting*, puede parecer inofensiva, pero conlleva una exposición digital de los niños y niñas que inevitablemente escapa de nuestro control. Aun cuando las imágenes no tengan ningún tipo de connotación sexual y se compartan sin mala intención, éstas pueden ser igualmente descargadas o manipuladas sin nuestro consentimiento (e incluso sin nuestro conocimiento) por parte de terceros con intenciones ilícitas. En los casos más graves, pueden utilizarse para generar CSAM digitalmente, a partir de fotografías reales y cotidianas.

Según INCIBE, el 81 % de los bebés tiene presencia en Internet con apenas seis meses de vida.[10] Es necesario, por tanto, visibilizar y concienciar sobre este riesgo, promoviendo prácticas más conscientes y seguras en el entorno digital, también por parte de las familias, para preservar la privacidad, la seguridad y el bienestar de los niños, niñas y adolescentes.

«Un riesgo muy grande es el contenido que subimos y la poca importancia que le damos a quienes lo ven».

—Chica adolescente

- **Materiales autogenerados**

Las imágenes o vídeos también pueden estar producidos por los propios niños, niñas y adolescentes, mostrándose en posiciones «sugerentes» o sexualizadas, o en conductas más explícitas, de manera voluntaria o bajo coacción, en contextos que pueden ir desde la intimidad y la curiosidad sexual hasta la presión social o la manipulación y explotación por parte de terceros.

Una de las formas de generación de este contenido es a través de la práctica del *sexting*, referida al intercambio de material sexualmente explícito a través de las tecnologías, incluyendo imágenes, vídeos o textos de carácter sexual. Se trata de una práctica consolidada entre los y las adolescentes,[11] como también evidencian los datos del muestreo: un 27,1 % de los chicos y chicas enviaron mensajes, fotos o vídeos íntimos o sexuales suyos voluntariamente durante la infancia o adolescencia, y el 40,2 % refirieron conocer a alguien que lo había hecho.

Desde una perspectiva de derechos de la infancia, es esencial abordar estos casos autogenerados con cautela, reconociendo que las dinámicas de poder, la presión social y la falta de información pueden poner en riesgo el consentimiento y la protección de los chicos y chicas. Incluso cuando puedan ser consideradas voluntarias, estas conductas plantean riesgos, pues como sucede siempre en el entorno digital, una vez compartido el contenido escapa al control de quien lo genera, abriendo la

10 Instituto Nacional de Ciberseguridad (INCIBE) (s.f.). *Sharenting:* cuando los padres ponen en riesgo la imagen de sus hijos. INCIBE.

11 Gámez Guadix, M., de Santisteban, P., & Resett, S. A. (2017). Sexting among Spanish adolescents: Prevalence and personality profiles. Psicothema, 29(1), 29.34.

puerta a múltiples formas de victimización. Los materiales producidos pueden ser redistribuidos sin consentimiento, utilizados por personas adultas con fines sexuales, utilizados para la sextorsión, o terminar circulando en entornos donde pueden ser explotados por agresores sexuales, constituyendo así una forma de abuso y explotación sexual. Destaca que, en nuestra encuesta, el 100 % de quienes dijeron haber sido víctimas de explotación sexual[12] afirmaron conocer qué era el *sexting*, frente al 60 % de quienes no habían sido víctimas.

> ***«Este tipo de imágenes parten de la sed de aprobación social y la tendencia en esa edad a asumir riesgos. Si a eso le sumas la curiosidad, el despertar sexual y una capacidad de autocontrol limitada, tenemos el escenario perfecto para los agresores».*** —Profesional del ámbito de la psicología y la criminología

Preocupa además que estos materiales estén pasando a formar parte del conjunto de contenido de abuso y explotación sexual infantil que circula en la red, incluso cuando se generan en contextos inicialmente privados, voluntarios o no delictivos. Al respecto, la IWF ha alertado que, de las 275.652 páginas web analizadas que contenían CSAM en 2023, el 92 % incluía imágenes autogeneradas, y el 70 % de estas correspondían a niños y niñas de entre 7 y 10 años.[13] Estos datos reflejan tanto la temprana edad de inicio en la producción de este tipo de contenidos como la alta vulnerabilidad de quienes los generan, muchas veces en contextos de escasa supervisión adulta, búsqueda de aprobación o carencias afectivas.

A pesar de ello, llama la atención que la mayoría de chicos y chicas no perciban como un riesgo el envío consentido de este tipo de material. De hecho, son aún menos quienes identifican estas conductas como de riesgo cuando el envío se dirige a una persona adulta. También preocupa que más del 65 % no perciban como un riesgo el envío o reenvío de imágenes sin el consentimiento de la persona menor de edad representada en ellas.

> ***«Que expongan contenido delicado en otra red social que no sea la mía y sin mi autorización y la utilicen para sexualizar mi imagen de cualquier manera y que circulen por ahí».***
> —Chica adolescente

12 Alguien me dio dinero, alcohol o drogas, o me hizo algún regalo o favor para ver fotografías, vídeos míos o transmisiones en directo sin ropa, de contenido erótico o sexual.

13 Internet Watch Foundation (IWF). Annual Report 2023. 'Self-generated' child sexual abuse.

Tabla 1. ***Riesgos percibidos en el entorno digital en relación con el envío de contenido íntimo.***[14]

	%
Envío consentido de fotos o vídeos íntimos a otros adolescentes	41,3 %
Envío consentido de fotos o vídeos íntimos a personas adultas	32,9 %
Envío o reenvío de fotos o vídeos íntimos sin el consentimiento del menor	34,7 %

En los talleres, se vieron algunas diferencias entre chicas y chicos respecto a la percepción del riesgo la difusión de imágenes íntimas: las chicas consideran que las consecuencias son más graves para ellas, considerando que los chicos podrían recibir validación social si se compartiesen esas imágenes, y que, además, ellos comparten más contenidos de terceras personas sin pensar las consecuencias. Por su parte, a los chicos creen que es algo a lo que ellas están más expuestas.

En cuanto a los motivos que podrían llevar a una persona menor de edad a compartir imágenes o vídeos íntimos o sexuales de sí mismos, los más señalados fueron no saber que puede ser peligroso (48 %), creer que es algo normal o que no tiene consecuencias negativas (46,3 %), la búsqueda de atención, afecto o validación (42,5 %), o la expectativa de una ganancia a cambio (40,4 %). Este último motivo se vincula de forma más clara con dinámicas de explotación o autoexposición, al implicar una lógica de intercambio.

«Estamos viendo mucho material online autogenerado o prácticas relacionadas con el sexting, que no es una forma de victimización, pero ese material termina circulando por la red o es utilizado para extorsionar y que los NNA sigan produciendo este tipo de materiales o incluso para mantener una relación sexual física».

—Experta en explotación sexual

14 Independientemente de que te pasaran a ti o no, ¿cuáles crees que fueron los riesgos a los que tú y tus amigos y amigas os enfrentasteis en el entorno digital antes de cumplir los 18 años?

Tabla 2. ***Motivos para el intercambio de contenidos sexuales en Internet siendo menor de edad.***

	%
No saber que puede ser peligroso	48,0 %
Presión de alguien más (chantaje, manipulación o engaño)	38,4 %
Expectativa de recibir dinero, regalos o favores	40,4 %
Creer que es algo normal o que no tiene consecuencias	46,3 %
Buscar atención, afecto o validación	42,5 %
Para impresionar o encajar con sus amistades	39,5 %
Como muestra de amor o confianza en una relación de pareja	37,9 %
Influencia de redes sociales o de personas famosas	32,1 %
Por curiosidad o exploración de su identidad	25,1 %

Tipificación penal de las conductas relacionadas con la producción y consumo de material de abuso sexual

Las imágenes de abuso sexual infantil (CSAM) constituyen delitos graves tipificados tanto en la legislación europea como en la española. El artículo 189 del Código Penal recoge formas de explotación sexual vinculadas a espectáculos pornográficos y a la elaboración de material pornográfico, siguiendo en gran medida los criterios de la Directiva Europea y del Convenio del Consejo de Europa sobre Ciberdelincuencia, aunque sin aludir expresamente al material gris o CSEM.

Este artículo no solo penaliza a quienes organizan o se lucran de estas prácticas, sino también a quienes las consumen, toleran o permiten.

En este sentido, en el ámbito de los espectáculos exhibicionistas y el CSAM,[15] se introducen sanciones específicas dirigidas al «cliente» entendido como público receptor, tanto en el plano físico como digital. Estas medidas reconocen que la demanda de este tipo de contenidos constituye, en sí misma, una forma de alimentar las dinámicas de explotación, y actúan sobre la base de proteger no solo a la víctima concreta sino a la infancia y la adolescencia como colectivo.

El Código Penal también incluye en el CSAM las representaciones realistas de menores en actos sexuales, o de sus órganos sexuales con fines sexuales. Además, el Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, actualmente en tramitación, amplía esta protección, incorporando un nuevo tipo penal (art. 173 bis) que sanciona las ultrafalsificaciones, reforzando la protección frente a estas conductas.

Finalmente, el *sexting* también puede tener consecuencias jurídicas incluso cuando se produce de forma voluntaria entre menores de edad, especialmente si las imágenes se comparten sin consentimiento. En estos casos, puede considerarse un delito de revelación de secretos (art. 197 del Código Penal), con agravantes si la persona afectada es menor de edad. Su difusión, incluso si la persona que lo comparte también es menor, también podría tipificarse como delito de pornografía infantil bajo el 189. De hecho, existe una categoría de materiales particularmente compleja desde el punto de vista legal: los materiales creados por menores de edad que representan a otros niños y niñas, ya que podrían ser considerados CSAM. Esto conlleva un riesgo real de judicialización de adolescentes como autores de delitos, incluso cuando también han sido víctimas de coacción, manipulación o engaño. Muchas chicas y chicos desconocen estas implicaciones legales.

3.2. Explotación a través de transmisiones en directo

El *live streaming* de abuso sexual infantil es la retransmisión en directo, a través de plataformas de *streaming*, de actos de abuso sexual cometidos contra niños y niñas, con una audiencia conectada desde cualquier parte del mundo.

Esta práctica representa uno de los fenómenos más alarmantes y complejos de la explotación sexual infantil en entornos digitales, pues a diferencia de los materia-

15 Respecto a estos delitos, el Código Penal todavía emplea el término «pornografía infantil».

les y representaciones digitales que acabamos de analizar, el *live streaming* se caracteriza por el componente de simultaneidad: el abuso ocurre en tiempo real. Esto provoca que, en muchos casos, los espectadores no se limitan a observar, sino que interactúan con el abuso en curso. A través de los chats en directo pueden dar instrucciones, hacer peticiones específicas o pagar para que se realicen ciertos actos, convirtiéndose así en coautores del abuso, participando en tiempo real, aunque no tengan contacto físico con el niño o niña.[16]

El *modus operandi* suele involucrar la participación de intermediarios o facilitadores, muchas veces familiares o personas del entorno del niño o niña, que organizan las sesiones de abuso: acuerdan con los clientes la fecha, hora y duración del *streaming*, establecen los precios (que varían según la edad y el número de niños y niñas implicados, o los actos solicitados), y proporcionan el entorno para la retransmisión.

Desde una perspectiva legal, esta modalidad puede englobar múltiples formas de violencia sexual, tales como la explotación infantil a través de la prostitución, la realización forzada de actos sexuales con o sin contacto físico, y la producción de CSAM. Sin embargo, el componente de simultaneidad supone un reto significativo en términos de detección e investigación, ya que, si la retransmisión no se graba, no queda evidencia física en el dispositivo. Incluso cuando se graba para generar CSAM, el contenido suele subirse de forma encriptada a servidores en la nube, y los enlaces se comparten de manera oculta, lo que dificulta su trazabilidad y la atribución del delito. Los pagos, además, se realizan a través de sistemas bancarios, criptomonedas u otras formas digitales de transacción, dificultando su rastreo.

> ***«La gente accede al contenido, pero el contenido no circula. Cuando el contenido no circula, no se detecta. Entonces, la investigación es mucho más complicada».***
>
> —Profesional del ámbito de justicia

El *live streaming* puede entrelazarse con conductas relacionadas con la autoexposición o sobreexposición digital, que se analizarán en un próximo informe, en las que los propios menores de edad participan activamente en conductas sexuales que son retrasmitidas, motivados por la búsqueda de validación, presión social, chantaje emocional o recompensas simbólicas, y muchas veces sin plena conciencia de las consecuencias de estos actos.

16 A nivel internacional, el *live streaming* ha sido conceptualizado también como «abuso infantil por encargo», «prostitución infantil por webcam», «abuso infantil a distancia».

Turismo sexual digitalizado

El *live streaming* ha permitido también la transformación de formas tradicionales de explotación sexual, como el turismo sexual infantil, al eliminar la necesidad del desplazamiento físico del agresor. Esta modalidad solía implicar que hombres, mayoritariamente de países occidentales, viajaran a contextos marcados por la pobreza, la desigualdad y la escasa regulación —especialmente en el Sudeste Asiático, América Latina o África— para abusar sexualmente de niños y niñas. En la actualidad, las tecnologías digitales se emplean para planificar, coordinar, visualizar e incluso facilitar estos abusos a distancia, a través de transmisiones en directo.

Esta práctica ha ganado terreno gracias a la creciente demanda de contenidos «personalizados» por parte de usuarios occidentales, que pueden acceder en tiempo real a retransmisiones de abusos. En muchos casos intervienen redes criminales que actúan como intermediarias entre familias o comunidades empobrecidas y los usuarios finales, ofreciendo servicios que incluyen la «disponibilidad a la carta» de niños y niñas para prácticas sexuales específicas durante las transmisiones en directo.[17]

Las agresiones se organizan en espacios controlados como domicilios o habitaciones alquiladas. Las víctimas suelen ser grabadas sin su consentimiento o conocimiento, difundiendo después las grabaciones en redes internacionales de distribución de CSAM, lo que genera un ciclo de revictimización constante.

A la complejidad tecnológica para la investigación y detección de estos casos, se suma el componente transnacional del delito, lo que requiere una cooperación internacional sólida y eficaz para rastrear los pagos, las direcciones IP y el entorno donde se produce la retransmisión,[18] y planea enormes desafíos para la identificación y protección de las víctimas, muchas veces en contextos de vulnerabilidad y pobreza extremas.

17 Diaconía (2024). Guía para profesionales del ámbito educativo. Trata en el mundo digital: protegiendo a los menores. Madrid: Diaconía.

18 Europol (2019). Internet Organised Crime Threat Assessment (IOCTA) 2019. The Hague: Europol.

«Depredadores que, de países occidentales, contactan principalmente con redes del sudeste asiático, que les consiguen vídeos, o sea, les consiguen menores para hacer streaming en directo con menores a la carta».

—Fuerzas y cuerpos de seguridad

La Directiva 2011/93/UE

La Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil es el instrumento jurídico clave de la Unión Europea para la armonización penal y la protección integral de niñas, niños y adolescentes frente a la violencia sexual, reforzando un enfoque centrado en la víctima, preventivo y transnacional. Este instrumento incorpora de forma explícita y transversal el entorno digital como espacio de comisión del delito, medio de explotación y objeto de regulación preventiva.

Recoge el abuso sexual (artículo 3), la explotación sexual (artículo 4), la pornografía infantil[19] (artículo 5) y el *grooming* (artículo 6). Así, la explotación sexual recoge las siguientes conductas:

- La **prostitución infantil,** definida como la utilización de un niño, niña o adolescente en actividades sexuales en las que se entregue o prometa dinero u otra forma de remuneración o contraprestación como pago por su participación en estos actos, independientemente de que el pago, la promesa o la contraprestación se entregue o se haga a la persona menor de edad o a un tercero.
- Los **espectáculos pornográficos,** entendidos como «la exhibición en directo dirigida a un público, incluso por medio de las TIC: i) de un niño, niña o adolescente participando en una conducta sexualmente explícita real o simulada, o ii) de los órganos sexuales de un niño, niña o adolescente con fines principalmente sexuales» (art. 2.e).

19 Término que emplea la Directiva, que en la nueva propuesta se actualiza.

La pornografía infantil, diferenciada de las infracciones relacionadas con la explotación sexual, se define como:

- Todo material que represente de manera visual a un niño, niña o adolescente participando en una conducta sexualmente explícita, real o simulada, y toda representación de los órganos sexuales de un menor de edad con fines principalmente sexuales.
- Todo material que represente de forma visual a una persona que parezca ser un niño, niña o adolescente participando en una conducta sexualmente explícita real o simulada o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales. Sin embargo, la propia Directiva prevé una cláusula de discrecionalidad que permite a los Estados decidir si aplicar o no sanciones en estos supuestos.
- Imágenes realistas de un niño, niña o adolescente en conductas sexualmente explícitas o imágenes realistas de sus órganos sexuales, con fines principalmente sexuales. También para este supuesto se permite la discrecionalidad en cuanto a sanciones, siempre que el material se haya creado y conservado para uso privado sin riesgo de difusión, y no incluya imágenes reales de niños y niñas.

Esta directiva está siendo revisada por las instituciones europeas, en respuesta a los cambios tecnológicos y al aumento de los delitos sexuales cometidos contra la infancia y la adolescencia en entornos digitales. Esta revisión se basa en los resultados del ejercicio de evaluación llevado a cabo en 2022, en el que se identificaron limitaciones importantes en su aplicación, particularmente en los ámbitos de la prevención, la cooperación transfronteriza, la investigación digital y la atención a las víctimas. Algunos aspectos clave de esta reforma son:

- la actualización del lenguaje, sustituyendo el término «pornografía infantil» por «material de abuso sexual infantil» (CSAM), en consonancia con las recomendaciones de organismos internacionales.
- la ampliación de la definición de delitos relacionados con el abuso sexual infantil en toda la UE, así como introducción de penas más elevadas para los autores. Entre los nuevos delitos que se incorporan se encuentran la transmisión en directo de abusos sexuales a niños, niñas y adolescentes, la posesión o intercambio de manuales conocidos como «guías pedófilas», y la inclusión del CSAM creado mediante IA.

4. Dinámicas de captación para la explotación sexual de la infancia y la adolescencia en entornos digitales

Las posibilidades tecnológicas, y el propio cambio en las dinámicas relacionales del entorno digital (¿qué es un desconocido en una red social?), también han transformado las dinámicas de captación de niñas, niños y adolescentes con fines de explotación sexual, adaptando métodos que van desde estrategias directas y agresivas hasta procesos de manipulación y embaucamiento progresivo, cada vez más sofisticados y que pueden tener diferentes objetivos. Actualmente, las estrategias más comunes incluyen el *grooming online* y la sextorsión, que por sí solas ya constituyen formas de violencia.

El *grooming*. Esta forma de violencia, analizada en estudios previos,[20] se presenta en este contexto como una de las formas más frecuentes y complejas de captación de niños, niñas y adolescentes con fines de explotación sexual. Basándose en la manipulación, el engaño y la coacción, busca obtener materiales digitales de contenido sexual (tanto para su uso personal o como para su venta), generar encuentros sexuales en el ámbito digital o en el físico, o involucrar a la niño o niña víctima en redes de explotación. El intercambio de imágenes suele iniciarse de una manera aparentemente voluntaria, aunque es habitual que derive en coacción.

En 2023, el Ministerio del Interior registró 525 denuncias por hechos relacionados con el *grooming*, lo que supone un incremento significativo respecto al año anterior (408). Sin embargo, como en otras violencias, es solo la punta del iceberg: el 33,5 % de los y las jóvenes participantes en nuestra encuesta habían tenido contacto con una persona adulta con fines sexuales en el entorno digital, siendo más las chicas (35,6 %) que los chicos (26,5 %) quienes habían tenido este contacto. Respecto a las conductas asociadas al contacto con fines sexuales, las chicas mostraron un mayor riesgo de recibir fotos o comentarios sexuales sin haberlos solicitado y de que una persona adulta contactara con ellas con fines sexuales. También las chicas adolescentes participantes en el taller reconocían que en Internet están expuestas a todo tipo de personas y que no siempre es fácil identificar perfiles falsos o con malas intenciones.

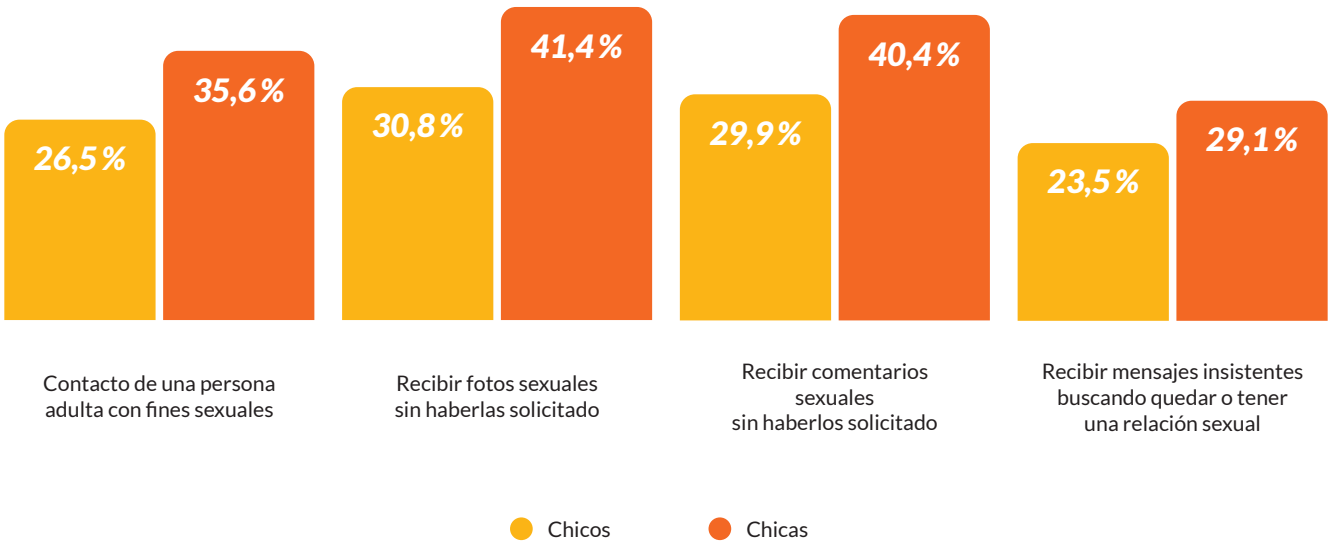
> ***«Cuando ha pasado mucho tiempo y días puede haber confianza, aunque no conozcas a la persona en persona».***
>
> —Chico adolescente

20 Véase: Derechos sin Conexión (2024); *Online grooming* (2023); y Violencia Viral (2019).

Tabla 3. ***Riesgos asociados al grooming.***[21]

Situación	Ellos mismos	Persona conocida
Contacto adulto con fines sexuales	33,5 %	35,9 %
Recibir fotos sexuales sin haberlas solicitado	38,9 %	47,9 %
Recibir comentarios sexuales sin haberlos solicitado	38,0 %	45,9 %
Recibir mensajes insistentes buscando quedar o tener una relación sexual	27,0 %	34,2 %

Figura 3. ***Conductas asociadas al grooming, por género.***



Las tecnologías permiten que, para los agresores que emplean estas tácticas (*groomers*), el contacto con víctimas pueda ser inmediato, masivo y constante, y puede producirse a través de todos los espacios en los que la infancia y adolescencia accede de forma habitual: redes sociales, plataformas de videojuegos, canales de *streaming*, aplicaciones de mensajería, etc. Los agresores adaptan sus estrategias

21 De las siguientes experiencias, ¿cuál o cuáles te pasaron a ti o a alguien que conocías? Señala tantas opciones como sean necesarias.

de contacto en función del perfil de la víctima. Por ejemplo, en función del género, utilizando los videojuegos *online* para acceder a principalmente a niños, mientras que redes como Instagram, TikTok o YouTube se usan más para contactar con niñas. En ambos casos, una vez hecho el primer contacto, se trasladan a aplicaciones de mensajería (WhatsApp, Telegram o Discord), donde hay un mayor nivel de intimidad, privacidad y riesgo.

> ***«Utilizan todo canal imaginable en la captación y contacto con NNA en las redes en abierto. Desde los foros de los videojuegos, de venta de entradas, club de fans de famosos que están en el aro de los niños, clubes deportivos que llaman la atención a los niños o de seguidores de estos...».***
>
> —Profesional del ámbito de la justicia

La encuesta confirma la variedad de vías de contacto usadas por los explotadores, destacando el contacto a través de redes sociales como Instagram (68 %) o X/Twitter (44 %), aplicaciones de mensajería como WhatsApp (48 %) o de citas como Tinder (44 %) y Grindr (48 %). Cabe tener en cuenta también el contacto también a través de juegos *online* y *streaming* (44 %).

Tabla 4. ***Plataformas de contacto de los explotadores.***[22]

Instagram	68 %	Twitch	36 %
TikTok	40 %	Snapchat	28 %
WhatsApp	48 %	Only Fans	24 %
Youtube	28 %	Tinder	44 %
Telegram	40 %	Grindr	48 %
X/Twitter	44 %	Webs de *sugar daddies* y similar	36 %
Discord	32 %	Juegos *online* y *streaming online*	44 %

22 Porcentaje sobre las víctimas de explotación sexual.

Aplicaciones para citas

Las aplicaciones de citas como Tinder, Bumble, Badoo o Grindr, están destinadas únicamente a personas que hayan cumplido los 18 años, y así lo indican en los sitios de descarga. Sin embargo, no cuentan con ningún sistema de verificación de edad que permita comprobar de manera fiable la mayoría de edad del usuario: basta con introducir una fecha de nacimiento para registrarse, y solo se solicita un documento de identidad en caso de que la propia persona usuaria indique una edad inferior a la permitida.

De este modo, en la práctica, no se dan impedimentos para que chicos y chicas adolescentes puedan acceder a estas aplicaciones: de hecho, en la encuesta hemos visto como algunos de los y las participantes utilizaron este tipo de aplicaciones antes de cumplir los 18, con una edad media de acceso entre los 15 y los 16 años. La presencia de menores de edad en estos espacios posibilita que puedan entrar en contacto con personas adultas con fines sexuales, con los riesgos que ello implica, incluyendo en relación al *grooming*, la captación con fines de explotación sexual y otras formas de violencia que pueden derivarse el intercambio de imágenes o solicitudes sexuales con personas adultas.

Es necesario por tanto que estas aplicaciones no se limiten a indicar que solo son aptas para mayores de 18 años, sino que adopten sistemas de verificación de edad que de forma efectiva permitan restringir el acceso de personas menores de edad.

Es frecuente que el agresor disponga de información íntima del niño o niña, así como de material que puede utilizar para exigir más contenido a través del chantaje o la extorsión. Por ello, otro factor clave para los agresores parece ser el nivel de exposición pública de los perfiles: el número de amistades o seguidores, la cantidad de información personal compartida o de imágenes o vídeos.[23] El análisis realizado coincide con estas conclusiones: mientras que todas las víctimas de explotación sexual digital habían compartido información personal o íntima en Internet durante su infancia o adolescencia, este porcentaje se reducía al 33,8 % para el grupo de no víctimas.

23 Europol (2019). Internet Organised Crime Threat Assessment (IOCTA) 2019.

El *grooming* suele describirse como un proceso progresivo, en el que el agresor actúa de forma planificada para crear un vínculo emocional con el niño o niña víctima antes de introducir, de manera gradual, elementos de contenido sexual. Sin embargo, actualmente se perciben algunos cambios respecto al *grooming* «tradicional»:

- Cada vez en más casos las agresiones se dan «solamente» en el entorno digital, no pasando al físico.
- **Contactos simultáneos y masivos:** aunque la mayoría se comunicaban con una sola víctima, el 12,5 % mantenía conversaciones paralelas con múltiples niñas y niños.[24] A esta capacidad de acción masiva se suma una tendencia preocupante hacia la sofisticación de las estrategias de manipulación: se detectan ataques planificados en los que los agresores, o incluso redes organizadas, recopilaban información previa sobre las víctimas, incluyendo vulnerabilidades emocionales, conflictos familiares, acoso, estado anímico o rutinas cotidianas.
- **Las peticiones sexuales llegan más rápido:** cada vez es más habitual que los agresores se «salten» la fase de creación de vínculo emocional y las peticiones sexuales se produzcan de forma inmediata. Frente a estas peticiones, es también cada vez más frecuente que los propios menores de edad respondan de manera inmediata, aceptando las solicitudes. Esta aceleración del proceso responde tanto a la hipersexualización en entornos digitales como a una normalización del intercambio de contenido íntimo, en una etapa donde la exploración sexual es clave. Esto los lleva a acceder a solicitudes incluso sabiendo que provienen de personas adultas, sin que sea necesario ese proceso previo de creación de confianza.

En este sentido, llaman la atención los datos obtenidos respecto a la percepción de los riesgos en el entorno digital: mientras que más de la mitad de los chicos y chicas (50,3 %) consideraba que uno de los principales riesgos en el entorno digital era el contacto con personas desconocidas con posibles malas intenciones, solo un 32,9 % menciona como riesgo el envío consentido de imágenes íntimas a personas adultas, riesgo que como se ha visto se percibe incluso por debajo del envío consentido de fotos o vídeos íntimos a otros adolescentes. Destaca también la falta de conocimiento sobre el *grooming*: tan solo el 23,6 % de participantes manifestó conocer lo que era, aunque al poner a prueba este conocimiento se constató que parte de este porcentaje tenía solo un conocimiento parcial de lo que implicaba este fenómeno, y solo el 17,3 % identificó correctamente todas las conductas que pueden constituir *grooming*.

24 Ministerio del Interior (2025). Investigaciones policiales por delitos de *online child sexual grooming* en España.

«Nos encontramos cada vez más con casos en los que el contacto se da a través del grooming y la agresión sexual se comete en la propia red. (...) El Tribunal Supremo ya ha dicho que no hace falta que sea offline, sino también online, porque aquí lo importante es la lesión a la libertad sexual del niño o niña. Y esto es un cambio de enfoque muy importante». —Profesional del ámbito de la justicia

El papel de la IA en las estrategias de manipulación

La inteligencia artificial desempeña un papel creciente en la sofisticación de las estrategias de los agresores. Esta tecnología les permite ocultar las habilidades lingüísticas reales de un adulto cuando se hace pasar por un menor de edad, imitando con realismo la forma de expresarse de niños y niñas, facilitando así el engaño y la manipulación. Esta tecnología también permite mantener conversaciones simultáneas y realistas con múltiples víctimas, además de generar imágenes falsas que facilitan que puedan presentarse como niños, niñas o adolescentes.

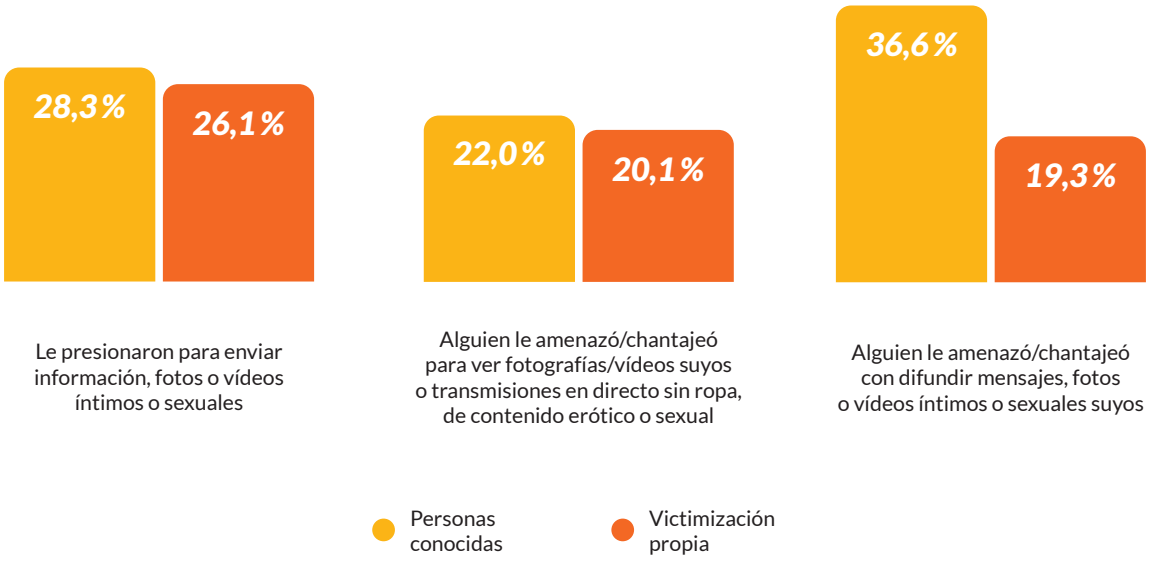
Técnicas agresivas o coercitivas. Frente al intercambio de material aparentemente voluntario que se da en el *grooming*, hay casos en los que los agresores recurren desde el inicio a técnicas más agresivas para obtener imágenes, como el hackeo o acceso no autorizado a dispositivos, o mediante el uso de *malware*, que permite activar cámaras o robar archivos sin el conocimiento de la persona usuaria. El chantaje posterior suele ocurrir en espacios digitales con comunicación en tiempo real, como Discord, chats de videojuegos o grupos privados de mensajería.

«Yo no me llevo el móvil al baño cuando voy a ducharme, no sabes si te han puesto parches desde cualquier web o un juego o han podido hacer alguna cosa». —Chico adolescente

Además, se han reportado casos de adolescentes captadas mediante falsas ofertas laborales, particularmente en sectores como el modelaje o imagen de marcas, donde se solicita el envío de imágenes, que posteriormente serán utilizadas como chantaje sexual o económico.

«Los agresores manipulan a los NNA ofreciéndoles algo de su interés, como enlaces o plugins aparentemente inofensivos, que en realidad contienen software malicioso para espiarlos o extorsionarlos». —Experta en ciberseguridad

Figura 4. ***Amenazas y chantajes para el envío de contenido íntimo o sexual.***



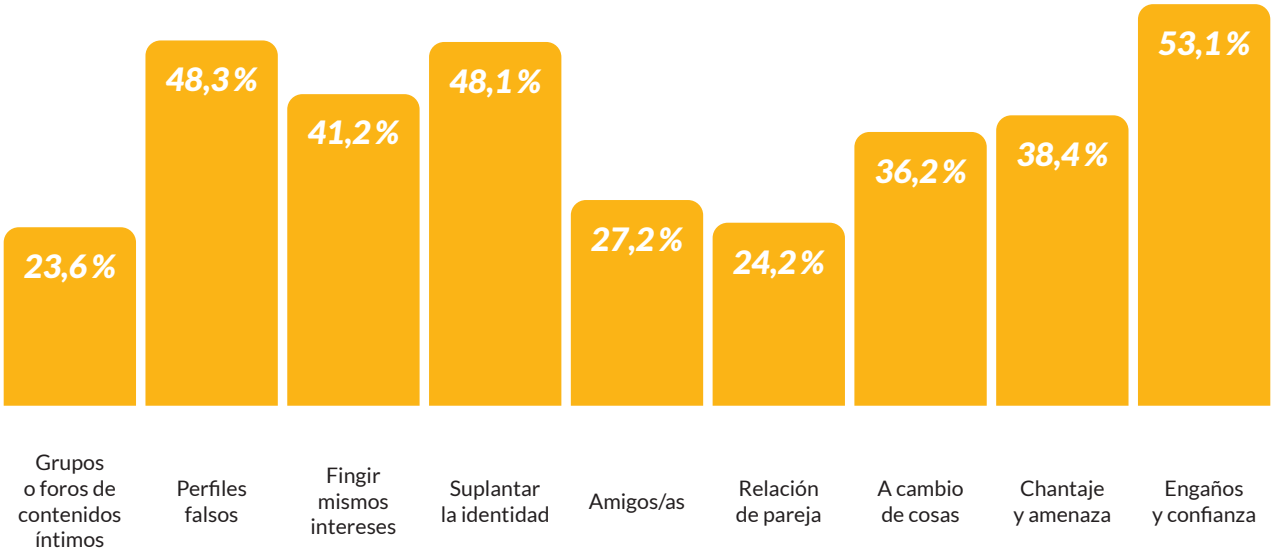
Gran parte de los y las jóvenes encuestados respondieron haber padecido durante la infancia y la adolescencia situaciones que se pueden vincular como formas de coerción o sextorsión en entornos digitales: un 26 % indicó que, siendo menores de edad, fueron presionados para enviar contenido íntimo o sexual; un 20 % sufrió amenazas o chantajes para mostrar contenido erótico o sexual; y casi el mismo porcentaje fue amenazado o chantajeado con la difusión de materiales de contenido sexual en los que aparecían. Las chicas reportaron con mayor frecuencia haber sido presionadas para enviar este tipo de contenido: un 28,5 %, en comparación con un 18,4 % de los chicos, lo que supone una diferencia de más de 10 puntos porcen-

tuales. Además, los y las jóvenes respondieron en porcentajes más elevados haber conocido a alguien que había vivido alguna de estas situaciones.

Del mismo modo, al preguntarles directamente por el motivo para el intercambio de contenidos sexuales en Internet siendo menor de edad, un 38,4 % lo relacionó con situaciones de presión por parte de otra persona, chantaje, manipulación o engaño.

Sin embargo, cuando se les pregunta por sus creencias y percepciones sobre formas de captación en el entorno digital, tienden a señalar con mayor frecuencia los métodos relacionados con la manipulación y el engaño, los perfiles falsos o fingir intereses comunes, bastante por encima de los chantajes y amenazas. Tan solo el 23,6 % señalaron los grupos o foros de contenidos. Destacan también las menores tasas de respuesta para los amigos y amigas y las relaciones de pareja, lo que puede apuntar a una menor percepción del riesgo dentro de los vínculos afectivos.

Figura 5. ***Creencias respecto a métodos de captación y acceso a víctimas.***



Abuso en el entorno cercano para la producción de CSAM. Aunque las formas de captación analizadas hasta ahora implican contacto a través de entornos digitales, existen otras dinámicas especialmente graves que suelen comenzar en el entorno cercano del niño o niña, en las que la violencia sexual presencial se combina con el uso de tecnologías para la producción, registro y difusión del abuso.

Por ejemplo, cuando el CSAM incluye contacto físico, su producción implica necesariamente una agresión sexual física al niño, niña o adolescente, que es registrada en formato audiovisual con el objetivo de ser visualizada, distribuida o intercambiada en entornos digitales. En algunos casos, este proceso de captación y abuso puede estar precedido por una fase de *grooming* o por dinámicas de coacción ejercidas por personas desconocidas. Sin embargo, los datos disponibles y las observaciones de agentes clave coinciden en que lo más habitual es que la agresión provenga del propio entorno del niño o niña víctima: familiares, cuidadores u otras figuras de referencia con acceso cotidiano y relaciones de confianza, que aprovechan su cercanía y posición de poder para victimizar al niño o niña y ejercer control sostenido. Las tecnologías digitales, como cámaras domésticas, móviles, o aplicaciones de mensajería, se convierten en herramientas para la producción y distribución del abuso.

Una característica especialmente alarmante de este fenómeno es la identificación reiterada de víctimas de edades extremadamente tempranas, incluso lactantes y niñas y niños menores de 3 años, en el CSAM.[25] Este grupo representa una franja de máxima vulnerabilidad y de mayor gravedad en el nivel de violencia y daño infligido. En estos casos, el agresor suele ser un adulto del entorno familiar directo, lo que implica situaciones de abuso sexual sostenidas en el tiempo.

> ***«Son personas de su círculo con ese tipo de impulsos sexuales que además ofrece un material que es inédito y muy valorado. Produce y distribuye porque alimenta su ego de ser reconocido».*** —Fuerzas y cuerpos de seguridad

Captación para la explotación en contextos trasnacionales. Este modelo de explotación se articula a través de redes organizadas que operan como intermediarias a nivel local, principalmente en regiones con alta desigualdad y debilidad institucional, captando a niños, niñas y adolescentes en situaciones de extrema vulnerabilidad (pobreza, falta de protección parental, exclusión educativa) y los someten a formas de abuso a cambio de compensaciones económicas para sus familias o cuidadores.

La captación puede producirse por vía presencial a través de redes comunitarias, vecinos o incluso familiares que actúan como reclutadores, y también puede darse mediante contacto digital directo. En este segundo caso, las familias pueden ser convencidas con promesas de oportunidades, regalos o dinero, o engañadas para que crean que sus hijos o hijas van a participar en actividades legítimas, como el modelaje o entretenimiento.

25 Interpol. Base de Datos Internacional sobre Explotación Sexual de Niños.

5. El perfil de los groomers y explotadores

El análisis de los perfiles de *groomers* y de explotadores de niños y niñas en entornos digitales revela que no existe un perfil único, aunque sí se han identificado algunos patrones comunes. Se destaca además que, en muchos casos, puede verse que diferentes personas participan en distintas fases del proceso, formando lo que algunas expertas han denominado como una cadena de explotación sexual infantil.

- **La mayoría son hombres:** En 2023, el 93,4 % de los detenidos e investigados por delitos de *grooming* en 2023 España fueron hombres, según datos del Ministerio del Interior.[26] Diversos estudios coinciden en señalar la prevalencia mayoritaria de hombres, también en el contexto nacional.

- **Se trata de personas jóvenes:** La franja de edad más común fue de 18 a 25 años, aunque la edad media de los agresores identificados en atestados policiales se sitúa en torno a los 28 años,[27] y se destaca que un 13,2 % eran menores de edad. En otros estudios, el perfil más común identificado es el de un hombre de nacionalidad española de unos 35 años.[28]

- **Pueden actuar solo en el entorno digital:** A nivel nacional, análisis oficiales indican que el 66 % de los agresores actuaba únicamente en el entorno digital, mientras que el 34 % buscaban encuentros presenciales.[29] En este sentido, también se ha clasificado a los agresores en función de sus objetivos: *groomers* que buscan el contacto físico para agredir sexualmente a niños y niñas; los motivados exclusivamente por interacciones digitales, como la obtención de CSAM o el cibersexo; o los mixtos o duales, que combinan ambos objetivos, dependiendo de la oportunidad y el contexto.

- **En muchos casos no ocultan su identidad:** Aproximadamente la mitad de los agresores no oculta quién es, lo que puede generar una falsa sensación de confianza o seguridad en la víctima.

- **No siempre son personas desconocidas:** El 35 % de los casos pertenece al entorno cercano del niño, niña o adolescente.[30] Del mismo modo, los resultados de la encuesta muestran que, si bien en los casos detectados de explotación sexual predominaban los adultos desconocidos, en un número significativo de situaciones el agresor era una persona conocida por la víctima, especialmente cuando la agresión la cometió otra persona menor de edad.

- **La motivación no siempre es sexual:** Existen casos de *grooming* y extorsión con fines económicos, o en los que se combina la motivación sexual con la económica, lo que evidencia perfiles más explotadores de agresores. En esta línea, la NCMEC advertía de que la coacción y/o extorsión centrada en el beneficio económico, en lugar de la gratificación sexual, era una tendencia en crecimiento vinculada a la explotación sexual digital. Esta tendencia también se está incrementando en España.

---

26 Portal Estadístico de Cibercriminalidad; Ministerio del Interior (2025).

27 Ministerio del Interior (2025). Investigaciones policiales por delitos de *online child sexual grooming* en España.

28 Riberas-Gutiérrez et al. (2023).

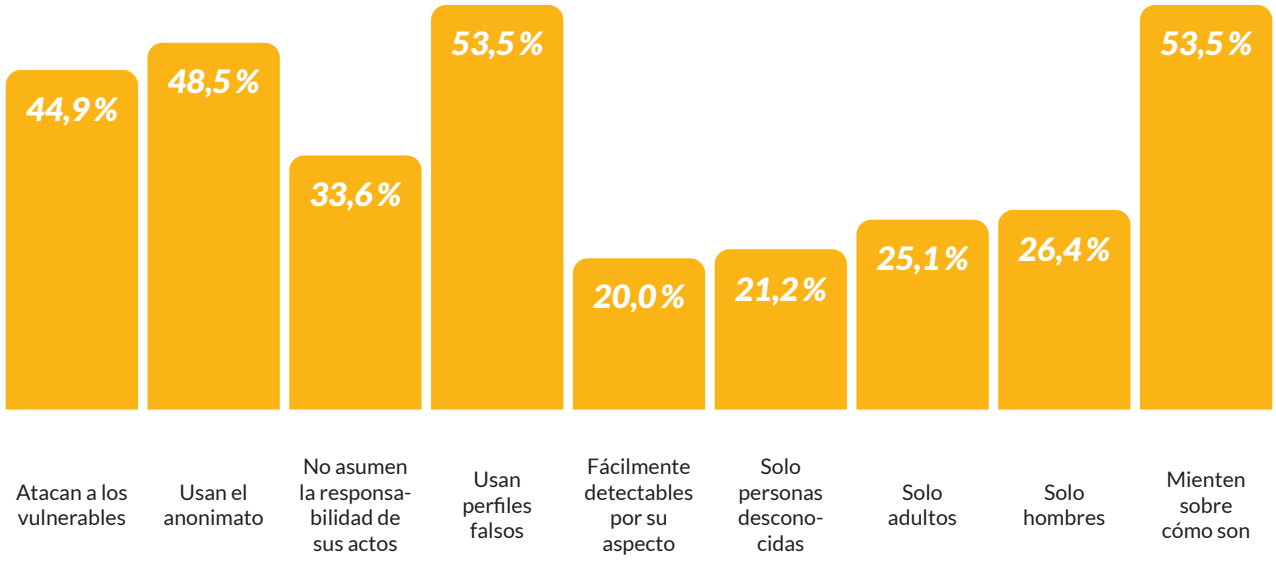
29 Ministerio del Interior (2025).

30 Riberas-Gutiérrez et al. (2023).

«En España no se detecta presencia de crimen organizado detrás de esta actividad delictiva, pero sí el intercambio económico. Va evolucionando, cada vez crece más y es posible que organizaciones criminales finalmente intenten llevarse su pedazo del pastel». —Fuerzas y cuerpos de seguridad

Algunos de estos datos contrastan con las creencias que tienen los chicos y chicas sobre los agresores en el entorno digital. Al preguntarles por su percepción sobre estos perfiles, más de la mitad pensaban que mienten sobre cómo son realmente (53,5 %), que se esconden tras perfiles falsos (53,5 %), o que usan el anonimato de Internet para comentar y amenazar (48,5 %). En cambio, tan solo el 26,2 % pensaba que los explotadores eran solo hombres. Por ello, estas respuestas ponen de relieve la importancia de trabajar la concienciación sobre la diversidad de estos perfiles, para que chicos y chicas estén alerta también ante situaciones que puedan producirse en su entorno cercano.

Figura 6. ***Imagen de los victimarios en el entorno digital.***



5.1. El perfil de los consumidores de CSAM

Consideración específica merece el consumo o visualización de material de abuso sexual infantil. El consumo de CSAM no solo constituye un delito grave y una forma

de violencia contra la infancia, sino que también se ha identificado como un factor de riesgo para la comisión de agresiones sexuales físicas. En este sentido, el informe del grupo finlandés *Protect Children*,[31] que a través de cuestionarios publicados en la *dark web* logró recoger datos de 4.549 infractores anónimos que visualizaban material ilegal en varios países, reveló que el 44 % de los encuestados que visualizaban CSAM consideró contactar con un niño o niña después de ver CSAM, y el 37 % lo hizo efectivamente.

Diversidad de perfiles. Los estudios disponibles evidencian una notable diversidad de perfiles entre los consumidores, y subrayan diferencias clave entre quienes mantienen contacto directo con niñas, niños y adolescentes y producen o difunden CSAM, y entre quienes solo visualizan este material, sin haber cometido agresiones ni haberlo producido. Este segundo grupo suele mostrar una mayor disposición al tratamiento, y algunos programas experimentales han logrado reducir tanto el consumo como la gravedad del material visionado. También se ha distinguido entre quienes buscan y visualizan material ilegal de forma delibrada y quienes buscan contenido de chicas jóvenes o infantilizadas (*teens*) sin ser conscientes de que son menores de edad.

Motivaciones para el visionado. En el proyecto *Protect Children*, un tercio de los encuestados admitió que el interés sexual en menores de edad era una de las razones principales por las que buscaban CSAM, pero destaca que más del 50 % afirmaron que no estaban buscando ese tipo de imágenes cuando las vieron por primera vez (aunque más tarde sí las buscasen de forma intencionada). Esta «exposición accidental» resulta particularmente preocupante, subrayada por el hecho de que más de dos tercios de los encuestados afirmaron haber visto por primera vez CSAM cuando aún eran menores de edad, el 40 % de los cuales tenía menos de 13 años. Otro motivo para la búsqueda de CSAM desde una edad temprana se relacionaba con situaciones de victimización propias: se buscaba este material para comprender mejor el propio abuso o situación de explotación vivida, a través de la visualización de material que representara esta vivencia.

Menores de edad. La exposición de menores de edad a estos contenidos resulta particularmente alarmante. En este sentido, las autoridades británicas ya están advirtiendo de un descenso significativo en la edad de los detenidos por abuso sexual digital, siendo cada vez más los adolescentes o preadolescentes identificados por el consumo de CSAM.[32]

---

31 Insoll, T., Ovaska, A., & Vaaranen Valkonen, N. (2021). ReDirection Survey Report: CSAM users in the dark web – Protecting children through prevention. Protect Children.

32 Grant, H. (2025, 5 de abril). «I didn't start out wanting to see kids»: Are porn algorithms feeding a generation of paedophiles – or creating one? The Guardian.

También en relación a la producción de CSAM, agentes clave señalan una preocupación creciente por la documentación de casos en los que otros menores de edad, incluso hermanos o amigos cercanos, participan activamente en la producción de este material. Los medios utilizados pueden incluir coacciones, amenazas o presiones para forzar la creación de imágenes o vídeos, así como la difusión no consentida de imágenes íntimas previamente compartidas (*sexting* sin consentimiento). También se han registrado casos en los que se graban y comparten sin permiso actos sexuales entre iguales, o incluso agresiones sexuales directas que son registradas en formato audiovisual. Estas dinámicas suelen combinar violencia, exposición digital y falta de conciencia sobre la magnitud del daño provocado.

«Tenemos siempre en la cabeza a una persona mayor de edad o que se hace pasar por un NNA. No siempre se cumple este requisito, pueden ser menores de edad. Conocemos casos de hermanos que utilizan a sus hermanos menores para la creación de este tipo de contenidos y materiales».

—Persona experta en explotación sexual

Se trata de un fenómeno que pone en evidencia la urgencia de diseñar políticas de prevención e intervención centradas en la educación y la reeducación, siempre desde un enfoque de infancia.

«El problema ha crecido exponencialmente. Hace unos años la edad media estaba en 17 años, y ahora tenemos chavales de 14, 13 e incluso 12 años».

—Experta en derechos digitales de la infancia y la adolescencia

¿Puede influir el consumo de pornografía?

La relación entre la pornografía y las diferentes formas de abuso y explotación sexual todavía es controvertida. Sin embargo, diversas investigaciones y agentes clave señalan hacia el consumo de pornografía como un elemento a considerar para el abordaje de la visualización de CSAM, especialmente el consumo temprano y/o de contenido violento.

El citado artículo de The Guardian recoge que algunos hombres detenidos por la posesión o visualización de CSAM, señalan una trayectoria hacia este material a través del consumo abusivo de la pornografía «legal» y la escalada de contenidos cada vez más extremos, facilitado por las recomendaciones y algoritmos de las páginas pornográficas.

Algunos trabajos han proporcionado evidencias que respaldan que una exposición temprana a la pornografía adulta puede ir desensibilizando y contribuir a una progresión hacia contenidos cada vez más extremos e incluso ilegales. En esta línea, en el proyecto *Protect Children*, el uso intensivo de pornografía se describe como uno de los «factores facilitadores»: reveló cómo algunas personas comenzaron viendo pornografía legal para adultos a una edad temprana, y con el tiempo empezaron a consumir material cada vez más extremo a medida que se desensibilizaban al contenido. Por otro lado, también se ha evidenciado que quienes acceden a CSAM tienden a visualizar pornografía adulta con mayor frecuencia, y a consumir contenidos más violentos, extremos o ilegales que quienes no lo hacen.[33]

Expertos del ámbito de la protección de la infancia advierten que la disponibilidad masiva de pornografía violenta que cada vez más rompe con tabúes sociales que tradicionalmente protegían a la infancia, podría estar contribuyendo a la desensibilización y escalada en algunos consumidores. En un informe previo,[34] ya se vio cómo el consumo de pornografía influye en la construcción del deseo sexual y las prácticas sexuales de los y las adolescentes, una influencia que los propios chicos y chicas reconocían, y cómo este consumo podía influir también en la percepción de la violencia, las desigualdades y las prácticas de riesgo en las relaciones sexuales.

«El consumo de este material funciona como una adicción, lo que puede llevar a una escalada en la búsqueda de contenido más extremo».

—Profesional del ámbito de la psicología y la criminología

33 Salter, M., Zajdow, R., & Salter, R. (2024). Understanding the relationship between adult pornography consumption and child sexual abuse material (CSAM) offending: A review of emerging evidence. Child Abuse & Neglect, 150, 106472.

34 Save the Children (2020). (Des)información sexual: pornografía y adolescencia.

6. Factores de riesgo

Cuando examinábamos las creencias de los chicos y chicas respecto a las personas agresoras en el entorno digital, veíamos que algo menos de la mitad (44,9 %) creía que estos perfiles atacaban solo a los «vulnerables». Pero, ¿cómo puede configurarse esa vulnerabilidad? En este apartado se analiza cómo la explotación sexual infantil digital se nutre de múltiples desigualdades y factores individuales, sociales y culturales, sin que sea posible identificar un único perfil de víctima.

6.1. Factores relacionados con el uso de las tecnologías

Uso intensivo de las tecnologías. A mayor tiempo en Internet, mayor exposición y, por consiguiente, mayor probabilidad de victimización, particularmente si no cuentan con herramientas adecuadas de protección. Al respecto, datos de Interpol indican que durante la pandemia de COVID-19 se produjo un aumento en las actividades relacionadas con el abuso y la explotación sexual infantil a través de Internet.[35]

Escasa educación digital y falta de acompañamiento. Una escasa formación en ciberseguridad, privacidad y reconocimiento de situaciones de riesgo, aumenta una falsa sensación de seguridad, que puede reducir las barreras sociales habituales, fomentar una confianza excesiva y desactivar mecanismos de alerta ante riesgos como el contacto o solicitudes de personas desconocidas. Esto, junto a una escasa educación afectivo-sexual, limita tanto la capacidad de protección como la de reconocer conductas abusivas o la autoidentificación como víctimas. En la encuesta, el conocimiento sobre qué constituye una situación de explotación sexual digital fue menor en el grupo de víctimas (36 %) que en el grupo de no víctimas (74,5 %), lo que efectivamente sugiere que la falta de información podría actuar como un factor de riesgo frente a este tipo de situaciones. Además, el 48 % de quienes enfrentaron situaciones de explotación sexual no contaron con supervisión ni interés parental respecto a su actividad digital, frente al 33,7 % de quienes no fueron víctimas de estas situaciones.

> ***«Cuanto más pequeños más riesgo, sobre todo si además no han tenido una supervisión parental o un acompañamiento en el buen uso de herramientas».***
>
> —Persona experta en explotación sexual

35 INTERPOL (2020). Riesgos y tendencias en relación con el abuso y la explotación sexual de menores: repercusiones de la COVID-19.

También se preguntó por la supervisión de las figuras cuidadoras cuando se iniciaron en el uso de su teléfono móvil propio: uno de cada tres jóvenes de la muestra señaló que sus padres o cuidadores no mostraron mucho interés o no supervisaron su actividad digital. De hecho, al analizar los datos de uso de dispositivos y supervisión de figuras adultas en el grupo de víctimas de explotación sexual, se puede ver que el 48 % de quienes enfrentaron situaciones de explotación sexual no contaron con supervisión ni interés parental respecto a su actividad digital, frente al 33,7 % del grupo no victimizado.

Privacidad negociable y falsa percepción de control. Los niños y niñas crecen en la era digital desarrollando simultáneamente una identidad física y una identidad digital, en la que la línea entre lo público y lo privado es difusa, lo que implica una forma distinta de entender la privacidad y de gestionar su exposición digital. Por un lado, las redes sociales se centran en la exposición, la validación externa y el acceso a la vida privada de otros. Por otro, la privacidad se concibe como una «moneda de cambio» en relaciones de amistad o de pareja, considerando compartir contraseñas o fotos íntimas, una prueba de confianza, compromiso o amor. Aunque reconocen la dificultad para controlar la información una vez compartida, no siempre lo identifican como riesgo, especialmente en contextos que consideran de confianza. El desconocimiento sobre las posibles consecuencias de estas conductas dificulta que niños y niñas identifiquen situaciones de riesgo o abusivas y que, cuando logran reconocerlas, los sentimientos de vergüenza, culpa o miedo a ser juzgados por haberse puesto en riesgo impidan que busquen ayuda o cuenten lo ocurrido. El temor a decepcionar a sus familias o a enfrentar burlas por parte del entorno también dificultan esta búsqueda de ayuda, particularmente en el caso de los chicos.

«No puedes controlar la imagen nunca es seguro nada».

—Chica adolescente

El análisis de la encuesta evidencia el riesgo de compartir información personal: un 35 % de los y las jóvenes encuestadas afirmó haber compartido información personal en Internet cuando aún eran menores de edad, pero destaca que, mientras que todas las víctimas de explotación sexual digital habían compartido información personal o íntima en Internet durante su infancia o adolescencia, este porcentaje se reducía al 33,8 % para el grupo de quienes no fueron víctimas.

«Los adolescentes no conciben la privacidad como algo inviolable, sino como algo negociable».

—Jurista especializada en violencias sexuales digitales

Tabla 5. ***Información personal compartida en Internet.***

	%
Mi nombre completo	25,5 %
Mi dirección	14,6 %
Números de teléfono	20,0 %
Contraseñas	14,4 %
Fotos personales	24,0 %
Vídeos personales	22,5 %
Información sobre mi familia o amigos	18,0 %
Ubicación en tiempo real o lugares que frecuentaba	19,0 %
Datos sobre mi escuela o lugar de estudio	18,5 %
Mis gustos, aficiones o rutinas diarias	24,3 %
Información financiera (como datos de tarjetas o cuentas)	13,3 %
Conversaciones privadas (mensajes, chats)	18,3 %

En este sentido, resulta fundamental repensar cómo se abordan conceptos como el consentimiento, la privacidad o la libertad en la era digital. No pueden trasladarse sin matices desde la esfera física a la digital, ni aplicarse desde una lógica adulto-centrista.

«Las nuevas generaciones han nacido con Internet, pero curiosamente caen muchísimo en la trampa. Son víctimas propiciatorias, no toman las medidas necesarias para evitar caer en este tipo de actuaciones. Hay que concienciar y educar». —Fuerzas y cuerpos de seguridad

Desinhibición en el entorno digital

El entorno digital no solo replica las conductas del mundo físico, sino que modifica en gran medida la manera en que las personas, especialmente la infancia y la adolescencia, se comportan, se expresan y se relacionan, promoviendo conductas que difícilmente adoptaríamos de forma presencial. Así lo constata el informe «Beneficios y riesgos del uso de Internet y las redes sociales»,[36] cuyos datos indican que el 60 % de los menores de 25 años reconoce actuar de forma distinta en línea que en la vida real. Esta desinhibición puede tener una dimensión positiva, favoreciendo la capacidad de autoexpresión, pero también una faceta negativa al facilitar conductas arriesgadas o incluso agresivas.

Entre algunos elementos del entorno digital relacionados con la desinhibición encontramos: el anonimato, que puede reforzar la sensación de impunidad; la distancia física y emocional, que reduce la empatía y el sentimiento de responsabilidad; la despersonalización o deshumanización, vinculada a la no percepción de otros usuarios como personas reales; y la idea de que el entorno digital «no es la vida real», lo que lleva a considerar que las normas no son tan importantes. A esto se suma la impulsividad, favorecida por la inmediatez de la comunicación, que dificulta la reflexión, y la búsqueda constante de atención y validación en redes sociales.

«Cuando voy a un instituto pregunto a una niña si una persona adulta a la que acaba de conocer hace 5 minutos le pide en ese momento una foto 'sugerente' que haría y todas responden que no lo harían, entonces les digo ¿por qué entonces es distinto si los hacen por Internet? Muchas no saben que contestar». —Fuerzas y cuerpos de seguridad

36 Observatorio Nacional de Tecnología y Sociedad (ONTSI) (2022). Beneficios y riesgos del uso de Internet y redes sociales. ONTSI.

6.2. Factores individuales

Factor de vulnerabilidad	Factores y dinámicas específicas	Riesgo	Consideraciones
Características personales	**Perfiles de apariencia más vulnerable:** necesidad de atención y afecto, baja autoestima, dificultades de socialización, escasa red de apoyo, problemas de salud mental, entornos sociales o familiares vulnerables o conflictivos.	Contacto con desconocidos, intercambio de imágenes íntimas, aceptación de encuentros presenciales.	En ambos casos, es más probable que se asuman conductas como interactuar con personas desconocidas, publicar o enviar información o fotografías íntimas, hablar sobre sexo con extraños o incluso aceptar un encuentro presencial con alguien a quien han conocido solo de forma digital.
	Perfiles sociales y extrovertidos: muestran confianza, seguridad y apertura en redes sociales, donde cuentan con una amplia lista de contactos y seguidores.	Sobreexposición en redes sociales, percepción reducida del riesgo.	
Edad	**Edades tempranas.**	Producción de CSAM por parte del entorno cercano: familiares o personas de confianza que generan y distribuyen imágenes y videos, con alto valor en redes pedófilas por ser material «inédito».	Un análisis realizado por Interpol en 2018,[37] a partir de una muestra aleatoria de imágenes y vídeos de CSAM, reveló que el 60 % de las víctimas no identificadas eran niños y niñas en etapa prepuberal. También concluyó que, cuanto menor era la edad de la víctima, mayor era la gravedad del abuso.
	Adolescencia y preadolescencia, etapas caracterizadas por la necesidad de aceptación y pertenencia, influencia del grupo de iguales, despertar de la sexualidad, la construcción de la identidad y la menor percepción del riesgo.	Facilitan conductas como el contacto con personas desconocidas, el intercambio de imágenes íntimas o la sobreexposición en redes sociales. En esta etapa también aumenta la probabilidad de recibir solicitudes sexuales no deseadas.	Los datos obtenidos en la encuesta reflejan como estas características se vinculan con las motivaciones que llevan al intercambio de contenidos sexuales en Internet: un 42,5 % señaló la búsqueda de atención afecto o validación como principal motivo; el 39,5 % indicó como razón impresionar o encajar con sus amistades; y un 25 % apuntó la curiosidad o la exploración de la identidad.

37 ECPAT International & INTERPOL (2018). Summary – Towards a global indicator on unidentified victims in child sexual exploitation material. ECPAT International.

Factor de vulnerabilidad	Factores y dinámicas específicas	Riesgo	Consideraciones
Orientación sexual e identidad de género	**Niños, niñas y adolescentes LGTBIQ+** enfrentan riesgos específicos por situaciones de discriminación, aislamiento, falta de referentes, rechazo del entorno y/o falta de aceptación social o familiar. Ausencia de información adecuada sobre diversidad sexual y de género. Búsqueda de espacios de comprensión, compañía y exploración sexual.	Exposición a dinámicas de riesgo y manipulación, establecer lazos con personas desconocidas. La búsqueda de pertenencia y comprensión puede ser instrumentalizada por adultos que se presentan como aliados o mentores, facilitando dinámicas de captación, abuso y explotación.	Las y los adolescentes LGTBIQ+ comparten imágenes íntimas más del doble que sus pares,[38] en parte como forma de explorar su identidad o buscar aceptación, pero también como resultado de presiones, chantajes o dinámicas de manipulación. Esta realidad subraya la necesidad de incorporar una perspectiva interseccional en las estrategias de prevención y protección frente a la explotación sexual infantil digital.
	Niños cisgénero homosexuales.	Constituyen uno de los subgrupos más expuestos debido a la prevalencia de varones adultos entre los agresores y a la hipersexualización de los niños gais, especialmente en el entorno digital.	Los chicos cis no heterosexuales es un subgrupo que reporta más experiencias de riesgo y una mayor tendencia a gestionar en solitario situaciones de peligro, lo que incrementa su exposición y reduce las posibilidades de intervención y protección.[39]
Carencias materiales y afectivas	Niños y niñas que viven en contextos de pobreza o precariedad.	Los agresores aprovechan las necesidades no cubiertas (alimento, ropa, techo, acceso a recursos educativos) ofreciendo gratificaciones económicas a cambio de contenido sexualizado.	Las carencias materiales y efectivas pueden tener implicaciones específicas en las dinámicas ligadas a la «autoexposición» en redes como OnlyFans o webs de *sugardating*, fenómeno que abordaremos próximamente.
	Necesidad de pertenencia emocional y social.	El escaso apoyo afectivo, situaciones de rechazo o discriminación pueden y la urgencia por sentirse aceptados puede llevarles a exponerse a situaciones de riesgo.	

38 Thorn (2022). Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2021.

39 Ibid.

«En edades muy tempranas de bebés de 3 meses a 3 años hay mucho contenido muy grave y desgarrador. También desde los 3 años hasta la preadolescencia, porque no quieren aún que tengan formado el cuerpo, y después adolescentes con el cuerpo ya formado».

—Fuerzas y cuerpos de seguridad

«Cuanta más necesidad tengas de pertenencia y cuanta más necesidad económica tengas, más vulnerable eres a este tipo de explotaciones». —Jurista especializada en violencias sexuales digitales

El impacto del género

El género condiciona los riesgos y dinámicas en la explotación sexual. Las chicas están sobrerrepresentadas en todas las formas de violencia sexual, pero es importante reconocer que los chicos también son víctimas, especialmente en el entorno digital.

En la encuesta realizada, no se encontraron diferencias estadísticamente significativas en cuanto al género de las víctimas de explotación sexual: el 2,1 % de chicos frente al 2,6 % de chicas. A nivel nacional, de las 525 víctimas de *grooming* registradas por el Ministerio del Interior, el 65,5 % eran niñas y adolescentes, pero destaca el aumento de niños y chicos adolescentes respecto a 2022, cuando las niñas representaban el 75 %. En relación al CSAM, el análisis de la Interpol[40] concluía que el 65 % de las víctimas mostradas eran niñas, el 31 % niños, y el 4 % mostraba a ambos, y que cuando se mostraba a niños, el abuso tendía a ser más grave.

Como ya se ha abordado en apartados anteriores, las estrategias de acercamiento y formas de captación también varían según el género de la víctima. En general, los niños muestran una mayor propensión a concretar encuentros presenciales, muchas veces motivados por la curiosidad o el deseo de experimentar, lo que los expone a un mayor riesgo de sufrir agresiones sexuales fuera del entorno digital.

40 ECPAT International & INTERPOL (2018).

En cambio, las niñas tienden a recibir más solicitudes de contacto y muestran una mayor disposición al envío o intercambio de contenido íntimo o sexual, sin que ello derive necesariamente en un encuentro físico.

Es importante comprender además cómo la socialización masculina tradicional impone importantes barreras para que los niños y chicos adolescentes puedan reconocer y señalar situaciones de violencia sexual. Desde edades tempranas, aprenden a reprimir sus emociones, evitar mostrarse vulnerables y no pedir ayuda, lo que refuerza la falsa creencia de que la victimización sexual es incompatible con la masculinidad. Así como las niñas tienden a normalizar determinadas situaciones de explotación sexual creyendo que forman parte de una relación afectiva, los niños pueden llegar a negar o minimizar lo vivido, impidiendo su reconocimiento como víctimas y el acceso a apoyo y reparación.[41] En este sentido, los chicos de los talleres relativizaron la gravedad del daño sexual si les ocurriera a ellos, mostrando más preocupación por las consecuencias sociales que sobre los impactos emocionales o sexuales, como posibles burlas o ridiculizaciones.

«Las chicas cuando hay un componente sexual, son más presionadas para enviar imágenes íntimas y, al mismo tiempo, más castigadas socialmente por hacerlo, reproduciendo patrones de doble moral que han existido históricamente, ahora amplificados por Internet».

—Profesional del ámbito de la psicología y la criminología

«De nosotros se burlarían y se reirían, si es una chica la llamarían guarra». —Chico adolescente

41 Pereda, N., Águila-Otero, A., Codina, M., & Cabrera, M. (2022). Guía común de actuación para la detección, notificación y derivación de casos de explotación sexual contra la infancia en centros residenciales, con especial atención a niñas y adolescentes. Delegación del Gobierno contra la Violencia de Género.

6.3. Mandatos de género

El hecho de la gran mayoría de personas que ejercen violencia sexual sean hombres, tanto en el entorno digital como fuera de él, evidencia la dimensión estructural estas violencias. Los mandatos de género y la hipersexualización, interiorizados a través de la educación, los medios de comunicación y las redes sociales, condicionan cómo se relaciona la infancia y la adolescencia, cómo se ven a sí mismos y cómo se muestran en Internet. Esto hace que muchas veces sus interacciones en redes sociales respondan a un intento de cumplir con lo que se espera de ellos y ellas socialmente en función de las expectativas de género, y no tanto a un deseo propio.

> ***«El entorno virtual, con su distancia y despersonalización, y en un contexto de por sí de hipersexualización, amplifica estas dinámicas, haciendo que muchos adolescentes participen en comportamientos que no responden a su verdadera voluntad, sino a presiones».***
>
> —Jurista especializada en violencias sexuales

Así, en Internet, y particularmente en las redes sociales, se reproducen y amplifican las lógicas del sistema patriarcal, perpetuando jerarquías, representaciones sexistas y relaciones de poder desiguales, presiones que, como se ha visto en estudios anteriores, afectan de forma diferenciada a chicos y chicas.[42] Las chicas y chicos también señalan diferencias de género en el uso de redes sociales, en concreto sobre las imágenes y los cuerpos: las chicas refieren que sus imágenes suelen ser sexualizadas por la mirada masculina, incluso si no tienen esa intención, y también visibilizan con mayor claridad la desigualdad de poder y la vulnerabilidad de personas LGTBI+. Mientras, los chicos identifican que las chicas comparten más contenido «sugerente» y perciben mayor presión sobre ellas, aunque sin profundizar tanto en el impacto emocional o reputacional.

> ***«Los chicos pueden ver una foto muy inocente y convertirla en algo sexual, creo que la mayoría de las chicas no hacen eso».*** —Chica adolescente

42 Save the Children (2024). Desinformación y discurso de odio en el entorno digital.

6.4. Sexualización infantil

La infancia cada vez está más sexualizada en los espacios digitales. Se trata de un fenómeno preocupante y cada vez más normalizado, que consiste en la adopción precoz de actitudes, expresiones o valores relacionados con la sexualidad adulta, y se manifiesta a través de la exposición del cuerpo en redes, la reproducción de gestos y estéticas sexualizadas o en la idea de que su valor personal depende de su apariencia física.

> ***«Una cosificación del cuerpo de las niñas y niños con videos en los que con 6 años se maquillan o con 12 años tienes que tener un cuerpo de 22, niños obsesionados con la imagen, con el gimnasio, etc.».***
>
> —Profesional del ámbito de la psicología y la criminología

Estos comportamientos, muchas veces aprendidos por imitación de referentes digitales o alentados por algoritmos de plataformas que premian la exposición corporal con una mayor visibilidad de los perfiles, pueden conducir a situaciones de riesgo como la captación, pues como hemos visto los agresores aprovechan la sobreexposición de imágenes autogeneradas como vía de acercamiento, chantaje o coacción. La normalización de la sexualización de la infancia contribuye además a que muchas de estas conductas sean percibidas como naturales o esperables, dificultando su cuestionamiento o detección como factores de riesgo.

> ***«Estamos imponiendo a los niños unas conductas que afectan a algo muy esencial de su desarrollo y de su evolución, que no respetan su capacidad de evolución normal».*** —Profesional del ámbito de la justicia

Factores de riesgo y comisión de conductas abusivas

Los mismos factores que incrementan la vulnerabilidad de los niños y niñas también pueden facilitar la comisión de conductas abusivas. Así, el acceso temprano no supervisado a Internet, junto con la desconexión emocional, la desinhibición digital y la exposición a contenidos inapropiados, puede distorsionar la comprensión del consentimiento y de las relaciones afectivas y sexuales. Todo ello, unido a la sensación de protección que otorga el anonimato, puede llevar a conductas violentas o delictivas, a veces sin ser plenamente conscientes del daño que causan, lo que puede generar una inversión de roles donde quienes han sido víctimas de violencia o exposición sexualizada reproducen esas conductas hacia sus pares, a veces bajo la falsa percepción de consentimiento o juego.

La creciente sexualización del entorno digital, la promoción de modelos de relaciones desiguales y el acceso a contenidos perjudiciales como la pornografía, proporcionan el caldo de cultivo para este fenómeno. Desde el ámbito de la justicia juvenil, se observa con preocupación un incremento de casos en los que los agresores son adolescentes y el canal de comisión del delito ha sido una red social, un grupo de mensajería o una plataforma de vídeo en línea. Esta violencia entre iguales plantea desafíos específicos para los sistemas de protección y justicia, que deben responder equilibradamente a la complejidad del desarrollo evolutivo, desde un enfoque reeducador y una perspectiva de infancia.

7. Consecuencias de la explotación sexual digital en la infancia y adolescencia víctima

La explotación sexual digital implica múltiples formas de violencia, que generan profundos impactos en el desarrollo integral de la infancia y adolescencia víctimas, agravados por la capacidad de difusión y permanencia que ofrece el entorno digital. Estas secuelas pueden extenderse durante años e incluso décadas, afectándoles durante la etapa adulta.

Impacto emocional	Destacan el miedo, la vergüenza, la culpa, la ansiedad o la impotencia. Pueden no llegar a entender lo ocurrido, sintiendo confusión, o racionalizarlo como algo «normal», especialmente si hubo manipulación. Autoinculpación por haber consentido o participado voluntariamente en el intercambio, que a su vez refuerza la vergüenza, el miedo a ser juzgados y el temor a que su entorno descubra lo sucedido.
Efectos en el comportamiento	Retraimiento, irritabilidad, aislamiento social, agresividad, conductas autolesivas o ideación suicida.[43] Otros efectos incluyen la disminución del rendimiento académico, el absentismo escolar y dificultades de concentración. El consumo de sustancias puede aparecer como mecanismo de evasión o para intentar gestionar el dolor emocional.
Impacto psicológico	Las consecuencias más comunes son la ansiedad generalizada, la depresión, el trastorno de estrés postraumático (TEPT), trastornos del sueño y trastornos alimentarios. Muchas víctimas experimentan conflictos con su autoimagen y autoestima, especialmente cuando si ha habido manipulación, lo que afecta al desarrollo de su identidad. Entre los efectos más severos se encuentran la disociación y el *shock* emocional. Estos síntomas tienden a cronificarse en ausencia de intervención especializada, de modo que a largo plazo pueden darse trastornos de la personalidad. Diversos estudios longitudinales han establecido una correlación significativa entre el abuso sexual infantil y conductas suicidas en la adultez, especialmente en contextos de revictimización prolongada como la explotación sexual digital.[44]
Efectos físicos	El estrés crónico derivado del trauma puede manifestarse en forma de somatizaciones, como dolores persistentes, trastornos digestivos o enfermedades autoinmunes, ampliamente documentadas en víctimas de violencia sexual.
Impacto a nivel social	Dificultades de socialización: desconfianza hacia los demás, dificultades relacionales (dependencia emocional, evitación de relaciones íntimas, miedo o incapacidad para establecer vínculos afectivos), retraimiento o aislamiento, que interfieren en el desarrollo de relaciones afectivas sanas y sostenidas.[45] La circulación de contenido íntimo puede afectar la trayectoria vital: la posibilidad de ser reconocida o expuesta en nuevos entornos (laborales, académicos o personales) genera miedo, autocensura y limitación de oportunidades.
Desarrollo sexual	Pueden aparecer disfunciones sexuales, en forma de evitación o aversión al contacto físico; hiperactividad sexual, como respuesta traumática; mayor riesgo de mantener relaciones sexuales sin protección, etc.[46] Otra consecuencia preocupante es la reproducción del abuso, ya sea como víctimas recurrentes o, en algunos casos, como agresores, en contextos donde no se ha producido una reparación emocional ni acceso a recursos de apoyo.

43 Medrano, J. L. J., López Rosales, F., & Gámez-Guadix, M. (2018). Assessing the links of sexting, cybervictimization, depression, and suicidal ideation among university students. Archives of Suicide Research, 22(1), 153–164.

44 Putnam, F. W. (2003). Ten-year research update review: Child sexual abuse. Journal of the American Academy of Child & Adolescent Psychiatry, 42(3), 269–278.

45 Hailes, H. P., Yu, R., Danese, A., & Fazel, S. (2019). Long-term outcomes of childhood sexual abuse: An umbrella review. The Lancet Psychiatry, 6(10), 830-839.

46 World Health Organization (2017). Responding to children and adolescents who have been sexually abused: WHO clinical guidelines.

La difusión digital de este abuso y explotación provocan un impacto específico y agravado: vulnerabilidad crónica y pérdida de control sobre la propia intimidad que tiene consecuencias como el miedo, la ansiedad, la disociación o incluso la negación de la propia identidad. Además, elimina la privacidad de la revelación de la experiencia de abuso, al haber sido expuesta. La permanencia y posible reaparición del material impiden el cierre emocional del proceso, lo que implica una revictimización constante.

> ***«Que sus imágenes se difundan a través de Internet que provoca primero sentimiento de vergüenza y posteriormente de sentirse vulnerable de forma constante y permanente (las imágenes son el hecho palpable de los ocurrido) que se mantiene en el tiempo».***
>
> —Experta en explotación sexual

> ***«Tiene una consecuencia mayor por la continuidad de la victimización, el material circula y no sabes quien tiene acceso por lo tanto el valor de la incertidumbre es un elemento característico. Estas víctimas siempre piensan quien estará mirando el contenido o quien lo tendrá».***
>
> —Psicóloga forense especializada en violencia sexual contra la infancia

7.1. Factores que influyen en el impacto

Estos impactos impacto pueden variar considerablemente en función de diversos factores clave:

» **La edad en el momento de la victimización:** influye decisivamente en la comprensión y el procesamiento de la violencia. Los niños y niñas más pequeños, aunque puedan no entender plenamente lo ocurrido, pueden sufrir impactos profundos en su desarrollo emocional y neurológico. Por su parte, los y las adolescentes, que atraviesan una etapa de construcción de la identidad y fuerte necesidad de aceptación social, pueden experimentar una gran angustia, culpa y miedo, especialmente ante la posible difusión de contenido íntimo.

- **La duración y gravedad de la explotación:** especialmente cuando esta es continuada o implica la circulación prolongada de material, intensifican el trauma y refuerzan en las víctimas la sensación de pérdida de control.
- **El género:** niñas y niños pueden experimentar y expresar el dolor de forma diferente, influidos por estereotipos de género. El impacto emocional de la explotación sexual es mayor en las chicas,[47] mientras que por su parte los chicos suelen enfrentar mayores barreras para verbalizar su victimización, debido a las normas sociales asociadas a la masculinidad. Estas diferencias pueden atribuirse a factores socioculturales y a los modos en que se socializa a los géneros respecto a la sexualidad y la privacidad.
- **Las características personales:** la resiliencia individual, la autoestima, las habilidades emocionales previas, la capacidad de afrontamiento o experiencias anteriores.
- **Factores sociales, culturales e institucionales:** la revictimización institucional o la falta de apoyo adecuado por parte de la familia y de los recursos disponibles puede dificultar seriamente el proceso de recuperación. En contraste, cuando la familia responde con empatía y apoyo, validando la experiencia del niño o niña y creyendo en su relato, se genera un entorno protector esencial, lo que actúa como un factor clave en la prevención de trastornos de salud mental a largo plazo, facilitando una recuperación más estable y positiva.[48] El acceso temprano y adecuado a recursos especializados es crucial para que puedan procesar lo ocurrido de forma segura y con acompañamiento profesional.

> ***«Un entorno comprensivo y sin juicios facilita su recuperación y la estigmatización agrava el daño».***
>
> —Psicóloga forense especializada en violencia sexual contra la infancia

A nivel social, sin embargo, todavía persiste una tendencia a responsabilizar a quienes padecen estas violencias, especialmente cuando han participado activamente en el intercambio de imágenes, lo que dificulta el reconocimiento de estos casos como agresiones sexuales.

En este sentido, en la encuesta se preguntó quién consideraban que era la persona responsable de las situaciones en las que una persona menor de edad vendía conte-

47 El informe de Fundación Mutua Madrileña revela que el 54,5 % de las chicas reportaron un impacto grande o muy grande ante el chantaje con la difusión de contenido íntimo, frente al 32,4 % de los chicos.

48 Ullman, S. E. (2003). Social reactions to child sexual abuse disclosures: A critical review. Journal of Child Sexual Abuse, 12(1), 89–121.

nido íntimo o sexual en Internet. Aunque la mayoría de las respuestas sitúan la responsabilidad en la persona que compra el contenido (65,9 %), las figuras parentales (62,9 %) o las plataformas digitales (60,1 %), resulta significativo que casi el 60 % de las personas encuestadas (59,5 %) atribuya también la responsabilidad al propio menor de edad, evidenciando así esta tendencia.

> ***«Son denuncias muy difíciles de tomar por la vergüenza y la sensación de consentimiento, aunque no sea válido porque es menor, pero les condiciona. Muchas veces son obligados por los padres y madres, pero hay falta de iniciativa del NNA».*** —Fuerzas y cuerpos de seguridad

A la hora de situar la responsabilidad, los chicos y chicas adolescentes diferencian en base al contexto y la intención con la que se haya producido el envío de imágenes. Así, cuando el contenido se comparte con alguien de confianza, se responsabiliza en mayor medida a quien difunde traicionando esa confianza.

> ***«Confías en la otra persona y si luego hay peleas o algo esa persona te traiciona».*** —Chico adolescente

También en los supuestos en los que hay manipulación o engaño, la responsabilidad principal la sitúan en el agresor, aunque también adjudican parte de la responsabilidad al niño o niña por haber asumido el riesgo y por haber participado en el envío. Si ha habido robo de imágenes, implica la falta de responsabilidad del menor de edad. En cambio, en los supuestos en los que consideran que hay un beneficio, adjudican una mayor responsabilidad al niño o niña que ha compartido este material.

> ***«Cuando es alguien de confianza hay traición pero si la vendes o la intercambias por unas zapatillas eres responsable porque lo haces por interés».*** —Chica adolescente

Por otro lado, consideran que el nivel de responsabilidad que puede tener el chico o chica cambia con la edad: a los 12 años, la responsabilidad recae en los progenitores; a los 16 años, consideran que ya existe un grado mayor de responsabilidad personal.

«Si envías una foto siempre tienes responsabilidad por hacerlo, aunque no conozcas todos los riesgos en el fondo de ti sabes que hay riesgo». —Chica adolescente

Vínculo traumático

En los contextos de explotación sexual infantil puede establecerse entre las víctimas y los explotadores una dinámica de vínculo traumático o coercitivo,[49] que consiste en la formación de lazos emocionales fuertes y disfuncionales hacia el agresor, especialmente en situaciones donde existe una alternancia entre el abuso, la manipulación emocional y expresiones de afecto o validación. El niño o niña víctima puede llegar a desarrollar sentimientos de dependencia, lealtad o justificación hacia el agresor, lo que dificulta que pueda reconocer la naturaleza de la explotación e identificarse como víctima, suponiendo una barrera para la denuncia y la búsqueda de ayuda.

Esta dinámica de dependencia es especialmente compleja en los entornos digitales, donde se ejerce un control constante, reforzando el vínculo mediante técnicas de *grooming*, chantaje emocional y sextorsión. Además, la utilización de recompensas emocionales o promesas de afecto refuerza la percepción distorsionada de una relación «especial», «amorosa» o «afectiva».

El vínculo traumático también puede alimentar sentimientos de culpa, vergüenza y miedo en los niños y niñas, quienes tienden a internalizar la responsabilidad de lo ocurrido porque han participado en esa relación, temiendo ser juzgadas o sufrir represalias si cuentan o revelan lo ocurrido. Todo ello dificulta la denuncia de las víctimas y perpetúa, silencia e invisibiliza la explotación digital.

49 Pereda, N., Águila-Otero, A., Codina, M., & Cabrera, M. (2022).

8. Investigación, detección y abordaje: el doble papel de las tecnologías

La creciente sofisticación tecnológica ha transformado, por un lado, las dinámicas de captación y explotación y, por el otro, las posibilidades de detección e investigación por parte de las autoridades. Las tecnologías juegan además un doble papel en este proceso, pues al tiempo que ofrece ventajas que son aprovechadas por explotadores, también plantea posibilidades y herramientas que pueden utilizarse en la investigación de estos delitos, aunque su uso aún enfrenta importantes desafíos técnicos y jurídicos, y se ha centrado principalmente en la detección de CSAM.

> ***«El volumen de datos en Internet es abrumador. Aunque el contenido ilegal representa un porcentaje muy pequeño en cifras absolutas equivale a cientos de miles de archivos diarios, lo que dificulta enormemente su rastreo (...) La colaboración constante entre instituciones, ciudadanía y empresas es fundamental para enfrentar el problema».***
>
> —Fuerzas y cuerpos de seguridad

8.1. Las nuevas tecnologías como obstáculo para detectar e investigar

Lejos de ser un fenómeno estático, la explotación sexual digital se adapta a los avances tecnológicos mediante el uso de tecnologías que buscan la protección de la privacidad y datos personales de los usuarios. Estas tecnologías tienen aplicaciones legítimas en este sentido, pero que los explotadores han aprovechado para sus propios fines, creando importantes y constantes desafíos para los operadores policiales y judiciales.

- **Encriptación y cifrado de extremo a extremo:** Aplicaciones de mensajería como WhatsApp, Telegram o Signal, emplean este tipo de cifrado para proteger la privacidad de las comunicaciones. En entornos cifrados resulta prácticamente imposible acceder a la información si no existe una denuncia previa o una investigación en curso contra usuarios específicos. De este modo, los contenidos ilegales ya no circulan por redes abiertas, donde antes podían detectarse mediante metabuscadores especializados, sino que ahora se ocultan en espacios privados, donde solo se comparten enlaces de acceso, lo que dificulta enormemente la detección de casos y la obtención de pruebas.

» **Uso de la *dark web* y de la red TOR:** Constituye una parte del Internet no indexada por motores de búsqueda tradicionales y de estructura descentralizada, diseñada deliberadamente para no ser accesible de manera convencional: requiere el uso de software específico como TOR (*The Onion Router*), que oculta la identidad del usuario. De este modo, la *dark web* se ha consolidado como uno de los espacios principales para la producción y distribución de CSAM de forma oculta y anónima, y también donde los explotadores y pedófilos también se comunican, comparten métodos y crean comunidades: en la *dark web* existen foros, *marketplaces* y canales dedicados a la distribución de este material, enfocados en nichos especialmente alarmantes, como el abuso a bebés, niños no verbales o contenido de extrema violencia y tortura.[50] También facilita el contacto anónimo con posibles víctimas para su captación y la coordinación de actos de abuso en vivo, como el *live streaming*.

«En la dark web es fácil entrar, pero difícil llegar a los foros donde se comparte material. Es imposible desanonimizar, cuando se hace es porque los fallos son suyos».

—Fuerzas y cuerpos de seguridad

Puntos ciegos para la investigación penal

La Fiscalía General del Estado[51] advierte que, al estar el cifrado cada vez más integrado en todas las capas de la comunicación digital (aplicaciones móviles, almacenamiento en la nube, dispositivos físicos) se multiplican los puntos ciegos para la acción penal. Investigaciones recientes muestran que el cifrado se usa tanto para proteger el contenido de la comunicación, como para ocultar su propia existencia.

50 EUROPOL (2019) Internet Organised Crime Threat Assessment (IOCTA).

51 Fiscalía General del Estado (2024). Memoria de la Fiscalía General del Estado. Año 2023.

Un ejemplo reciente es la Operación *Chemosh*, coordinada por Europol, donde se descubrió que grupos organizados intercambiaban material de abuso sexual infantil a través de chats encriptados utilizando stickers o emojis aparentemente inofensivos que ocultaban contenido ilícito en su interior. Este tipo de prácticas muestra el creciente grado de sofisticación en el uso del cifrado para dificultar la detección y el rastreo.[52]

Así, la investigación de delitos mediante estas tecnologías implica técnicas de análisis forense digital altamente especializadas. A nivel nacional, el uso intensivo de la *dark web* está llevando a las autoridades a desplegar técnicas de investigación más invasivas, que suponen también un desgaste y riesgo mayor, como la infiltración de agentes encubiertos en foros especializados para la recopilación de pruebas, siempre bajo control judicial estricto.

«Se ciberpatrulla en determinados chats y círculos privados que se sospecha que puede haber intercambio de material por la experiencia ya de muchos años y se va rastreando por ahí». —Fuerzas y cuerpos de seguridad

» **Almacenamiento en la nube y distribución a través de enlaces:** La «computación en nube» es un sistema que permite a los usuarios almacenar archivos y ejecutar programas en servidores remotos sin necesidad de instalarlos en dispositivos locales,[53] lo que ofrece ventajas significativas en términos de accesibilidad para diferentes servicios, como el correo electrónico o el almacenamiento de imágenes. Los explotadores han aprovechado estas ventajas para distribuir CSAM de forma segura y anónima, utilizando «casilleros cibernéticos» protegidos por contraseñas y muchas veces cifrados, cuyo acceso solo comparten mediante el intercambio de credenciales, o a cambio de otros materiales de abuso o dinero. El intercambio de enlaces en lugar de compartir directamente los archivos evita dejar rastros directos de este material en sus propios dispositivos.

52 Europol (2019). Operation Chemosh: How encrypted chat groups exchanged emoji "stickers" of child sexual abuse. Europol Newsroom.

53 ECPAT International (2020). Summary paper on online child sexual exploitation. ECPAT International.

Las empresas proveedoras de servicios en la nube, por su parte, generalmente desconocen el contenido alojado, salvo que implementen sistemas proactivos de detección. Por otro lado, el enorme flujo de información que circula en la nube dificulta todavía más la identificación de archivos ilícitos. A ello se suma que los proveedores de servicios operan en múltiples países, lo que plantea retos legales y jurisdiccionales.

«La falta de armonización legal internacional complica la persecución del delito, ya que lo que en un país es ilegal, en otro puede no serlo». —Fuerzas y cuerpos de seguridad

» **Inteligencia artificial:** La expansión de la IA representa uno de los retos emergentes más complejos en la detección e investigación de la explotación sexual infantil digital, particularmente debido a la facilidad para la creación de nuevo CSAM. Aunque para ello se necesita un volumen considerable de imágenes de la víctima desde múltiples ángulos, éstas pueden obtenerse fácilmente de las redes sociales en las que se publican, lo que aumenta el riesgo de que cualquier niño o niña pueda ser víctima potencial.[54]

La ausencia de protocolos efectivos para la detección y notificación del contenido sexualizado en algunas plataformas de IA agrava este problema, mientras que la falta de uniformidad del marco normativo a nivel internacional supone otro obstáculo. En España la creación y posesión de CSAM digital o sintético sí se considera delito, pero muchos países todavía no han legislado sobre este material, lo que permite que los delincuentes operen desde jurisdicciones «refugio» más laxas.

La existencia de este material dificulta seriamente la identificación de las víctimas reales, ya que combinan imágenes de abusos reales con contenido generado digitalmente, a menudo difíciles de distinguir. Ello puede significar que los y las investigadores inviertan tiempo y recursos en identificar a niños, niñas y adolescentes que realmente no han sido agredidos, desviando esfuerzos que afectan al rescate de víctimas reales. El crecimiento exponencial de este material incrementa estos desafíos operativos.

54 NetClean (2018). NetClean Report 2018.

«Plantea serias dificultades para distinguir entre víctimas reales y contenido generado artificialmente, y afecta el proceso de identificación y rescate de las víctimas».

—Fuerzas y cuerpos de seguridad

» ***Live streaming:*** Una de las principales dificultades tecnológicas radica en que no deja rastro digital del delito cometido: no se graba ni almacena el contenido, lo que impide obtener pruebas forenses del abuso más allá de registros de transferencia de dinero o tiempos de conexión.[55] Esto impide formular cargos por posesión de CSAM, ya que legalmente no existe archivo que lo respalde. Además, las emisiones suelen realizarse mediante plataformas protegidas por cifrado de extremo a extremo, con sistemas de pago anónimos basados en criptomonedas o remesas internacionales, lo que impide el patrullaje o la vigilancia del contenido en tiempo real y complica que las autoridades puedan intervenir de forma inmediata.[56]

Tratamiento legal del live streaming

El *live streaming* plantea vacíos normativos, pues en muchos marcos jurídicos nacionales e internacionales no está tipificado como delito autónomo, y las imputaciones penales dependen de la existencia de delitos conexos como la producción de CSAM o la prostitución infantil.[57]

En España tampoco se recoge de forma específica en el Código Penal, pero podría castigarse bajo diferentes artículos. Por ejemplo, la visualización de la retransmisión podría dar lugar a un hecho tipificable como prostitución y explotación infantil bajo el artículo 188.1 o podría ser considerado como espectáculo pornográfico recogido y castigarse la conducta bajo el 189. Si además se grabase, entonces daría lugar a un delito de posesión de CSAM, tipificado en el 189.5, y si quien visualiza además participa o interactúa, por ejemplo dando órdenes o indicaciones, se les podría imputar la agresión sexual. Por otro lado, bajo el 188.1 y el 189.1 se podría perseguir a quienes facilitasen estas retransmisiones.

55 Christensen, L. S., & Woods, J. (2024). «It's Like POOF and It's Gone»: The Live-Streaming of Child Sexual Abuse. Sexuality & Culture, 28(1), 1467–1481.

56 Napier, S., Teunissen, C., & Boxall, H. (2021). Live streaming of child sexual abuse: An analysis of offender chat logs. Trends & Issues in Crime and Criminal Justice, 639. Australian Institute of Criminology.

57 ECPAT International (2020). Summary paper on online child sexual exploitation.

» ***Deleters* y eliminación rápida de material:** Se refiere a la eliminación inmediata del CSAM tras su visualización, sin almacenarlo en sus dispositivos. En muchos casos, este comportamiento está asociado a redes de intercambio entre iguales (P2P o *peer-to-peer*), donde los agresores descargan, consumen y eliminan tanto los archivos como las plataformas empleadas para ello.

> ***«Utilizan aplicaciones con un único visionado estilo Snapchat e incluso en WhatsApp que dificulta su detección».*** —Fuerzas y cuerpos de seguridad

Esto plantea múltiples dificultades técnicas y legales: la detección y obtención de pruebas depende principalmente de que los dispositivos estén encendidos y los archivos sean todavía accesibles en memoria volátil. De lo contrario, la evidencia puede desaparecer antes de que se realice cualquier intervención policial.

Para hacer frente a este fenómeno, las estrategias de investigación deben incorporar respuestas tecnológicas más ágiles y mecanismos judiciales que permitan intervenciones rápidas. La informática forense avanzada, la detección proactiva mediante ciberpatrullaje y el uso de inteligencia artificial para identificar patrones de descarga y eliminación también se perfilan como herramientas clave.

» **Computación descentralizada:** Se trata de un tipo de red en la que no hay una autoridad central que controle todo, de modo que el procesamiento y la comunicación se reparten entre muchos ordenadores o dispositivos conectados entre sí, y que funcionan de forma autónoma, normalmente a través de *peer-to-peer*. Son modelos que se usan cada vez más en servicios como redes sociales, almacenamiento de información, intercambio de criptomonedas o sistemas de aprendizaje automático, que no dependen de un único servidor. Como no hay una autoridad central que controle estas plataformas, algunas de ellas pueden convertirse en espacios donde se comparte contenido ilegal. Aunque en algunos casos existen normas internas o moderación comunitaria, se trata de mecanismos muy irregulares y poco sólidos, que recaen generalmente en personas voluntarias, que pueden verse expuestas a un fuerte impacto emocional al enfrentarse a este tipo de contenidos.[58]

58 Spence, R., et al. (2023). The psychological impacts of content moderation on content moderators: A qualitative study. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 17(4), Article 8.

Eliminar completamente el contenido ilegal de forma rápida en estas redes es casi imposible: incluso si un grupo actúa para eliminarlo, puede seguir disponible en otros espacios donde no se tomen medidas, o no se tomen con la misma rapidez.

» **Recomendadores algorítmicos:** Las plataformas digitales utilizan sistemas de recomendación basados en IA para personalizar el contenido que se muestra a cada usuario, y que pueden generar riesgos para niños, niñas y adolescentes: por ejemplo, se ha demostrado que pueden aumentar la exposición a situaciones de riesgo como el *grooming*, contenidos sexuales o violentos.[59] Asimismo, diversas investigaciones[60] han alertado sobre cómo plataformas como Instagram o TikTok pueden facilitar el contacto entre pedófilos y posibles víctimas, a través de mecanismos de recomendación de cuentas, *hashtags* o contenido atractivos para potenciales agresores.

  Este fenómeno se conoce como *grooming* algorítmico. La falta de transparencia sobre el funcionamiento de estos sistemas dificulta su auditoría externa y la identificación de sesgos que favorezcan dinámicas explotadoras.

» **Realidad extendida:** Las tecnologías de realidad extendida (XR), que incluyen la realidad virtual (VR), la realidad aumentada (AR) y la realidad mixta (MR), fusionan el mundo físico con el digital, creando entornos muy inmersivos. A diferencia de las plataformas digitales tradicionales (en dos dimensiones), donde se pueden aplicar filtros y sistemas de moderación para imágenes, vídeos o texto, los entornos XR permiten interacciones efímeras, como conversaciones de voz o gestos corporales en tiempo real, que no siempre quedan registradas. Esta falta de trazabilidad técnica dificulta la aplicación de medidas de seguridad y plantean problemas para la detección de posibles abusos.

8.2. Posibilidades tecnológicas para la detección e investigación

» **Detección de material conocido:** Una de las herramientas tecnológicas más consolidadas para la detección de CSAM ya conocido (es decir, material que ya ha sido previamente detectado e identificado como CSAM) es el sistema de *hashing*. Esta técnica consiste en convertir imágenes o vídeos en una «huella digital» única (*hash*), que permite compararla con bases de datos de CSAM previamente identificado, sin necesidad de volver a visualizar el contenido ilegal. A pesar de su fiabilidad, esta tecnología todavía presenta limitaciones: cambios mínimos en el contenido pueden alterar el hash y dificultar su detección, lo que puede dar lugar tanto a falsos negati-

59 Véase: Stray et al. (2024) y Ofcom. (2024), en la bibliografía de este estudio.

60 Por ejemplo, los trabajos de Horowitz, J. et al (7 de junio de 2023) y de Thiel, D. et al (2023).

vos (contenido no detectado) como a falsos positivos (contenido no ilegal erróneamente identificado como tal).

» **Detección de material no conocido:** La detección de CSAM no conocido (material nuevo o inédito por no haber sido identificado o detectado previamente) plantea desafíos mucho mayores que la detección de material previamente identificado. En estos casos, no existe una «huella digital» con la que comparar las imágenes, por lo que es necesario recurrir a herramientas más complejas basadas en IA y aprendizaje automático (*machine learning*), que pueden identificar patrones visuales o textuales relacionados con el abuso.[61]

Así, los **clasificadores automáticos** son algoritmos que analizan imágenes y las agrupan según patrones que han aprendido previamente. Pueden identificar contenido sospechoso fijándose en elementos como la desnudez, el tono de piel, las proporciones del cuerpo o la presencia de niños, niñas y adolescentes. Algunas de estas herramientas son muy precisas cuando identifican una imagen como ilegal (precisión), aunque eso no significa que consigan encontrar todas las imágenes ilegales (cobertura). Cuando se analizan elevados volúmenes de datos, los desequilibrios entre precisión y cobertura plantean serias dificultades.[62]

Por otra parte, los avances en **IA predictiva** han abierto nuevas posibilidades para la detección proactiva de contenidos abusivos y para la identificación de víctimas: algunos de sus usos más útiles incluyen revisar automáticamente imágenes encontradas en registros policiales, comparar lugares que aparecen en fotos con bases de datos de casos abiertos y encontrar conexiones sospechosas entre usuarios.

«Las herramientas de IA nos ayudan a organizar material por edad, idioma o región, facilitando la identificación de víctimas». —Fuerzas y cuerpos de seguridad

61 Thorn & WeProtect Global Alliance (2024). Evolving Technologies. Horizon Scan. A review of technologies carrying notable risk and opportunity in the fight against technology-facilitated child sexual exploitation.

62 Por ejemplo, una tasa de falsos positivos del 0,1% aplicada a una plataforma con mil millones de mensajes diarios, produciría un millón de alertas erróneas al día, lo que requeriría cientos de personas para verificar manualmente los casos, una carga considerada inviable en la práctica CRIN (2022). "Explaining the technology for detecting child sexual abuse online".

Detección del grooming

El desarrollo de tecnologías de detección de *grooming* representa un desafío aún mayor, pues los comportamientos asociados a este fenómeno varían mucho entre contextos y culturas, lo que dificulta su generalización. El lenguaje utilizado por los agresores puede ser ambiguo o parecer inofensivo, lo que hace más probable que los sistemas se equivoquen, tanto al no identificar casos reales como al señalar erróneamente interacciones legítimas. Por eso, muchas plataformas están apostando por sistemas híbridos en los que la IA realiza una primera detección automática y los contenidos sospechosos son revisados posteriormente por personal humano especializado.

» **Detección de patrones de comportamiento y señales de riesgo:** La aplicación de los clasificadores y de la IA predictiva al análisis de comportamiento y la identificación de patrones anómalos constituye una de las áreas más prometedoras para anticipar situaciones de explotación sexual *online*. En lugar de buscar contenido explícito, este enfoque se centra en cómo interactúan las personas para detectar señales que puedan indicar *grooming*, coerción o intentos de captación. Algunos ejemplos de señales de alerta incluyen: adultos que interactúan mucho con menores de edad sin tener un vínculo previo; uso temprano de lenguaje sexual o manipulador; intentos de trasladar la conversación a espacios más privados o cifrados; o respuestas que muestran presión emocional, aislamiento o control. También se usa para detectar a personas reincidentes, que intentan volver a las plataformas con otras cuentas o identidades. Para ello, se utilizan tecnologías que crean una «huella digital» de cada usuario y analizan sus patrones de uso para identificar coincidencias.

  Estos sistemas son capaces de analizar tanto el texto de los mensajes como otros datos (tiempo de respuesta, la ubicación o el historial de interacciones), lo que permite generar alertas tempranas que pueden ser revisadas por moderadores humanos.[63]

» **Inteligencia artificial generativa:** Permite automatizar y optimizar tareas clave como la clasificación de material a identificar, reduciendo la exposición directa de los analistas a contenidos de abuso; la detección de

63 Thorn (2024). Youth perspectives on online safety, 2023.

manipulaciones digitales, útil para identificar CSAM sintético o digital; o la extracción de información contextual, como elementos visuales, objetos o escenarios presentes en imágenes y vídeos, que pueden facilitar la identificación y localización de víctimas y agresores.

Sin embargo, el uso de esta tecnología requiere salvaguardas específicas para evitar otros riesgos. Al respecto, varios organismos han señalado algunos principios esenciales, como prohibir el uso de material de CSAM para entrenar estos modelos, incluso cuando se trata de material modificado, anonimizado o generado artificialmente; realizar auditorías técnicas y éticas de forma periódica; incorporar mecanismos de trazabilidad como marcas de agua o etiquetas de metadatos que ayuden a identificar cuándo un contenido ha sido generado por IA; y supervisión humana efectiva.

» **Diseño seguro y verificación de edad:** La implementación de mecanismos eficaces de verificación de edad y el diseño seguro de las plataformas digitales desde su concepción (*safety by design*) es fundamental para garantizar la navegación segura de niños y niñas. Así, además de impedir el acceso a contenidos perjudiciales, la verificación de edad puede servir para ofrecer experiencias personalizadas y seguras, por ejemplo, limitando funcionalidades de contacto con personas desconocidas o estableciendo configuraciones de privacidad por defecto según la edad del usuario.

» **Moderación de contenidos en entornos cifrados y de realidad extendida:** La expansión de tecnologías digitales ha llevado a la proliferación de entornos cada vez más complejos para la moderación de contenidos, como las plataformas con cifrado de extremo a extremo o los espacios inmersivos basados en realidad virtual y aumentada. Frente a este reto, se han propuesto tecnologías como el escaneo del lado del cliente (*client-side scanning*), que analiza los contenidos antes de su cifrado y envío. Sin embargo, esta solución ha generado controversia debido al riesgo de vulnerar derechos fundamentales y abrir la puerta a prácticas de vigilancia masiva.

Otra estrategia emergente es la moderación basada en señales de comportamiento (*content-oblivious moderation*), que permite detectar patrones sospechosos, como la frecuencia de envíos o cambios en los contactos, sin acceder directamente al contenido, lo que resulta especialmente útil en sistemas cifrados.

Asimismo, se están desarrollando sistemas adaptados a los contextos de realidad extendida, que incluyen algoritmos para identificar comportamientos invasivos entre avatares, análisis en tiempo real del lenguaje verbal mediante procesamiento de lenguaje natural, o la detección de gestos o movimientos físicos relacionados con el abuso. Algunas plataformas también están introduciendo funciones de grabación y análisis forense bajo

alerta, que almacenan información como ubicación virtual o duración de la sesión, útiles en procesos de denuncia e investigación.[64]

Necesidad de equilibrio entre privacidad y protección

Uno de los debates más complejos es el que enfrenta el derecho fundamental a la protección de la infancia y la adolescencia con el derecho a la privacidad, particularmente en lo que respecta al uso de tecnologías de detección en entornos cifrados. El cifrado de extremo a extremo que utilizan las plataformas de mensajería más populares resulta clave para garantizar la confidencialidad de las comunicaciones, pero a la vez supone un obstáculo para la detección de formas de explotación. Ante este problema, algunas de las soluciones técnicas propuestas para facilitar la detección de contenidos han sido objeto de fuertes controversias, al considerar que pueden abrir la puerta a formas de vigilancia masiva, incompatibles con el Estado de Derecho.

Conscientes de este dilema, muchas de las soluciones tecnológicas propuestas han tratado de integrar desde su diseño principios de proporcionalidad, minimización y supervisión humana. Así, lejos de apostar por una lógica de «seguridad o privacidad», las iniciativas más avanzadas plantean modelos híbridos en los que se busca el equilibrio entre ambos derechos, reconociendo que tanto la protección de la infancia y la adolescencia como la privacidad en el entorno digital son pilares fundamentales en cualquier democracia. Este enfoque también está presente en las propuestas legislativas europeas más recientes, que establecen que las tecnologías a utilizar para la detección de CSAM deben ser las menos intrusivas posibles, aplicadas de forma limitada en el tiempo y sujetas a control judicial. Sin embargo, el encriptado de comunicaciones y las posibilidades de desencriptación para detectar CSAM siguen siendo discutidos en la Unión Europea. La propuesta de la Comisión para un Reglamento sobre la prevención y la lucha contra el abuso sexual infantil fue criticada por el Supervisor Europeo de Protección de Datos y por el Comité Europeo de Protección de Datos por considerar que dejaba excesivamente desprotegido el derecho al secreto de las comunicaciones,[65] de modo que la propuesta sigue debatiéndose en el Consejo de la Unión Europea.[66]

64 Para más información sobre los sistemas inmersivos y estas herramientas, véase: NSPCC (2023), Davidson et al. (2024).

65 EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse adopted on 28 July 2022.

66 Ver Anexo.

9. Recomendaciones

9.1. Fortalecimiento del conocimiento, datos e investigación sobre la explotación sexual digital de la infancia y la adolescencia

La explotación sexual de la infancia y la adolescencia en entornos digitales constituye un fenómeno complejo de violencia hacia la infancia, que agrupa múltiples dinámicas y formas de violencia interrelacionadas, y no siempre resulta sencillo distinguir algunas de estas conductas, o incluso identificarlas como formas de explotación. La falta de estudios que abarquen la explotación sexual digital de la infancia y la adolescencia tomando en cuenta todo su contexto dificulta el abordaje efectivo de este fenómeno. Así, es necesario:

- **Impulsar la producción de investigaciones periódicas y específicas sobre la explotación sexual digital de la infancia y la adolescencia en España,** con perspectiva de género, que permitan conocer su prevalencia, identificar nuevas tendencias y dinámicas, evaluar el impacto de las políticas públicas y ajustar las intervenciones preventivas, judiciales y de atención a las víctimas. A estos efectos se podría utilizar el informe de evaluación anual que ha de elaborar el órgano encargado de impulsar la estrategia para la erradicación de la violencia sobre la infancia y la adolescencia de acuerdo con el artículo 21.2 LOPIVI.
- **Poner en marcha el Registro Unificado de Violencia contra la Infancia recogido en la LOPIVI,** que contenga datos desagregados y accesibles sobre violencia sexual digital contra la infancia y adolescencia.
- **Favorecer estudios específicos de la explotación sexual centrados desde una perspectiva interseccional,** para ajustar las estrategias de prevención y protección de los niños y niñas más vulnerables frente a la explotación sexual infantil *online*.

> ***«El avance en la comprensión de la violencia sexual digital es lento, y aunque la concienciación ha mejorado, sigue siendo un área con grandes vacíos. En el plano físico se han logrado progresos, pero en la esfera digital algunos conceptos parecen haber retrocedido décadas».***
>
> —Jurista especializada en violencias sexuales digitales

- **Fomentar la investigación sobre agresores en entornos digitales, especialmente en perfiles explotadores,** para identificar características y factores de riesgo que ayuden al diseño de estrategias preventivas y mecanismos de detección.

9.2. Medidas preventivas: ámbito educativo

La exposición temprana a tecnologías digitales sin una adecuada educación en su uso seguro y responsable y sin un acompañamiento por parte de las personas cuidadores incrementa significativamente la vulnerabilidad de los niños, niñas y adolescentes. A pesar de haber nacido en la era digital, existe una brecha entre las habilidades tecnológicas y la comprensión de sus implicaciones, que lleva a una falsa sensación de control. Es necesario reconocer esta falta de preparación entre los denominados nativos digitales e invertir en programas educativos que promuevan un uso digital responsable. Algunas medidas clave son:

- **Incorporar de forma transversal en el currículo educativo la educación digital en el uso seguro y responsable de las tecnologías junto a la educación afectivo-sexual integral (reglada, desde edades tempranas, y adaptada a cada fase educativa),** atendiendo a las particularidades de la socialización y entorno digital de la infancia y adolescencia, abordando de manera adaptada a cada etapa aspectos clave como el consentimiento, la privacidad, el *sexting*, el acceso a la pornografía, la gestión de la identidad digital, presiones ejercidas en este ámbito y herramientas para establecer límites saludables en entornos digitales. Así está previsto en el artículo 7.2 LOGILS y en el artículo 45 LOPIVI y en la Observación General n.º 25 del Comité de los Derechos del Niño.[67] Los propios chicos y chicas adolescentes demandaron en los talleres fomentar el buen uso de Internet y el conocimiento de los riesgos y consecuencias de determinados comportamientos, así como extender esta formación a progenitores y a otras personas de su entorno, incluyendo contenidos en educación sexual digital.

- **Formar a los y las profesionales del sector educativo es fundamental,** incorporando elementos específicos relacionados con las dinámicas que facilitan la explotación sexual. Las formaciones deben incluir asimismo el refuerzo del deber de notificación frente a cualquier sospecha de estas formas de violencia.

- **Implementar de forma efectiva en todos los centros escolares la figura de la coordinación de bienestar,** contemplada en la LOPIVI. La formación de esta

67 Comité de los Derechos del Niño: Observación General núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital, CRC/C/GC/25.

figura debe incluir necesariamente las violencias sexuales en los entornos digitales.

Prevención desde una mirada adolescente

Cualquier actuación con la infancia y la adolescencia, incluyendo el diseño de contenidos educativos, debe abordarse desde un enfoque de participación infantil, entendiendo que lo digital está intrínsecamente ligado al modo en el que los y las adolescentes, socializan, y descubren y exploran su sexualidad. Así, las estrategias preventivas deben prescindir del enfoque moralizante y adultocentrista, e incidir en educar en el uso responsable, en los riesgos del entorno digital, en la protección de la privacidad y en el consentimiento informado. El modo en el que los y las adolescentes establecen relaciones y viven su sexualidad debe tomarse en consideración para la elaboración de las respuestas de prevención, sensibilización y acompañamiento.

9.3. Medidas de concienciación y sensibilización

A pesar de su gravedad, el conocimiento y la comprensión de este fenómeno a nivel social todavía es limitada. En general, se tiende a subestimar las implicaciones que pueden resultar de la violencia digital, y todavía existe una tendencia a culpabilizar a los niños y niñas víctimas cuando se considera que son responsables de haberse puesto en una situación de riesgo, o incluso porque se cree que han consentido. Por ello, la lucha frente a la explotación sexual infantil y adolescente en entornos digitales debe incluir campañas y acciones de sensibilización y concienciación:

- **Campañas dirigidas a niños, niñas y adolescentes,** para concienciar sobre riesgos asociados a la explotación en el entorno digital y actuar frente a la normalización de determinadas conductas de riesgo, como el contacto con personas desconocidas, el *sexting* o la importancia de proteger la privacidad en el entorno digital, acompañadas de la elaboración de materiales **y guías específicas que otorguen herramientas concretas** que los niños, niñas y adolescentes puedan utilizar para protegerse en entornos digitales.
- **Campañas dirigidas a familias y personas cuidadoras** para concienciar sobre los riesgos reales que asumen tanto los niños y niñas como las propias familias

al subir imágenes a Internet, y cómo pueden ser usadas por terceras personas para fines no deseados.

- **Campañas dirigidas al conjunto de la sociedad:** concienciar y abordar sobre los riesgos de la sexualización de niños, niñas y adolescentes, y de formas de explotación sexual digital. De forma general, sigue siendo necesario concienciar sobre el impacto de las violencias en el entorno digital en niños, niñas y adolescentes.

9.4. Medidas de atención, acompañamiento y reparación

Cuando la prevención falla, es necesario asegurar un respuesta integral y efectiva centrada en la recuperación de los niños, niñas y adolescentes víctimas. Se debe:

- **Garantizar servicios integrales y especializados de atención a la infancia y adolescencia víctima,** que incluyan desde canales de denuncia confidenciales hasta acompañamiento psicológico y jurídico. Estos recursos deben estar integrados en los sistemas públicos de protección a la infancia y adolescencia, ser accesibles territorialmente y contar con un enfoque de derechos de infancia.
- **Es imprescindible que estas respuestas tengan en cuenta las particularidades de la violencia sexual digital.** Esto requiere de la formación específica de los servicios de atención psicológicos, sociales, educativos y sanitarios; protocolos de actuación adaptados por edades y género; medidas de acompañamiento a medio y largo plazo; y desarrollo de marcos de actuación centrados en la víctima, con proyectos piloto, evaluación del impacto y revisión continua de las intervenciones.

> ***«Los recursos de atención a víctimas de violencia sexual infantil tienen una base sólida en intervención, pero carecen de conocimientos sobre el ciberespacio y su impacto en la salud mental y el desarrollo neurológico de los NNA».***
>
> —Profesional del ámbito de la psicología y la criminología

Respuestas adaptadas a la violencia digital

Teniendo en cuenta los múltiples factores que influyen sobre la vulnerabilidad y el impacto de la explotación sexual digital, es necesario diseñar e implementar intervenciones específicas que contemplen esta violencia en este contexto particular. Estas intervenciones no tienen por qué coincidir con las utilizadas en casos de violencia sexual tradicional pues, aunque comparten muchas necesidades, es indispensable reconocer sus elementos diferenciadores: permanencia del daño, pérdida de control de la imagen, y el componente tecnológico como medio de agresión.

- **Diseñar e implementar modelos de atención y acompañamiento especializados** para niños, niñas y adolescentes que lleven a cabo conductas relacionadas con la explotación sexual digital, incluyendo:
  - » Dinámicas de coacción o manipulación de otros menores de edad.
  - » La creación de CSAM.
  - » Envío de imágenes sin consentimiento.

  Estas actuaciones deben partir de un enfoque de infancia y un abordaje educativo, restaurativo, que aborde la responsabilidad por el daño causado con procesos de reeducación y acompañamiento terapéutico. Las evidencias de programas existentes muestran la necesidad de combinar enfoques individualizados con el trabajo con las familias y el entorno, además del trabajo en grupo, adaptando las terapias a la edad, al desarrollo y al tipo de conducta identificada.

  Entre los elementos que deben abordarse, se destaca: la empatía, la comprensión del daño causado, el desarrollo de habilidades de autocontrol y gestión de las emociones, estrategias de comportamientos alternativos, y la gestión riesgos entornos digitales.

- **Deben diseñarse actuaciones específicas que aborden visualización de CSAM durante la adolescencia,** sin haber participado activamente en agresiones, basadas en la evidencia generada por programas existentes y considerar enfoques innovadores como las terapias anónimas, gratuitas y confidenciales

realizadas de forma telemática (chats interactivos), que han demostrado ser eficaces en el trabajo con estos perfiles de bajo riesgo. El abordaje combinado desde una perspectiva de infancia, salud mental, educación afectivo-sexual, trabajo individualizado y apoyo terapéutico también es clave.

Además, se destaca la **necesidad de actuar de forma preventiva** respecto a estas conductas y no únicamente de manera reactiva cuando ya se ha detectado la violencia o la conducta de riesgo. Para ello, resulta vital **fomentar investigaciones centradas en la identificación y comprensión de los factores subyacentes a estas dinámicas,** que generen evidencias, y en particular su relación con el consumo impulsivo de pornografía.

Programas de intervención para consumidores de CSAM

Existen programas pioneros de actuación y atención directa destinados a consumidores de CSAM que no han cometido agresiones sexuales, que están arrojando resultados positivos. Por ejemplo, el proyecto europeo STOP-CSAM,[68] financiado por la Comisión Europea, ofrece terapia anónima *online* a consumidores de CSAM, con el objetivo de prevenir la violencia sexual contra la infancia y la adolescencia. Entre 2023 y 2024, más de 2.000 personas fueron evaluadas y unas 400 participaron en sesiones terapéuticas a través de medios digitales. Los resultados son prometedores: el 80 % de los participantes redujo el consumo o la gravedad del contenido visualizado, y más del 50 % dejó de consumirlo por completo. La mayoría eran hombres jóvenes entre 18 y 30 años, con estudios superiores. El equipo implicado en este proyecto pionero señala que el acceso a un recurso de atención terapéutica anónima actúa como elemento motivador para personas que consumen y buscan ayuda sin haber sido detectados.

A nivel nacional, se lleva a cabo el programa «Fuera de la Red»,[69] que consiste en tratamiento terapéutico específico, en el ámbito de las penas y medidas alternativas, para personas condenadas por delitos de posesión o difusión CSAM en el entorno digital, que persigue disminuir el riesgo de reincidencia.

68 Ver ***comunicado.***

69 Fuera de la Red: ***Programa de Intervención frente a la delincuencia sexual con menores en la Red.*** Ministerio del Interior. Secretaría General Técnica.

Dada la complejidad de estos casos, los expertos coinciden en que las intervenciones para niños, niñas y adolescentes deben diferenciarse claramente de aquellas dirigidas a adultos. Las estrategias de prevención tienen que ser específicas para la infancia y estar basadas en la evidencia. Reconocer la existencia de perfiles y trayectorias diversas puede ayudar a diseñar estrategias de actuación específicas para prevenir mayores daños hacia la infancia.

9.5. Medidas en el ámbito judicial

El sistema judicial presenta aún grandes retos en la comprensión y valoración del daño causado por la violencia sexual digital, particularmente en la infancia y la adolescencia. Es urgente:

- **Garantizar una respuesta judicial especializada y adaptada a las especificidades de la violencia sexual digital contra la infancia y la adolescencia,** mediante la creación de las secciones especializadas en violencia contra la infancia y la adolescencia (LO 1/2025 de medidas en materia de eficiencia Servicio Público de Justicia) en todo el territorio. Los casos de explotación sexual digital que afectan a la infancia y la adolescencia deben ser conocidos por estas secciones, desde un enfoque de infancia y con el interés superior en el centro de cada proceso.

- Las formaciones a los jueces y magistrados deben incluir de forma específica las formas de violencia digital que afectan a la infancia y la adolescencia, así como sus consecuencias y efectos.

- **Extender y consolidar el modelo *Barnahus*,** integrado en el modelo especializado de justicia, asegurando que también integre los casos de violencia sexual en el entorno digital, para garantizar una actuación coordinada, especializada y adaptada a las necesidades de la infancia y la adolescencia que ha sido víctima en este entorno, reduciendo la victimización secundaria.

- Al mismo tiempo, es necesario el **fortalecimiento, a través de la dotación de recursos** de los equipos de investigación especializados y de los equipos de servicios sociales comunitarios y especializados, para la mejora de la prevención, el reporte, la detección, la investigación y la actuación.

Secciones de violencia contra la infancia y la adolescencia

El 3 de junio de 2025, el Consejo de Ministros aprobó el Real Decreto 422/2025, por el que se crean las secciones de violencia contra la infancia en los nuevos tribunales de instancia, que prometía el desarrollo de la justicia especializada conforme al mandato establecido en la LOPIVI hace cuatro años, y conforme a lo dispuesto en la LO 1/2025, de 2 de enero, de medidas en materia de eficiencia del Servicio Público de Justicia. Sin embargo, el texto solo prevé la creación de tres secciones especializadas para todo el Estado, en Madrid, Barcelona y Málaga, cada una de ellas con una única plaza judicial y sin crear fiscalías especializadas.

Aunque la implantación de estas secciones deba ser progresiva, partir de tres plazas resulta manifiestamente insuficiente: esta decisión deja fuera de una respuesta especializada a la mayor parte de la infancia y la adolescencia, que seguirá dependiendo de secciones de instrucción, sin enfoque de infancia. Es cierto que el Real Decreto prevé revisar las cargas de trabajo de estas secciones a partir del 31 de diciembre de 2026, pero este supone un plazo demasiado largo. Es necesario, por tanto, aumentar el número de secciones y plazas judiciales desde el inicio, para cumplir con los compromisos adquiridos bajo la LOPIVI, permitiendo sentar las bases de una justicia verdaderamente adaptada y accesible para la infancia y la adolescencia.

9.6. Medidas legislativas

Pese a los avances legislativos (en el ámbito europeo, con el DSA, la propuesta del Reglamento sobre prevención y lucha contra el abuso sexual infantil y la reforma de la Directiva de abuso sexual infantil; y en el nacional, mediante la LOPIVI y ahora la tramitación del PLO para la protección de personas menores de edad en entornos digitales), estos marcos penales no responden todavía abordando la explotación sexual digital de la infancia en su conjunto. Es necesario por tanto el refuerzo legislativo. Por otro lado, la implementación efectiva de las disposiciones legales y las políticas públicas es crucial.

De este modo, recomendamos:

Reforzar el marco normativo y de política pública nacional y europea para:

- Incorporar de forma explícita y coherente las distintas modalidades de explotación sexual digital de la infancia y la adolescencia en los marcos estratégicos y de política pública nacionales y europeos.
- Garantizar que el marco legal en materia de violencia sexual digital contra la infancia y adolescencia se mantenga permanentemente actualizado y con la dotación de recursos adecuados para su implementación, y con un enfoque tecnológicamente neutro, de forma que permita: adaptarse con agilidad a la rápida evolución de los entornos digitales, herramientas tecnológicas y *modus operandi* utilizados en la comisión de estos delitos; evitar vacíos legales derivados de la aparición de nuevas plataformas, formatos o prácticas que, sin una regulación flexible, podrían quedar fuera del alcance de la protección jurídica; y favorecer un enfoque que priorice la prevención.
- Impulsar la inclusión de una definición jurídica clara y armonizada de la explotación sexual digital en los instrumentos normativos europeos vinculantes, en particular en el marco de la revisión de la Directiva 2011/93/UE y del nuevo Reglamento sobre prevención y lucha contra los abusos sexuales a niños, niñas y adolescentes.
- A nivel nacional, velar por una transposición rigurosa y coherente de la futura normativa europea (Directiva y Reglamento) al ordenamiento jurídico español, que deberá incluir la actualización del Código Penal y otras normas relevantes para adaptar el lenguaje legal conforme a los estándares internacionales (por ejemplo, sustituyendo el término «pornografía infantil» por «material de abuso sexual infantil»). La transposición debe ir acompañada de estudios de impacto normativo, social y presupuestario, y de mecanismos efectivos de implementación (coordinación institucional, dotación de recursos, formación especializada y seguimiento independiente).

La voz de la infancia en el diseño del marco regulatorio del entorno digital

La participación infantil es un derecho reconocido por la Convención sobre los Derechos del Niño, que implica que los niños y niñas deben tener la oportunidad de expresar sus opiniones sobre asuntos que les afectan y que estas opiniones deben ser tenidas en cuenta en la toma de decisiones.

Así, solo a través de la inclusión de su perspectiva en el diseño de marcos regulatorios podrá garantizarse un entorno digital verdaderamente seguro, inclusivo, adecuado a sus necesidades y respetuoso con todos sus derechos.

9.7. Desarrollo tecnológico y responsabilidad de las empresas tecnológicas

En relación con la **innovación tecnológica:**

- Impulsar una innovación tecnológica que, más allá de la detección del CSAM, se oriente a la prevención, detección, obtención de pruebas e identificación de víctimas de todas las formas de explotación sexual.
- Asegurar que el uso de las tecnologías esté acompañado de garantías sólidas: supervisión humana, rendición de cuentas y protocolos claros entre plataformas, cuerpos policiales y servicios sociales. Es fundamental garantizar el respeto a los derechos fundamentales en su aplicación, prestando especial atención al equilibrio entre protección y privacidad, y promoviendo un enfoque ético y basado en evidencias.

Las plataformas digitales desempeñan un papel central en la explotación sexual de niños, niñas y adolescentes, tanto por ser el espacio donde se producen buena parte de los contactos, manipulaciones y difusión de contenidos, como por su capacidad técnica y operativa para prevenir, detectar y actuar frente a este tipo de violencia.

Por ello, las **empresas y plataformas tecnológicas** deben asumir un compromiso ético firme y desarrollar una cultura empresarial centrada en la protección de la infancia y la adolescencia:

- Establecer **mecanismos de verificación de edad efectivos** que impidan el acceso a páginas y contenidos perjudiciales para la infancia y la adolescencia, y que permitan adaptar las funcionalidades y el diseño de las plataformas en función de la edad. Estos mecanismos deben respetar los principios de minimización proporcionalidad y protección de datos.

- Implementación de **sistemas de moderación efectivos, transparentes y auditables,** que incluyan la detección de contenidos que sexualicen a la infancia o puedan suponer riesgos relacionados con formas de explotación.

- Asegurar la **transparencia de algoritmos y sistemas de recomendación,** abordando específicamente el fenómeno del *grooming* algorítmico.

- Aplicar **tecnologías de detección de material de abuso y explotación sexual** en sus plataformas, asegurando que sean éticas, eficaces, y que permitan el equilibrio entre privacidad y protección.

- Asegurar **mecanismos efectivos y ágiles para el reporte y la retirada de contenidos** ilícitos, y la colaboración con las autoridades en las investigaciones.

- Las **empresas desarrolladoras de IA** deben integrar medidas de prevención del uso indebido de sus herramientas.

Por su parte, las **administraciones públicas** deben avanzar hacia una mayor regulación del entorno digital y la responsabilidad del sector privado frente a la explotación sexual *online*, para:

- Establecer **obligaciones legales específicas para plataformas digitales y proveedores de servicios en línea,** que abarquen la detección y notificación de contenidos ilícitos, la verificación efectiva de edad, la validación de identidad de las personas que comparten o venden contenidos (especialmente en plataformas de intercambio de contenidos), la moderación proactiva de contenidos y el diseño seguro (*safety by design*) de entornos digitales, especialmente aquellos dirigidos o accesibles a niños, niñas y adolescentes.

- Promover **códigos de conducta y estándares técnicos comunes**, adaptados a las capacidades de plataformas de distinto tamaño, para garantizar que todas operen bajo criterios mínimos de protección digital de la infancia y la adolescencia. Al mismo tiempo, incentivar, promover y reconocer la incorporación de estándares máximos, con enfoque de infancia como valor añadido para las tecnologías y plataformas

- Fomentar la **auditoría externa y mecanismos de rendición de cuentas** del sector privado.

Así, es imprescindible avanzar hacia **una legislación de corresponsabilidad con las plataformas tecnológicas,** garantizando mecanismos efectivos de supervisión, sanción y rendición de cuentas para las empresas. La tramitación del PLO de pro-

tección de personas menores de edad en entornos digitales ofrece una oportunidad para adaptar y fortalecer el marco legal estatal con instrumentos concretos, asegurando su implementación efectiva.

> ***«Las plataformas digitales tienen una responsabilidad total en la prevención de la ESIA, ya que deberían controlar el contenido que circula en sus espacios».***
>
> —Profesional del ámbito académico

Necesidad de colaboración de las plataformas digitales para la detección, investigación y abordaje de la explotación sexual digital

La lucha contra la explotación infantil digital no puede ser eficaz si no existe una colaboración estructurada entre los Estados y las empresas tecnológicas y si no se articulan mecanismos compartidos para la detección y reporte transfronterizo de contenidos ilícitos, como ha indicado el eSafety Commissioner. La colaboración debe incluir el uso de herramientas tecnológicas avanzadas para detectar contenido delictivo como el reporte ágil a las autoridades, la retirada de contenidos y el apoyo a investigaciones. Sin embargo, esta cooperación es desigual: algunas grandes plataformas han implementado medidas proactivas relevantes para detección automatizada de material conocido, la moderación reforzada de contenidos, o la cooperación con organismos internacionales especializados, pero muchas plataformas todavía se escudan en principios como la neutralidad tecnológica, la privacidad de las comunicaciones o la ausencia de intencionalidad para evitar asumir responsabilidades concretas. Agentes clave también han advertido de que las plataformas, en algunos casos, podrían llegar a ser consideradas responsables penales si se demuestra conocimiento y beneficio económico directo, y reclaman avanzar hacia obligaciones legales basadas en el principio de diligencia debida, y no solo en medidas voluntarias o códigos de conducta.

El problema no es solo técnico, sino también estructural y político. Parte de la debilidad del sistema actual reside en la falta de una autoridad supervisora con capacidad de exigir una rendición de cuentas efectiva. Así, la autorregulación ha demostrado ser insuficiente: se necesita un marco jurídico claro, exigente y coherente, que establezca obligaciones vinculantes, protocolos de actuación, plazos de respuesta, y mecanismos de supervisión y sanción efectivos. La corresponsabilidad real exige que las plataformas cumplan con la legalidad vigente, desarrollando buenos mecanismos de «compliance» y canales de denuncia previstos en la legislación (DSA, y Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción), desarrollando una cultura organizacional centrada en la protección y la promoción de la infancia y la adolescencia. Esto requiere inversiones concretas en equipos especializados, colaboración activa con las fuerzas de seguridad y el diseño de espacios digitales seguros desde el diseño, con la participación de la infancia, las familias, y los y las profesionales de atención a la infancia.

«La protección de los NNA no puede depender exclusivamente de la voluntad de las plataformas».

—Jurista especializada en violencias sexuales digitales

9.8. Fortalecimiento institucional y la cooperación internacional

Finalmente, la explotación digital va más allá de las fronteras legales, tecnológicas y administrativas de los Estados, lo que exige estructuras de cooperación que garanticen una respuesta coordinada y efectiva. En este sentido, se hace necesario:

- **Establecer un mecanismo nacional de coordinación centralizada,** inspirado en modelos como el NCMEC estadounidense o el futuro Centro Europeo para la Prevención y Lucha contra el Abuso Sexual Infantil, previsto por el futuro Reglamento de la UE. Este centro debería facilitar la recogida y análisis de datos, la coordinación operativa entre instituciones, y el diseño de políticas públicas basadas en evidencia.

- **Reforzar la cooperación internacional en justicia penal y protección de la infancia y la adolescencia,** mediante acuerdos bilaterales y multilaterales que aseguren la trazabilidad de los delitos, el intercambio ágil de información y la actuación coordinada en contextos transfronterizos, especialmente ante la rápida circulación global de contenidos ilícitos. Las obligaciones de asistencia mutua y cooperación que contiene el Convenio del Consejo de Europa[70] sobre ciberdelincuencia son clave en este sentido.
- **Armonizar los protocolos de conservación de datos y respuesta inmediata,** asegurando que los proveedores de servicios digitales y las autoridades competentes cuenten con criterios comunes y plazos efectivos de actuación ante la detección o denuncia de contenidos relacionados con la explotación sexual digital.

10. Conclusiones

La explotación sexual digital de la infancia y la adolescencia supone una forma de violencia muy compleja, que abarca diferentes formas y se solapa o se da simultáneamente con otras violencias. Aunque adopta nuevas dimensiones en el entorno digital, es una violencia que se alimenta de dinámicas tradicionales en estos contextos, como el abuso de poder y la explotación de vulnerabilidades, y de factores sociales como la cosificación y la desigualdad, y que encuentra en lo digital un nuevo espacio para crecer, adaptarse y ocultarse. Identificar las dinámicas que la componen no siempre es fácil, por lo que todavía es necesario un esfuerzo conjunto, desde múltiples ámbitos, para hacer frente a este grave problema, que todavía tenemos que aprender a reconocer como sociedad.

No es sencillo. Nada en la lucha contra la explotación sexual de la infancia lo es. Ni siquiera admitir que el problema existe y que afecta a muchos más niños y niñas de los que pensamos es una tarea fácil: muchas de las formas de violencia que hemos abordado en este informe pueden resultar inimaginables para muchas personas. Pero aunque sea una realidad difícil de asumir no se puede mirar hacia otro lado. Es fundamental hablar de ello con claridad, sin eufemismos, entender cómo afecta a los niños, niñas y adolescentes y, sobretodo, cómo y por qué pueden llegar a suceder estas violencias, para poder prevenirlas.

70 Véanse los artículos 27 a 35 del Convenio del Consejo de Europa sobre cibercriminalidad hecho en Budapest el 23 de noviembre de 2001, serie de tratados del Consejo de Europa, nº 185, BOE núm. 226 de 17 de septiembre de 2010.

La información, por tanto, es clave: necesitamos, ante todo, saber. Investigar, generar evidencias, recopilar datos, formar a profesionales, concienciar a familias, educadores, niñas y niños, son acciones imprescindibles, proporcionando herramientas adecuadas. Pero, sobre todo, es necesaria una voluntad colectiva para acabar con los riesgos y violencias que se propagan por Internet, y con la impunidad que normalmente los acompaña.

Y es que el entorno digital no es neutro: es el resultado de lo que las y los usuarios le aportamos y, por tanto, un reflejo de la sociedad en la que vivimos. Las violencias no suceden porque sí en este espacio, sino que, más allá de los factores puramente técnicos, se sostienen por factores y conductas que las facilitan, y que como sociedad no podemos seguir normalizando. Es hora de reflexionar sobre nuestros comportamientos en Internet, particularmente en las redes y otros espacios a los que también tiene acceso la infancia y la adolescencia, y también sobre los contenidos que visualizamos, las narrativas que reproducimos sin cuestionar, las dinámicas que normalizamos (como la hipersexualización, los estereotipos de género o la cosificación del cuerpo), y el ejemplo que damos a la hora de compartir información, interactuar con otras personas, o compartir imágenes que no nos pertenecen. Las conductas en la red, las creencias que tenemos sobre lo que es aceptable o «normal» en el entorno digital, dan forma al contexto y los marcos dentro de los que se llega a tolerar o invisibilizar la explotación sexual digital.

Al mismo tiempo, debemos comprender que el entorno digital se ha configurado como algo más que una herramienta en el modo de vida actual, y de forma especial para la infancia y la adolescencia, para quienes supone un espacio más en el que se desarrollan, socializan, descubren y exploran su sexualidad y configuran su identidad. Es necesario dejar a un lado los prejuicios y enfoques culpabilizadores sobre las interacciones de riesgo que pueden asumir, y en su lugar preguntarse por qué las asumen y de qué manera se puede minimizar la exposición a estos riesgos, siempre desde un enfoque de derechos: los niños, niñas y adolescentes deben poder ejercer todos sus derechos de forma libre, segura y efectiva en todos los espacios en los que se desarrollan, incluido el digital.

Es nuestro deber conjunto asegurar que así sea: las familias, escuelas, plataformas digitales e instituciones públicas deben asumir un compromiso colectivo para construir un ecosistema digital verdadera y efectivamente protector con la infancia y la adolescencia, asumiendo que las consecuencias de todo lo que les sucede en este espacio, tanto las buenas como las malas, son igual de las de reales que las que tienen lugar en otros entornos, y afrontándolas con la gravedad que merecen.

Anexo. Marco legal para el abordaje de la explotación sexual en entornos digitales

Uno de los obstáculos en la lucha contra las diferentes formas de explotación sexual de la infancia y la adolescencia en entornos digitales es la falta de un marco jurídico armonizado que abraque todas estas manifestaciones y tenga en cuenta las nuevas realidades tecnológicas.

A nivel nacional, el Gobierno ha impulsado la tramitación del Proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales que incorpora obligaciones concretas para las plataformas digitales, proveedores de contenidos y fabricantes de dispositivos conectados. Por un lado, la obligación de establecer mecanismos eficaces de verificación de edad adecuados al nivel de riesgo del servicio, que deben ser auditables, proporcionales y respetuosos con los derechos fundamentales. Esta medida es clave para prevenir el acceso de menores de edad a servicios inadecuados o entornos donde puedan ser objeto de explotación o captación. Además, el deber de cooperación reforzada con las autoridades competentes, tanto en materia judicial como administrativa, que incluye la preservación y entrega rápida de evidencias electrónicas cuando sea requerido judicialmente, como ya prevé también el paquete e-evidence a nivel europeo.

El texto prevé una serie de reformas penales orientadas a adaptar el marco jurídico a los nuevos delitos tecnológicos:

- Prohibición de acceso a entornos virtuales como pena principal o accesoria, cuando el delito se haya cometido en estos espacios.
- Tipificación específica de los *deepfakes* de contenido sexual (ultrafalsificaciones), respondiendo al uso creciente de IA para generar CSAM sintético.
- Tipos agravados vinculados al uso de identidades falsas, que afectan a delitos como el abuso y la explotación sexual infantil (artículos 181 a 189).

A nivel europeo, en 2022, se aprobó el Reglamento de Servicios Digitales (DSA), un hito normativo que busca garantizar un entorno digital más seguro, respetuoso y transparente. El DSA reconoce la protección de niños, niñas y adolescentes como un objetivo político prioritario de la UE (considerando 71), que se traduce en obligaciones concretas para las plataformas digitales, especialmente aquellas que son utilizadas por la infancia y la adolescencia (considerando 46).

Pero sin duda, el instrumento jurídico europeo más relevante en relación a la protección frente al abuso sexual y algunas formas de explotación es el **Reglamento**

del Parlamento Europeo y del Consejo por el que se establecen normas para prevenir y combatir el abuso sexual infantil, cuya Propuesta todavía está siendo debatida entre los Estados miembro.

La Comisión Europea presentó en primer lugar un Reglamento provisional (Reglamento UE 2021/1232), que establece una derogación temporal del marco de privacidad contenido en la Directiva 2002/58/CE (Directiva e-Privacy), con el fin de permitir que los proveedores de servicios de comunicaciones interpersonales sigan detectando, notificando y eliminando voluntariamente material de abuso sexual infantil en línea. En 2022, la Comisión presentó una propuesta de Reglamento para consolidar estas obligaciones a través de un marco jurídico obligatorio y armonizado en la UE.

El Reglamento está diseñado para abordar tanto formas conocidas como emergentes de abuso sexual digital, incluyendo el CSAM y el *grooming*, mediante la imposición de obligaciones de detección, notificación y retirada de dichos contenidos. Estas obligaciones se aplican a todos los proveedores de servicios de alojamiento y comunicación interpersonal que operen en la UE, independientemente de su lugar de establecimiento. Entre sus medidas más destacadas:

» La creación del Centro Europeo para la Prevención y Lucha contra el Abuso Sexual Infantil (EUCSA),[71] al que se le asignan funciones clave: su papel como centro de coordinación y conocimiento técnico a nivel europeo, la gestión de bases de datos con indicadores para la detección de CSAM, la verificación del cumplimiento por parte de los proveedores de sus obligaciones de notificación y eliminación de contenidos, así como el apoyo a los Estados miembros en la protección y asistencia a las víctimas y en la coordinación de las actuaciones pertinentes.

> ***«Esto es algo importantísimo, como un NECMEC europeo para prevenir y luchar contra los abusos sexuales a menores y además que sea un facilitador a las empresas».***
>
> —Experta en derechos digitales de la infancia la adolescencia

» La obligación general de que los proveedores evalúen el riesgo de uso indebido de sus servicios para la difusión de CSAM, que deberá ir acompañada de medidas de mitigación adecuadas, como la aplicación de sistemas de verificación de edad.

71 La UE depende actualmente de entidades extranjeras como el NCMEC para la mayoría de los reportes de CSAM generados por las grandes plataformas digitales, lo que plantea importantes limitaciones operativas, jurídicas y de soberanía.

» Cuando una autoridad nacional detecte, a partir de las evaluaciones de riesgo, una amenaza significativa, podrá solicitar administrativa o judicialmente una orden de detección, que obligará al proveedor a implantar tecnologías automatizadas de reconocimiento de contenidos para identificar CSAM o *grooming*. Los propios proveedores podrán decidir qué tecnologías usar, debiendo ser lo menos intrusivas posibles. Estas órdenes deberán respetar el principio de proporcionalidad, y ser limitadas temporalmente (máximo dos años para CSAM y uno para *grooming*) y materialmente (parte del servicio afectado).

Esta propuesta, sin embargo, está siendo objeto de un intenso debate y de controversia entre los distintos miembros. En el foco de este debate, se encuentran principalmente las cuestiones relacionadas con la privacidad, además de la cuestión de la voluntariedad o la obligatoriedad de las empresas y plataformas para llevar a cabo actuaciones de detección.

La jurisprudencia a nivel europeo

La falta de precisión del marco legal que protege a la infancia frente a delitos sexuales cometidos mediante tecnologías plantea problemas para la efectiva protección de sus derechos humanos. En la sentencia *Söderman c. Suecia*,[72] relativa al caso de un hombre que grababa a su hijastra en el baño sin difundir posteriormente el material, evidenció vacíos legales que pueden llevar a la desprotección. Por ello, el Tribunal Europeo de Derechos Humanos (TEDH) reiteró la necesidad de contar con un marco jurídico efectivo y suficientemente protector de la infancia víctima de violencia sexual, exigiendo la existencia de disposiciones penales para los casos más graves.

El TEDH también exige en su jurisprudencia la necesidad de disponer de instrumentos legales suficientes para llevar a cabo las investigaciones precisas para proteger a las víctimas, y que estos deben de ser utilizados de acuerdo con las garantías legales precisas. Por ejemplo, en el caso *K.U. c. Finlandi*a,[73] un usuario creó un anuncio falso en Internet de un niño de 12 años buscando relaciones íntimas con hombres, utilizando la imagen y los datos de contacto reales del niño.

72 Sentencia del Tribunal Europeo de Derechos Humanos de 12 de noviembre de 2013 en el asunto Söderman c. Suecia, demanda n.º 5786/08.

73 Sentencia del Tribunal Europeo de Derechos Humanos de 2 de diciembre de 2008 en el asunto K.U. c. Finlandia, demanda n.º 2872/02.

El tribunal finlandés competente rechazó en su momento la solicitud de la policía para obligar al proveedor del servicio de las telecomunicaciones a revelar la identidad del infractor, pues la legislación nacional de la época no permitía a las autoridades exigir a los operadores de telecomunicaciones la revelación de la identidad de un usuario. En este caso, el TEDH declaró la violación del artículo 8 del Convenio Europeo de Derechos Humanos.

Sin embargo, para el TEDH, la protección de la infancia frente al abuso sexual no justifica cualquier intervención: en la sentencia *Trabajo Rueda c. España*,[74] declaró la vulneración del derecho a la vida privada de un hombre condenado por tener y compartir CSAM por Internet, pues la policía había procedido a inspeccionar los archivos de su ordenador sin orden judicial. A pesar de la urgencia del caso, el Tribunal consideró que obtener dicha autorización no habría impedido una investigación eficaz, y no encontró justificación para no haber procedido a ella.

74 Sentencia del Tribunal Europeo de Derechos Humanos de 30 de mayo de 2017 en el asunto Trabajo Rueda c. España, demanda n.º 32600/12.

Nota metodológica

La investigación para este informe se ha basado en una metodología de carácter cualitativo y documental. El análisis se ha basado, por un lado, en la revisión de marcos normativos internacionales, europeos y nacionales, así como de documentos estratégicos y propuestas legislativas en curso. Por otro lado, se ha realizado un análisis documental exhaustivo de literatura especializada, informes técnicos, estudios académicos e investigaciones recientes sobre el fenómeno, en castellano e inglés.

El informe incorpora también aportes clave procedentes del trabajo de campo cualitativo, que incluyó nueve entrevistas semiestructuradas con personas expertas de diversos ámbitos, y un grupo focal adicional con cuatro profesionales con experiencia directa en la intervención en casos de violencia sexual digital hacia la infancia. Estos insumos han permitido recoger percepciones, experiencias y valoraciones prácticas que complementan la dimensión normativa y analítica del trabajo:

- Profesionales del ámbito jurídico, incluyendo abogacía, fiscalía y judicatura, con especialización en derecho penal, derechos de la infancia y violencia sexual.
- Expertas en derechos digitales y protección de la infancia en el entorno digital.
- Representantes de cuerpos y fuerzas de seguridad especializados en ciberdelincuencia.
- Profesionales de instituciones públicas en materia de ciberseguridad.
- Profesionales del ámbito académico y la investigación en criminología, psicología, derecho y ciberdelincuencia.
- Profesionales del ámbito forense y de atención especializada en violencia sexual contra la infancia.
- Representantes de organizaciones de referencia en la lucha contra la explotación sexual infantil.

Además, se realizaron dos talleres de discusión no mixtos con chicas y chicos de entre 15 y 18 años, recogiendo sus opiniones desde una perspectiva de género para identificar las oportunidades y el riesgo de las TIC para los y las adolescentes y sus herramientas de afrontamiento, analizar y conocer sus opiniones sobre las formas de violencia sexual *online*, con especial atención al concepto de consentimiento e intercambio, y establecer propuestas de mejora para garantizar que Internet sea un espacio seguro para la infancia y adolescencia.

Por otro lado, el estudio cuantitativo se ha realizado mediante un diseño transversal basado en autoinforme, en el que se ha preguntado a una muestra de jóvenes de entre 18 y 21 años residentes en España sobre sus conocimientos, creencias y experiencias en relación con la explotación sexual en entornos digitales durante la adolescencia. La recogida de datos se llevó a cabo entre el 10 de marzo y el 26 de abril de 2025, en formato *online*. La muestra final obtenida consta de 1.008 participantes, con una media de 19,4 años (DT = 1,03).La mayoría eran estudiantes (98,4 %), aunque un 20,7 % compaginaba los estudios con un trabajo remunerado. En la Tabla 6 de detallan las características sociodemográficas.

Tabla 6. ***Características sociodemográficas.***

		n	%
Género	Masculino	234	23,2
	Femenino	773	76,7
	Otro	1	0,1
Edad	18	217	21,5
	19	342	33,9
	20	254	25,2
	21	195	19,3
Orientación sexual	Heterosexual	798	79,2
	Homosexual	37	3,7
	Bisexual	168	16,7
	Otra	5	0,5
País de origen	España	977	96,9
	Otro	31	3,1
Núcleo de convivencia	Familia de origen	760	75,4
	Amigos/as	166	16,5
	Pareja	17	1,7
	Solo/a	23	2,3
	En un centro	7	0,7
	Otro	35	3,5
Nivel socioeconómico	Bajo	22	2,2
	Medio-bajo	209	20,7
	Medio	546	54,2
	Medio-alto	227	22,5
	Alto	4	0,4
Ocupación	Solo estudio	783	77,7
	Solo trabajo	11	1,1
	Estudio y trabajo	209	20,7
	Ni estudio ni trabajo	5	0,5

En relación con la distribución territorial de los y las participantes según su comunidad autónoma de residencia, la mayoría procedía de Andalucía (26,7 %), Cataluña (18,2 %), Comunidad de Madrid (12 %) y Comunidad Valenciana (9,7 %). Esta concentración geográfica guarda coherencia con la distribución poblacional de jóvenes en esas edades a nivel nacional, ya que dichas comunidades autónomas son, según los datos más recientes del Instituto Nacional de Estadística (INE, 2025), las que cuentan con el mayor volumen absoluto de población joven. Aunque la muestra no es representativa en términos estadísticos, su validez se refuerza al reflejar tendencias demográficas reales del país, lo que permite inferencias razonables sobre el colectivo estudiado en contextos similares.

Tabla 7. ***Distribución por comunidades autónomas.***

CC. AA.	%	n
Andalucía	26.7	269
Aragón	2.3	23
Asturias	2.1	21
Baleares	1.1	11
Canarias	1.5	15
Cantabria	2.3	23
Castilla La Mancha	4.3	43
Castilla y León	5.8	58
Cataluña	18.2	183
Ceuta	0.3	3
Comunidad Valenciana	9.7	98
Extremadura	4.3	43
Galicia	3.3	33
Madrid	12	121
Melilla	0.3	3
Navarra	2.2	22
País Vasco	3.9	39

Bibliografía

» Açar, K. V. (2017). ***Webcam child prostitution: An exploration of current and futuristic methods of detection.*** International Journal of Cyber Criminology, 11(1), 98–109.

» Briere JN, Elliott DM. Immediate and long-term impacts of child sexual abuse. Future Child. 1994 Summer-Fall;4(2):54-69. PMID: 7804770.

» Christensen, L. S., & Woods, J. (2024). «It's Like POOF and It's Gone»: The Live-Streaming of Child Sexual Abuse. Sexuality & Culture, 28(1), 1467–1481.

» Comisión Europea (2023). ***Complementary impact assessment: Proposal for a Regulation laying down the rules to prevent and combat child sexual abuse.*** Publications Office of the European Union. Publicado el 27 de abril de 2023. ISBN 978-92-848-0446-7.

» CRIN (2022). ***Explaining the technology for detecting child sexual abuse online.***

» Davidson, J., Farr, R., Bradbury, P., & Meggyesfalvi, B. (2024). VIRRAC toolkit report: Virtual reality risks against children. Institute for Connected Communities, University of East London.

» Diaconía (2024). ***Guía para profesionales del ámbito educativo. Trata en el mundo digital: protegiendo a los menores.*** Madrid: Diaconía.

» Dushi, D. (2019). Online child sexual exploitation and abuse: Investigating the live streaming of child sexual abuse and the responses of the criminal justice system. European Journal of Crime, Criminal Law and Criminal Justice, 27(3), 189–206.

» ECPAT International & INTERPOL (2018). ***Summary – Towards a global indicator on unidentified victims in child sexual exploitation material.*** ECPAT International.

» ECPAT International (2018). ***Trends in Online Child Sexual Abuse Material.*** ECPAT International.

» ECPAT International (2020). ***Summary paper on online child sexual exploitation.*** ECPAT International.

» ECPAT International (2025). ***Terminology guidelines for the protection of children from sexual exploitation and sexual abuse.***

» eSafety Commissioner (2023). ***Generative AI—Tech trends position statement.***

» eSafety Commissioner (n.d.). ***Safety by design.***

» Europa Press (20 de marzo de 2025). ***Más del 50 % de participantes en el proyecto STOP-CSAM deja de consumir material de abuso sexual infantil.***

» Europol (2017). ***Online sexual coercion and extortion as a form of crime affecting children: Law enforcement perspective.*** European Union Agency for Law Enforcement Cooperation.

» Europol (2019). ***Operation Chemosh: How encrypted chat groups exchanged emoji 'stickers' of child sexual abuse.*** Europol Newsroom.

» Europol (2019). ***Internet Organised Crime Threat Assessment (IOCTA).*** The Hague: Europol.

» FAPMI-ECPAT España (2021). ***La explotación sexual de la infancia y la adolescencia: Monográfico.***

» Fiscalía General del Estado (2024). ***Memoria de la Fiscalía General del Estado. Año 2023.***

» Fry, D., Krzeczkowska, A., Ren, J., Lu, M., Fang, X., Anderson, N., & Steele, B. (2025). ***Prevalence estimates and nature of online child sexual exploitation and abuse: a systematic review and meta-analysis.*** The Lancet Child & Adolescent Health. DOI: 10.1016/S2352-4642(24)00329-8

» Gámez Guadix, M., de Santisteban, P., & Resett, S. A. (2017). ***Sexting among Spanish adolescents: Prevalence and personality profiles.*** Psicothema, 29(1), 29.34.

» Grant, H. (2025, 5 de abril). ***«I didn't start out wanting to see kids»: Are porn algorithms feeding a generation of paedophiles – or creating one?*** The Guardian.

» Greenberg, A. (2022, April 7). ***The crypto trap: Inside the Bitcoin bust that took down the web's biggest child abuse site.*** Wired.

» Grupo de trabajo de concienciación, proyecto 4NSEEK (2021). ***Abuso sexual de menores en Internet: un análisis de 4NSEEK.*** Instituto Nacional de Ciberseguridad (INCIBE), Asociación Portuguesa de Apoyo a las Víctimas (APAV), Guardia Civil (EMUME Central – Unidad Técnica de Policía Judicial), Cuerpo Nacional de Policía, Policía de Malta, EUROPOL – European Cybercrime Centre (EC3), UNICEF España, Federación de Asociaciones para la Prevención del Maltrato Infantil (FAPMI) – ECPAT España y EU Kids Online (Universidad del País Vasco).

» Grupo de Trabajo Interinstitucional sobre Explotación Sexual de Niñas, Niños y Adolescentes (2016). ***Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.*** ECPAT International.

» Hailes, H. P., Yu, R., Danese, A., & Fazel, S. (2019). Long-term outcomes of childhood sexual abuse: An umbrella review. The Lancet Psychiatry, 6(10), 830-839. DOI: 10.1016/S2215-0366(19)30286-X

» Horowitz, J., & Blunt, K. (2023, June 7). ***Instagram connects vast pedophile network.*** The Wall Street Journal.

» Insoll, T., Ovaska, A., & Vaaranen-Valkonen, N. (2021). ReDirection Survey Report: ***CSAM users in the dark web – Protecting children through prevention.*** Suojellaan Lapsia ry / Protect Children.

» Instituto Nacional de Ciberseguridad (INCIBE) (s.f.). ***Sharenting: cuando los padres ponen en riesgo la imagen de sus hijos.*** INCIBE.

» Internet Watch Foundation (2023). ***How AI is being abused to create child sexual abuse imagery.***

» Internet Watch Foundation (2022). ***Geographical hosting of URLs. Annual report 2022.***

» Internet Watch Foundation (2021). ***Annual Report 2020.*** Internet Watch Foundation.

» INTERPOL (2020). ***Riesgos y tendencias en relación con el abuso y la explotación sexual de menores: repercusiones de la COVID-19.***

» INTERPOL (s.f.). ***Base de Datos Internacional sobre Explotación Sexual de Niños.***

» Jonsson, L. S.; Fredlund, C.; Priebe, G.; Wadsby, M. y Svedin, C. G. (2019). ***Online sexual abuse of adolescents by a perpetrator met online: A cross-sectional study.*** Child and Adolescent Psychiatry and Mental Health, 13, Artículo 32.

» Medrano, J. L. J.; López-Rosales, F.; & Gámez-Guadix, M. (2018). ***Assessing the links of sexting, cybervictimization, depression, and suicidal ideation among university students.*** Archives of Suicide Research, 22(1), 153–164.

» Ministerio del Interior (2025). ***Investigaciones policiales por delitos de online child sexual grooming en España.*** NIPO 126-24-101-5.

» Ministerio del Interior. ***Cibercriminalidad.*** Portal Estadístico de Criminalidad.

» Montiel, I. (2016). ***Cibercriminalidad social juvenil: la cifra negra.*** IDP. Revista de Internet, Derecho y Política, 2016, n.º 22, doi:10.7238/idp.v0i22.2972.

» Napier, S.; Teunissen, C. ; & Boxall, H. (2021). ***Live streaming of child sexual abuse: An analysis of offender chat logs.*** Trends & Issues in Crime and Criminal Justice, 639. Australian Institute of Criminology.

» National Center for Missing & Exploited Children (NCMEC) (s.f.). ***CyberTipline Data.***

» National Institute of Standards and technology (NIST) of US department of Commerce (2024). ***Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile.***

» NCMEC (2024). ***Generative AI CSAM is CSAM.***

» NetClean (2018). ***NetClean Report 2018.***

» NSPCC (2023). ***Child safeguarding and immersive technologies.***

» Observatorio Nacional de Tecnología y Sociedad (ONTSI) (2022). ***Beneficios y riesgos del uso de Internet y redes sociales.*** ONTSI.

» Ofcom (2024). ***Protecting children from harms online. Vol. 5: What should services do to mitigate the risks.***

» Padilla López, L. (2025). ***El proxenetismo digital y la captación de menores en redes sociales: un análisis sobre la hipersexualización y el empoderamiento en plataformas online.*** Revista de Victimología, (19), 213–250.

» Pereda, N., Águila-Otero, A., Codina, M., & Cabrera, M. (2022). ***Guía común de actuación para la detección, notificación y derivación de casos de explotación sexual contra la infancia en centros residenciales, con especial atención a niñas y adolescentes.*** Delegación del Gobierno contra la Violencia de Género.

» Pfefferkorn, R. (2022). ***Content-oblivious trust and safety techniques: Results from a survey of online service providers.*** Journal of Online Trust and Safety.

» Putnam, F. W. (2003). Ten-year research update review: Child sexual abuse. Journal of the American Academy of Child & Adolescent Psychiatry, 42(3), 269–278.

» Reneses, M., Riberas-Gutiérrez, M., y Bueno-Guerra, N. (2024). ***«Me halagó». Una mirada integral a los factores de riesgo del acoso online: Uniendo las voces de víctimas, agresores y expertos mediante entrevistas en profundidad.*** Cyberpsychology: Journal of Psychosocial Research on Cyberspace , 18 (4), Artículo 3.

» Riberas-Gutiérrez, M., Reneses, M., Gómez-Dorado, A., Serranos-Minguela, L., & Bueno-Guerra, N. (2023). ***Online grooming: Factores de riesgo y modus operandi a partir de un análisis de sentencias españolas. Anuario de Psicología Jurídica,*** Avance *online*.

» Sabri, N., Teoh, A., Vaccaro, K., Chen, B., Dow, S., & ElSherief, M. (2023). ***Challenges of moderating social virtual reality.*** Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, April 23–28, 2023, Hamburg, Germany.

» Salter, M., Zajdow, R., & Salter, R. (2024). ***Understanding the relationship between adult pornography consumption and child sexual abuse material (CSAM) offending: A review of emerging evidence.*** Child Abuse & Neglect, 150, 106472.

» Save the Children (2019). ***Violencia Viral: Análisis de la violencia contra la infancia y la adolescencia en el entorno digital.***

» Save the Children (2020). ***(Des)información sexual: pornografía y adolescencia.***

» Save the Children (2024). ***Desinformación y discurso de odio en el entorno digital.***

» Save the Children International (2005). ***Position paper regarding online images of sexual abuse and other Internet-related sexual exploitation of children.***

» Seto, M. C., Hanson, R. K. y Babchishin, K. M. (2010). ***Contact sexual offending by men with online sexual offenses.*** Sexual Abuse: A Journal of Research and Treatment, 23(1), 124-145.

» Spence, R., Bifulco, A., Bradbury, P., Martellozzo, E., & DeMarco, J. (2023). ***The psychological impacts of content moderation on content moderators: A qualitative study.*** Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 17(4), Article 8.

» Stray et al. (2024). ***Building human values into recommender systems: An interdisciplinary synthesis.***

» Suler J. The online disinhibition effect. Cyberpsychol Behav. 2004 Jun;7(3):321-6. doi: 10.1089/1094931041291295. PMID: 15257832.

» Tech coalition (2025). ***Annual report 2024.***

» Technology Coalition (2023). ***Online grooming: Considerations for detection, response, and prevention.***

» Thiel, D., DiResta, R., and Stamos, A. (2023). ***Cross-platform dynamics of self-generated CSAM. Stanford Digital Repository.***

» Thorn & All Tech Is Human - ATIH (2024). ***Safety by Design for Generative AI: Preventing Child Sexual Abuse.*** Thorn Repository.

» Thorn & WeProtect Global Alliance (2024). ***Evolving Technologies. Horizon Scan. A review of technologies carrying notable risk and opportunity in the fight against technology-facilitated child sexual exploitation.***

» Thorn (2022). ***Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2021.***

» Thorn (2024). ***Youth perspectives on online safety,*** 2023.

» Ullman, S. E. (2003). Social reactions to child sexual abuse disclosures: A critical review. Journal of Child Sexual Abuse, 12(1), 89–121.

» UNICEF (2021). ***Children and digital marketing: Rights, risks and opportunities.***

» World Health Organization (2017). ***Responding to children and adolescents who have been sexually abused: WHO clinical guidelines.***

Agradecimientos: A todas las chicas y chicos que han participado en la investigación para este informe, tanto a quienes han dedicado su tiempo para responder a la encuesta como a los y las adolescentes que formaron parte de los talleres de discusión, compartiendo sus reflexiones y preocupaciones con nosotras. Gracias por hacer posible este informe.

A las y los profesionales que han compartido su saber y conocimiento en las entrevistas y grupos de discusión, y a través de aportaciones al informe: Ana Caballero, Cristina Gutiérrez, Elvira Tejada, Esther Pomares, Irene Montiel, Laira Serra, José García Serrano, Selma Fernández, Tania García Sedano, Raquel Rasposo, Iskander Segurola, Ignacio García Egea, Pilar Aranda i Lara, y Jorge Bardón.

Y a todas las compañeras de Save the Children que han contribuido para sacar adelante la mejor versión posible de este estudio: Carmela del Moral y Catalina Perazzo, por su guía y apoyo; Miguel Borque, Daniel Toda, Laura Soriano, Isabel Arrebola, Irati Álvarez y Martí Bàlius, por todas sus aportaciones; y a Irene Mejía y Ana Cabanillas, por hacer posible la participación de chicas y chicos.

Save the Children

Edita:

Save the Children España
Julio 2025

Save the Children

Colabora:

Asociación Europea para la Transición Digital

savethechildren.es