WeProtect GLOBAL ALLIANCE

PA

CRISP

EVALUACIÓN DE LA AMENAZA GLOBAL DE 2021

Contenidos

01

Preámbulo

Bienvenido a la tercera Evaluación de la amenaza global de la Alianza Global de WeProtect, la primera que hemos realizado desde nuestro lanzamiento como entidad independiente en abril de 2020.

Durante este tiempo, la COVID-19 ha supuesto un impacto sin precedentes. Internet ha ganado más importancia aún en las vidas de los niños. Para protegerlos de la explotación y el abuso sexual online, debemos entender primero el problema al que nos enfrentamos. Y, para hacerlo, debemos escuchar a los gobiernos, al sector privado, a la sociedad civil y, sobre todo, a las víctimas y supervivientes de abusos.

Por primera vez, hemos encuestado a miles de adultos jóvenes en todo el mundo acerca de su experiencia sobre daños sexuales en internet. Compartimos también información exclusiva de la industria tecnológica sobre su respuesta ante este delito. Hemos compilado datos de empresas de seguridad en internet y tendencias emergentes. Todo esto, combinado con una respuesta sin precedentes de nuestros miembros, nos ha proporcionado la evaluación más exhaustiva hasta el momento.

Nos han llamado la atención especialmente tres aspectos:

1 El alcance de la explotación y el abuso sexual a menores online está incrementándose. Este crecimiento sostenido está sobrepasando nuestra capacidad de reacción global. El abuso sexual a menores sigue siendo un problema crónicamente subfinanciado, por lo que hemos trabajado muy duro para construir la Alianza Global. 98 gobiernos, 53 empresas, 61 organizaciones de la sociedad civil y nueve instituciones internacionales, estamos de acuerdo en que el abuso a menores online es inaceptable. Estamos de acuerdo en que tenemos que colaborar para ponerle fin. Sin embargo, sabemos que hará falta un cambio radical en nuestra respuesta global.

2 Se debe priorizar la prevención como respuesta. En demasiadas ocasiones, se espera a que el abuso tenga lugar para actuar. Es esencial que haya una respuesta judicial y policial rotunda, pero una estrategia realmente sostenible pasa por prevenir activamente el abuso. Esto va más allá de favorecer la seguridad online de los niños, no se trata únicamente de «seguridad por diseño» y otras iniciativas que dificulten que los agresores se aprovechen de los servicios de internet, es mucho más que disuadir a los potenciales agresores. La prevención es todo esto, pero también mucho más. Tenemos que asegurarnos de crear entornos digitales seguros donde los niños puedan desarrollar todo su potencial. De momento, se está llevando a cabo un trabajo prometedor, pero nos hace falta más apoyo.

3 Hay esperanza. Durante la última década, la explotación sexual infantil y el abuso en internet han escalado posiciones en la agenda global. Se han implicado más países, empresas y organizaciones de la sociedad civil para abordar este delito. La tecnología de seguridad online está más avanzada y es más accesible que nunca, y los gobiernos están definiendo las responsabilidades de los proveedores de servicios de internet en la prevención y el tratamiento del abuso sexual infantil para que tomen medidas al respecto. El cambio puede ser más lento de lo que nos gustaría, pero se está produciendo. Nuestra función como Alianza es favorecer estos brotes verdes y ayudarlos a crecer.

Por último, nos gustaría dar las gracias a PA Consulting, a Crisp, a Economist Impact y al Comité Directivo dedicado al proyecto, así como a los que colaboran con nuestros miembros y a muchos otros, por hacer posible este documento. Sus ideas, planteamientos y compromiso han sido de un valor incalculable. Consideramos que el futuro de las evaluaciones de la amenaza global contará la historia de nuestra colaboración y, con creatividad, solucionaremos el problema y lograremos que los niños y las niñas de todo el mundo puedan disfrutar de los beneficios del entorno digital sin el riesgo de la explotación y el abuso sexual.

Iain Drennan
Director ejecutivo
Alianza Global WeProtect

Ernie Allen
Presidente
Alianza Global WeProtect

02

Resumen ejecutivo

Los menores de hoy en día se enfrentan a la amenaza constante de la explotación y el abuso sexual infantil en internet.

Nuestra respuesta global a este delito necesita un nuevo enfoque, de lo contrario más niños y niñas seguirán en peligro y sufrirán el trauma del abuso.

La mejor oportunidad para el cambio es aumentar la seguridad online de los niños y las niñas y minimizar las oportunidades para los agresores.

De acuerdo con las evaluaciones de la amenaza global anteriores, este informe revela que la explotación y el abuso sexual infantil sigue proliferando. **Muchas de las tendencias emergentes amenazan con incrementar aún más el volumen y la complejidad de los casos**, agravando los retos de quienes trabajamos para reducir el peligro y los daños.

Este informe también resalta las oportunidades de mejorar la respuesta, aprovechando un enfoque estratificado. Las autoridades, organizaciones de la sociedad civil, la industria tecnológica y las fuerzas de seguridad tenemos todos un papel que desempeñar.

Figura 1: El alcance del desafío.

El alcance del desafío

En 2020, **se intercambiaron 1 038 268** archivos multimedia individuales a través de la plataforma de clasificación y recopilación de material sobre abuso sexual infantil de INHOPE.[1]

En mayo de 2021, la Europol desmanteló una página web de abuso sexual infantil de la Dark Web con más de **400 000** suscriptores.[2]

Hay más de **3 000 000** de cuentas registradas en las 10 páginas más dañinas sobre abuso sexual infantil de la Dark Web.[3]

Por término medio, 30 analistas del Centro Nacional para Niños Desaparecidos y Explotados (NCMEC) procesan cada día **60 000** denuncias en línea de abuso sexual infantil a través de la CyberTipline.[4]

Al describir la rápida diversificación de los daños asociados a la explotación y el abuso sexual infantil, también consideramos las causas fundamentales de esta amenaza. En la actualidad, la tecnología está integrada en todos los aspectos de nuestra vida. Sin embargo, seguimos haciendo una falsa diferenciación en el tratamiento del abuso «en internet» (en contraposición a «en persona»), tal y como demuestran las penas más bajas por agresiones «en internet».[5] Esto pone de relieve hasta qué punto nuestra respuesta para gestionar este peligro ha fracasado.

Desde la Evaluación de la amenaza global de 2019, la naturaleza de los daños ha seguido ampliándose y diversificándose.

En los últimos dos años, la incidencia de las denuncias de explotación y abuso sexual infantil en internet ha alcanzado sus niveles más altos. Las pruebas indican que ha habido un aumento de:

- La incidencia de captación por internet.[6] [7]
- El volumen de material de abuso sexual infantil disponible en internet.[8]
- La difusión y distribución de material de abuso sexual infantil.[9]
- Streaming en directo de pago.[10]

La escala y el ritmo de este cambio no tiene precedentes, tal y como ilustran los datos del Centro Nacional para Niños Desaparecidos y Explotados de Estados Unidos (NCMEC) y la Internet Watch Foundation (IWF).

+100 %

Aumento de las denuncias por explotación sexual en internet, (Centro Nacional para Niños Desaparecidos y Explotados, NCMEC) [11]

De 2019 a 2020.

77 %

Incremento de material sexual infantil «autogenerado», (IWF) [12]

De 2019 a 2020.

La pandemia de la COVID-19 es sin lugar a dudas uno de los factores que ha contribuido al repunte de la explotación y el abuso sexual infantil en internet (véase el capítulo Tema: *COVID-19*). El aumento de los materiales sexuales «autogenerados» por menores es otra tendencia que representa un desafío en la actualidad.

El incremento de las denuncias no tiene por qué corresponderse con un incremento *proporcional* de las agresiones: algunas pueden deberse al aumento de la concienciación pública y de una detección más proactiva por parte de los proveedores de servicios de internet. No obstante, los niveles de abuso pueden ser mayores de lo que los datos disponibles sugieren:

1 La explotación y el abuso sexual infantil es un delito con una tasa de denuncia baja.[13] En una encuesta llevada a cabo por Economist Impact, el 54 % de los participantes dijeron haber sufrido daños sexuales por internet, entre los que se incluyen recibir contenido sexual explícito o solicitudes para hacer algo con lo que no se sentían cómodos.

   Y hay relativamente menos datos con respecto a la dimensión del problema en los países del Sur Global (véase Glosario de términos). Es muy probable que la tasa estimada de abuso y explotación deba revisarse al alza conforme se aborde esta ausencia de testimonios.

2 Aunque la mayor parte de las empresas que respondieron a la encuesta Alianza Global de WeProtect/Technology Coalition utilizan herramientas para detectar material de abuso sexual infantil (el 87 % y el 76 %, respectivamente, utilizan «hash-matching» de imagen y vídeo), solo el 37 % utiliza herramientas para detectar la captación por internet. Esto indica que un porcentaje significativo de estas actividades puede pasar inadvertido.[14]

   Incluso agresores con mínimas habilidades técnicas pueden evitar la detección mediante el uso de herramientas de servicios de mensajería encriptada y anonimato, de fácil acceso. En el otro extremo de la balanza, como ha apuntado Crisp, hay agresores de la Dark Web (véase Glosario de términos) que emplean técnicas avanzadas para encubrir sus actividades. La utilización de «servicios ocultos» para distribuir material de abuso sexual infantil se incrementó en un 155 % de 2019 a 2020.[15] Es probable que la detección sea baja en general, especialmente en aquellas jurisdicciones donde la capacidad de investigación digital es más limitada.

Las tendencias recientes tienen el potencial de alimentar el crecimiento sostenido de las agresiones:

- Las nuevas formas de monetizar el material de abuso sexual infantil y el aumento del contenido «autogenerado» por menores a cambio de dinero son factores que refuerzan la comercialización del abuso.
- El aumento del contenido «autogenerado» por menores presenta desafíos muy complejos para los legisladores.
- Los agresores están diversificando sus métodos de producción, por ejemplo coaccionando a los niños para que lleven a cabo actos sexuales y los graben («capping», en inglés). El centro australiano para luchar contra la explotación infantil (Australian Center to Counter Child Exploitation) reporta que el «capping» representa aproximadamente el 60 o el 70 % de las derivaciones a su unidad de identificación de víctimas.[16]

Este informe ayuda a formar una imagen más precisa del comportamiento de los agresores. Las pruebas no confirman el estereotipo que prevalece, el del agresor desconocido. El abuso sexual infantil a menudo lo perpetran familiares,[17] [18] [19] [20] y hay indicadores que señalan que esta situación ha empeorado con las restricciones de la COVID-19. Además, aunque algunos agresores se mueven por un interés sexual hacia los menores, este no es el único motivo que les lleva a actuar. Según la Fundación Lucy Faithfull, solo el 15 o el 20 % de los agresores con los que trabajan actualmente son pedófilos, «en el sentido de que se sienten atraídos sexualmente por niños y niñas preadolescentes».[21] En consecuencia, debemos tener más información sobre los distintos motivos que provocan una agresión para que, en el futuro, la disuasión y la prevención del abuso estén bien fundamentadas.

Debemos tener más información sobre los distintos motivos que provocan una agresión para que, en el futuro, la disuasión y la prevención del abuso estén bien fundamentadas.

Esta Evaluación de la amenaza global destaca las principales áreas de interés y las oportunidades emergentes para detener el aumento de la explotación y el abuso sexual infantil en internet.

La Estrategia Global de Respuesta de la Alianza Global de WeProtect (GSR, por sus siglas en inglés) proporciona una estrategia exhaustiva para acabar con la explotación y el abuso sexual infantil en internet.[22]

Esta Evaluación de la amenaza global identifica cuatro áreas de interés dentro del marco de respuesta:

Área de interés recomendada/ oportunidad:	Regulación en internet
Categoría de GSR:	Normativa/legislación

En algunos países, la respuesta legislativa está evolucionando para que la responsabilidad legal recaiga en los proveedores de servicios de internet.

La regulación de internet tiene el potencial de lograr que los entornos virtuales sean seguros para los menores. Son necesarios unos marcos legales de apoyo maduros y un buen asesoramiento para garantizar los resultados adecuados.

Área de interés recomendada/ oportunidad:	Fomento de la capacidad de las fuerzas de seguridad
Categoría de GSR:	Justicia penal

Mientras que algunas naciones disponen de una respuesta avanzada de las fuerzas de seguridad, muchas agencias policiales se enfrentan a retos que les impiden estar a la altura del problema. Muchas carecen de la financiación y los equipos necesarios y se ven desbordadas por la dimensión de las agresiones.

Los gobiernos deben aumentar su inversión en las fuerzas de seguridad para mejorar la vigilancia digital y permitir una mayor colaboración, con el objetivo de combatir las agresiones técnicamente sofisticadas y transfronterizas mediante la creación de unidades de investigación especializadas y multinacionales.

Área de interés recomendada/ oportunidad:	Cooperación voluntaria, transparencia y tecnologías de seguridad en internet
Categoría de GSR:	Tecnología

Unos potentes complementos de la regulación, como la cooperación voluntaria y la transparencia, permiten ofrecer la respuesta adecuada para afrontar esta amenaza que evoluciona a un ritmo muy rápido.

Desde la Evaluación de la amenaza global de 2019, se han tomado medidas significativas para que las plataformas cumplan con los principios de «seguridad por diseño» y estimulen la inversión global en tecnologías de seguridad en internet. Con los marcos de apoyo apropiados y una implementación más amplia, estas soluciones tienen el potencial de impulsar de manera significativa la respuesta general a esta amenaza.

Área de interés recomendada/ oportunidad:	Iniciativas sociales (varias)
Categoría de GSR:	Social

Es necesario centrarse nuevamente en un abanico de iniciativas sociales, como por ejemplo:

- Actuaciones destinadas a empoderar a los jóvenes para que desarrollen comportamientos sexuales saludables.
- Iniciativas que aborden las principales causas de la explotación y el abuso sexual infantil, como la actitud hacia las mujeres. Un informe de UNICEF descubrió que «el indicador más fuerte de la actitud de aceptación (del abuso sexual infantil) era... la idea de la dominancia del hombre sobre la mujer».[23]
- Actuación social con el fin de reducir los estigmas que impiden tanto el reconocimiento del abuso como la necesidad de ayuda de los agresores.

La explotación y el abuso sexual infantil en internet es uno de los problemas más urgentes y definitorios de nuestra generación.

Estas áreas de interés recomendadas tienen el potencial de impedir que la explotación y el abuso sexual infantil tengan lugar o se repitan. En términos generales, la prevención consiste en:

Reducir el riesgo de agresión, mediante la identificación de aquellas personas que pudieran cometer el delito, ayudándolas a afrontar comportamientos problemáticos y ofreciendo una buena gestión del riesgo de los agresores declarados culpables.

Reducir el peligro para los menores. Crear entornos más seguros para los niños. La responsabilidad de reducir el peligro de sufrir abusos no debería recaer en los menores.

Reducir el riesgo en general, neutralizando a los impulsores estructurales del abuso. La prevención efectiva abarca actuaciones sociales que aborden los motivos de la explotación y el abuso sexual infantil.

La prevención representa el mejor camino para garantizar la respuesta futura.

Esto debería coincidir con los servicios de primera línea, para continuar dando respuesta a cada caso, impidiendo las agresiones y apoyando a las víctimas y a los supervivientes. La clave radica en contemplar la inversión en prevención como una parte de la respuesta integral del sistema.

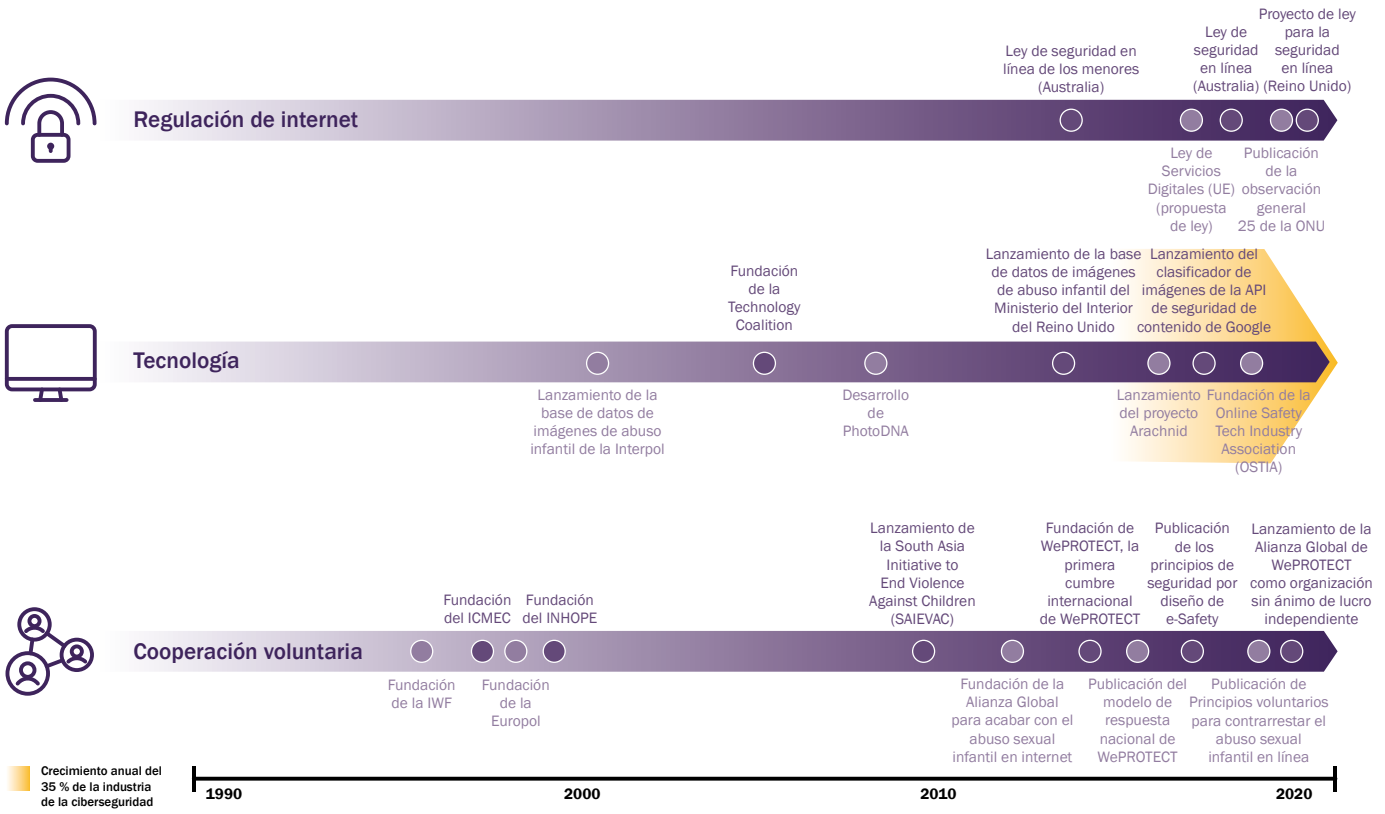
Juntos, tenemos el conocimiento, los medios y la oportunidad de pasar a la acción, de mejorar la respuesta mundial y de evitar que se haga daño a más niños y niñas.

La explotación y el abuso sexual infantil en internet es uno de los problemas más urgentes y definitorios de nuestra generación. Los países se enfrentan a retos distintos y se encuentran en diferentes fases de evolución en su respuesta ante esta amenaza. Algunos han experimentado un aumento acelerado del acceso a internet en los últimos años y su concienciación social de los peligros virtuales es todavía muy incipiente. En otros, ya hay una demanda social de acciones proactivas para afrontar el problema.

Las soluciones tecnológicas implementadas por los proveedores de servicios de internet, las estrategias legislativas locales que incentiven a las empresas multinacionales a mejorar su transparencia y la responsabilidad y la capacidad de respuesta general pueden comportar beneficios globales. La figura 2 muestra los avances clave que, en las últimas tres décadas, han impulsado la respuesta internacional ante la la explotación y el abuso sexual infantil en internet. Es probable que esta respuesta se sostenga en el tiempo, ya que los servicios de internet evolucionan y los consumidores de todo el mundo están cada vez más concienciados y son menos tolerantes con estos delitos.

Las recomendaciones clave que han surgido de la Evaluación de la amenaza global de este año se detallan en el Capítulo 7: *Recomendaciones.* Si bien las medidas deben diseñarse y priorizarse de acuerdo con el contexto local, se trata de acciones que todas las empresas, comunidades y gobiernos pueden emprender para mejorar su respuesta ante la explotación y el abuso sexual infantil en internet. Tenemos la responsabilidad de trabajar todos juntos para proteger a los menores. El año 2021 es una oportunidad sin precedentes para hacerlo, para mantener el impulso global y transformar nuestra respuesta colectiva.

Figura 2: Representación de algunos de los avances clave relacionados con los facilitadores de una mejor respuesta preventiva.



03 Introducción

DEFINICIONES CLAVE

El abuso sexual infantil consiste en «implicar a un niño o una niña [cualquier persona menor de 18 años] en actividades sexuales que él o ella no comprende del todo, para las que no está preparado/a a nivel de desarrollo y para las que no puede dar su consentimiento informado». Esta es la definición de abuso sexual infantil adoptada por la Alianza Global de WeProtect («the Alliance»), y se basa en las directrices de la Organización Mundial de la Salud[24] (OMS).

La explotación sexual infantil es una forma de abuso sexual que implica cualquier abuso o intento de abuso a una persona que se encuentra en una posición de vulnerabilidad, desequilibrio de poder o confianza. Esto incluye, aunque no se limita a, aprovecharse económica, social o políticamente de la explotación sexual de otra persona, lo cual puede cometerse de manera individual o en grupo. Lo que diferencia la explotación sexual infantil del abuso sexual infantil es la noción de intercambio que está presente en la explotación.[25] Ambos conceptos se solapan de manera significativa, porque la explotación es a menudo una característica del abuso y viceversa.[26]

La explotación y el abuso sexual infantil online se ven facilitados parcial o totalmente por la tecnología, es decir, por internet o por otras comunicaciones wifi. Este concepto también se conoce como OCSEA (por sus siglas en inglés) y como explotación y abuso sexual infantil facilitado por la tecnología.

Alcance

Este informe es la tercera Evaluación de la amenaza global que publica la Alianza para subrayar la dimensión y el alcance de la explotación y el abuso sexual infantil en internet con el objetivo de impulsar una respuesta.

La Evaluación de la amenaza global de 2019 concluía que las tendencias emergentes apuntaban a un «tsunami» de explotación y abuso sexual infantil online, «que dejaba a su paso un número cada vez mayor de víctimas y supervivientes".[27] Abordaba la amenaza desde cuatro perspectivas distintas: víctimas, agresores, tendencias tecnológicas y contexto socioeconómico.

Este informe adopta un enfoque «basado en los daños» para ofrecer un análisis más detallado sobre las diferencias entre las experiencias de víctimas y supervivientes, los métodos de los agresores, las tecnologías y los contextos socioeconómicos donde se producen los casos de explotación y abuso sexual infantil online. Esto se define en la Figura 3: Definiciones de los daños. Se trata de un enfoque que permite una evaluación más completa de los factores que intervienen en cada caso de daño, las oportunidades de actuación y las estrategias de respuesta.

Los daños analizados están interconectados entre ellos, tal y como se ilustra a partir de la Figura 4 en adelante.

También se analizan tres temas transversales:

- COVID-19.
- Tecnología.
- Regulación, cooperación voluntaria y transparencia.

NOTA SOBRE LA TERMINOLOGÍA DE LOS DAÑOS

Los «daños» (definidos en la Figura 3) son las descripciones de los abusos cometidos por los agresores. Estas descripciones no están formuladas para reflejar las experiencias de las víctimas y los supervivientes, sino que permiten analizar los factores vinculados a la agresión: sobre quién recae la responsabilidad principal de detener y prevenir dichas agresiones. Esta terminología no pretende bajo ningún concepto minimizar el impacto que tienen estos actos para las víctimas, cuyas consecuencias se analizan en función de cada daño en los estudios de caso correspondientes.

Figura 3: Definiciones de los daños

Daño	Definición
Captación de menores en internet con el propósito de explotación y abuso sexual	Un individuo establece una relación, se gana la confianza y conecta emocionalmente con un menor o un joven con el fin de manipularlo, explotarlo y abusar de él o ella (sirviéndose, parcial o completamente, de internet o de otras redes inalámbricas).[28] No siempre existe la intención de conocerse en persona. *Nota: algunas organizaciones usan el término alternativo «incitación en línea» (como define el NCMEC[29]) para referirse a este daño.*
Producción de material de abuso sexual infantil	Crear material de abuso sexual infantil *(véase Glosario de términos)* mediante imágenes, vídeos o grabaciones de audio en persona; crear contenido textual o material visual no fotográfico (por ejemplo, generado por ordenador); o manipular material de abuso sexual infantil ya existente para crear imágenes nuevas.
Buscar o visionar material de abuso sexual infantil	Buscar material de abuso sexual infantil en internet y verlo o intentar verlo.
Compartir y/o almacenar material de abuso sexual infantil	Descargar, almacenar, alojar, subir y compartir material de abuso sexual infantil.
Material sexual infantil «autogenerado»	Contenido de naturaleza sexual, incluyendo imágenes y vídeos de desnudos totales o parciales, que los propios menores han producido. El material sexual infantil «autogenerado» no es un daño por sí mismo (puede producirse de manera voluntaria y compartirse como parte de un intercambio apropiado para el desarrollo personal, por ejemplo si se da entre adolescentes). Sin embargo, hay situaciones en las que sí causa un perjuicio, principalmente: • Cuando se coacciona a un menor o adolescente para que produzca material sexual «autogenerado». • Cuando el material sexual «autogenerado» voluntariamente se comparte en contra de los deseos del adolescente. Este informe examina las características de la «autoproducción» perjudicial. Esta expresión aparecerá entrecomillada durante todo el informe para evitar dar a entender que existía una predisposición voluntaria del menor o joven implicado. Aunque el contenido pueda coincidir con la definición de material de abuso sexual infantil, es muy probable que la intención no sea clara por lo que no se puede dar por sentado en ninguna circunstancia.
Transmitir en directo explotación y abuso sexual infantil (streaming en directo)	Transmitir abusos y explotación sexual infantil en tiempo real a través de internet

Objetivos

El objetivo esencial de este informe es detallar la dimensión y el alcance de la explotación y el abuso sexual infantil en internet, con una evaluación que sea clara y comprensible para el público mundial. La finalidad es establecer una actuación basada en las pruebas, así como reconocer los significativos avances que se han logrado hasta la fecha y destacar las oportunidades de reducir el peligro para los menores, evitando el abuso antes de que se produzca.

Metodología

Este informe es un metaanálisis que sintetiza los hallazgos de múltiples estudios internacionales para incrementar su alcance global, construir una imagen holística de la amenaza y ofrecer una evaluación equilibrada allá donde la información esté incompleta o los expertos no se pongan de acuerdo (y disparar las alarmas cuando sea necesario).

Esta investigación secundaria se apoya en varios tipos de investigación primaria:

- Entrevistas con funcionarios de las fuerzas de seguridad, activistas de la seguridad infantil, académicos, representantes del sector tecnológico y otros expertos.
- Estudios de caso proporcionados por organizaciones miembro y sus afiliados.

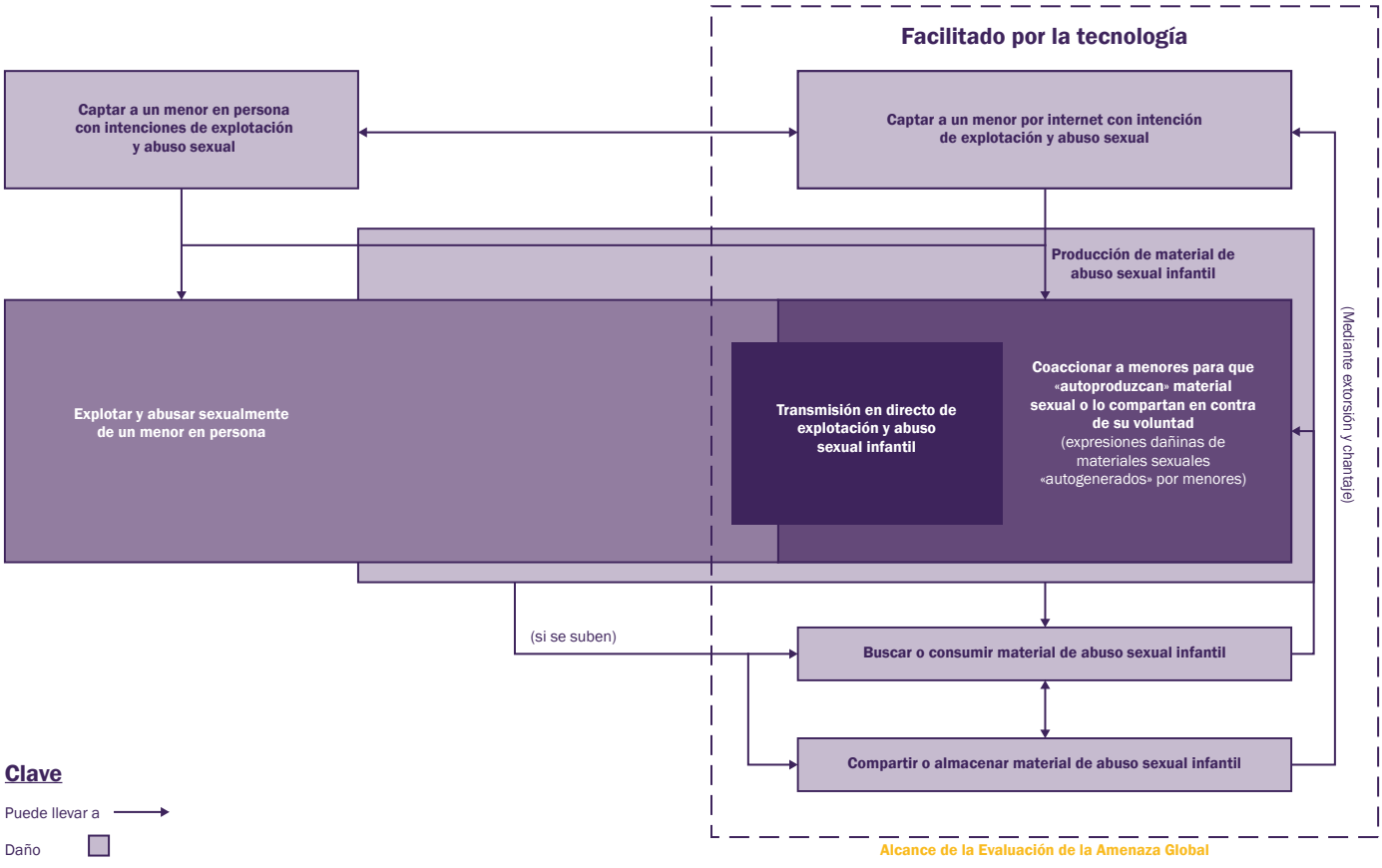
- Una encuesta anonimizada a 32 empresas tecnológicas a escala mundial llevada a cabo por la Alianza en colaboración con la Technology Coalition.
- Viñetas diseñadas por Crisp, uno de los principales proveedores de tecnologías de seguridad online. Estas viñetas se incluyen en la leyenda (ejemplo en la Figura 6).

El desarrollo de este informe lo lideró un Comité Directivo compuesto por 20 expertos de las fuerzas de seguridad, gobiernos, el sector tecnológico, organizaciones no gubernamentales e intergubernamentales (ONG y OIG) y la academia (véase la página 66).

CRISP

Crisp introduce en la agenda la gestión de riesgos de los agentes implicados y la competencia técnica de individuos y grupos para prevenir los daños, la desinformación y el abuso en internet. Su gráfica de gestión de los agentes implicados analiza las conversaciones digitales en tiempo real para sacar a la luz relaciones entre los agentes y sus grupos, con el fin de predecir los daños online lo antes posible. Crisp protege a más de dos mil millones de usuarios al día, lo que abarca aproximadamente a 450 millones de niños y niñas. **www.crispthinking.com**

Figura 4: Gráfico de los daños.



Enfoque de la investigación

58

Estudios de caso analizados

+230

Recursos consultados

55

Organizaciones consultadas

34

Entrevistas realizadas

04

ECONOMIST IMPACT

ECONOMIST IMPACT

Estimaciones de la exposición infantil a daños sexuales en internet y sus factores de riesgo

UN ESTUDIO GLOBAL DE LAS EXPERIENCIAS DE PERSONAS ENTRE 18 Y 20 AÑOS CUANDO ERAN MENORES

Internet, las redes sociales y otras aplicaciones y plataformas digitales pueden ser un arma de doble filo para los niños y los jóvenes. Representan un foro importante para socializar entre ellos, explorar su sexualidad de manera sana y forjar relaciones.[i] Sin embargo, al mismo tiempo, las tecnologías pueden utilizarse para facilitar la explotación y el abuso sexual infantil, tanto por parte de adultos (conocidos y desconocidos) como por otros compañeros, y pueden representar también una vía de acceso a contenido no adecuado para su edad.

Para ayudar a llenar el vacío de conocimiento global sobre la dimensión y el alcance potenciales de los daños sexuales en internet contra menores, Economist Impact y la Alianza Global de WeProtect llevaron a cabo un estudio que recopila testimonios de más de 5000 jóvenes de entre 18 y 20 años de 54 países de todo el mundo que tenían acceso a internet con regularidad cuando eran menores.[ii]

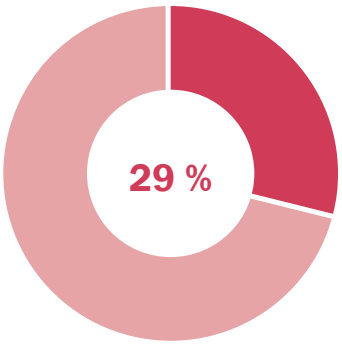
El cuestionario preguntaba a los participantes sobre su exposición a daños sexuales online y los factores de riesgo durante la infancia. Las preguntas se centraban en cuatro daños sexuales en internet.[iii] Estos daños son:

- Recibir contenido sexual explícito de un adulto o de alguien a quien no conocían antes de los 18 años.
- Recibir propuestas para mantener una relación sexual online explícita en secreto con un adulto o con un desconocido.
- Que un compañero, un adulto o un desconocido compartan imágenes suyas sexualmente explícitas sin su consentimiento.
- Recibir solicitudes de un compañero, un adulto o un desconocido para hacer algo sexualmente explícito en internet con lo que no se sentían cómodos.

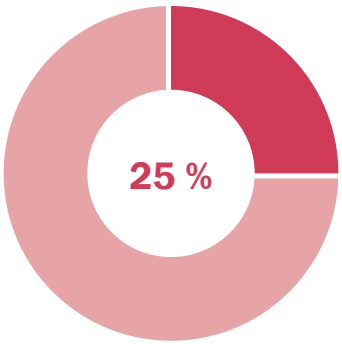
Los resultados clave de esta investigación se presentan a continuación. Los resultados completos y la metodología pueden consultarse en «*Estimates of childhood exposure to online sexual harms and their risk factors: A global study of childhood experiences of 18 to 20 year olds*» en la *página web de la Alianza Global de WeProtect.*

RESULTADOS CLAVE

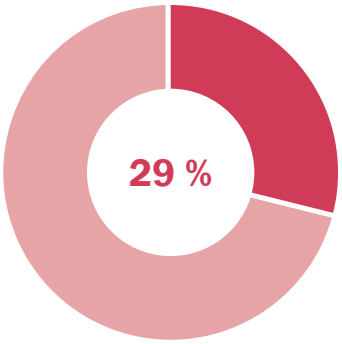
EL 54 % **de los encuestados ha sufrido al menos un daño sexual online durante su infancia.** [iv]



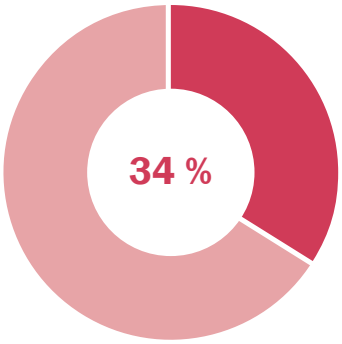
Recibieron contenido sexualmente explícito de un adulto conocido o desconocido antes de cumplir 18 años



Un adulto conocido o desconocido les pidió que mantuvieran en secreto parte de sus interacciones sexuales explícitas en línea

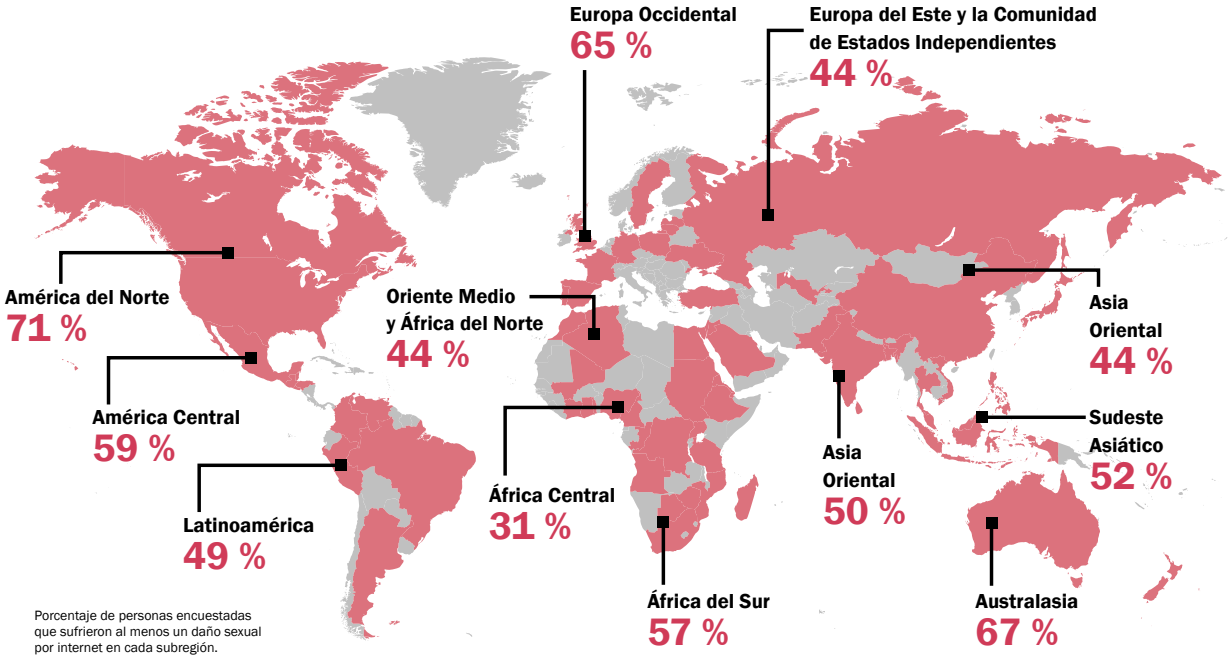


Alguien compartió imágenes o vídeos sexualmente explícitos de los menores sin permiso



Se les pidió que hicieran algo sexualmente explícito en línea que les resultaba incómodo

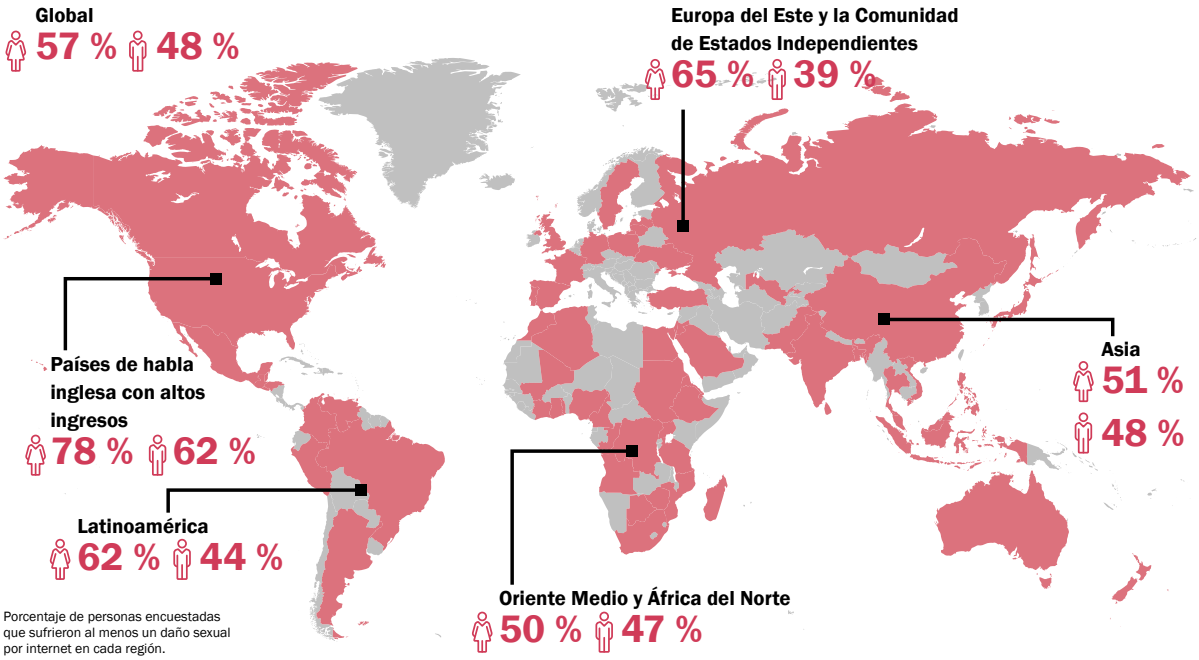
Los daños sexuales en internet a menores SUCEDEN EN TODOS LADOS...



Porcentaje de personas encuestadas que sufrieron al menos un daño sexual por internet en cada subregión.

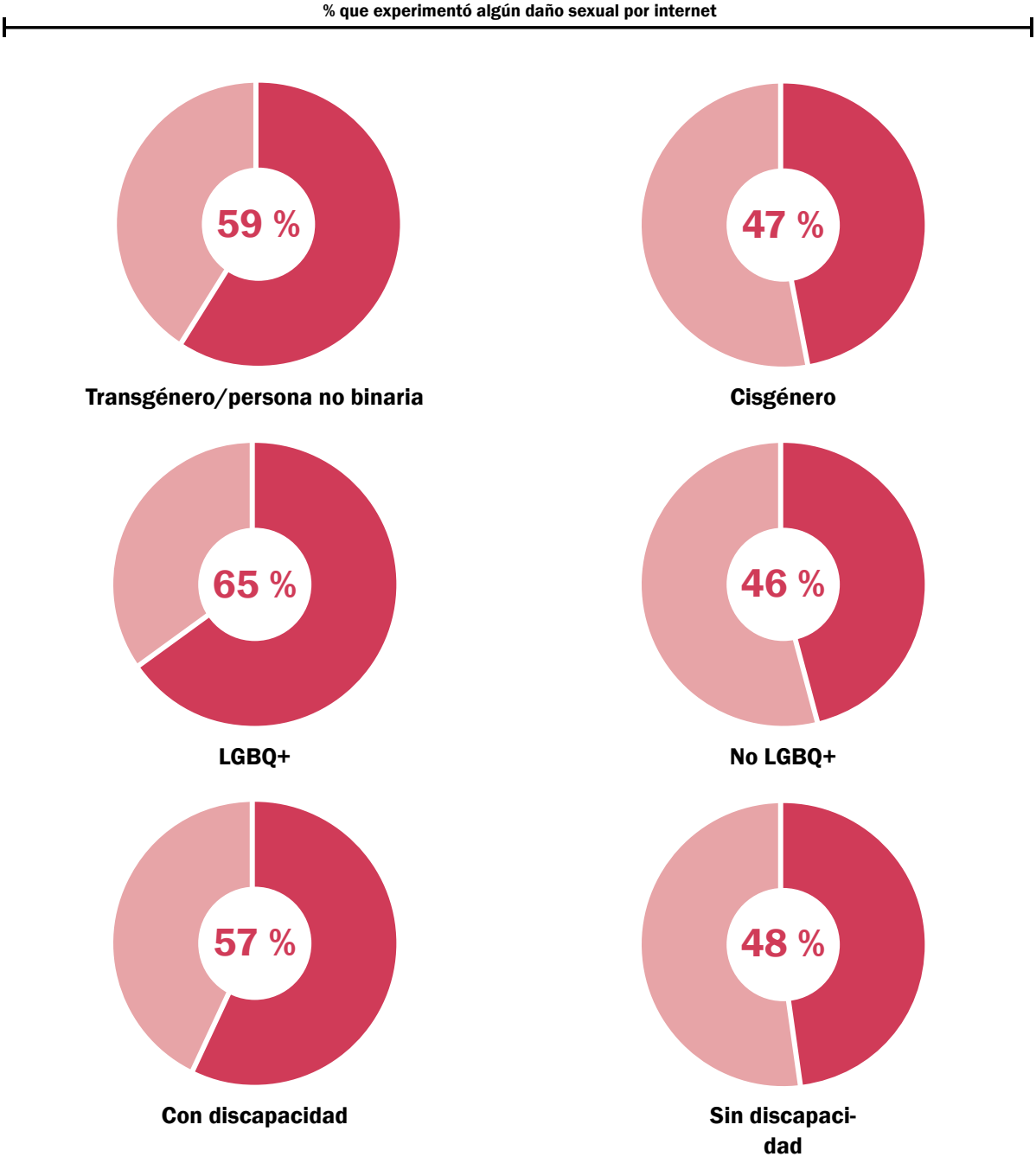
... y aunque las niñas están expuestas a un riesgo más alto,

CASI LA MITAD DE LOS NIÑOS ha sufrido al menos un daño sexual en internet.



Porcentaje de personas encuestadas que sufrieron al menos un daño sexual por internet en cada región.

Los encuestados que se identificaron como transgénero/no binario, LGBQ+ o discapacitados presentaron UN MAYOR PELIGRO de sufrir daños sexuales online durante la infancia.



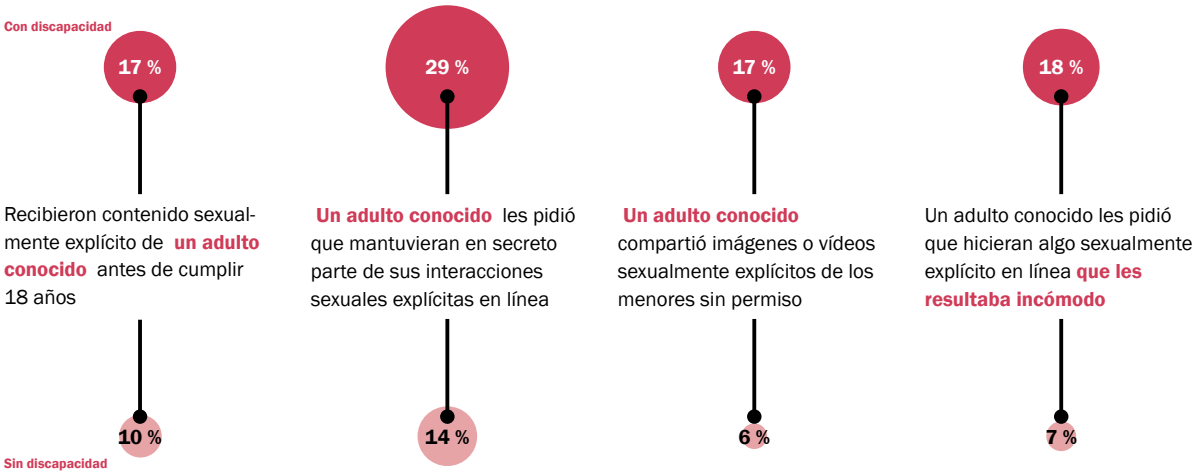
Porcentaje de personas encuestadas que sufrieron al menos un daño sexual por internet según se autoidentifiquen.

Se preguntó a los encuestados si se autoidentificaban como transgénero/persona no binaria, LGBQ+ o persona con discapacidad. Los datos de este gráfico se han sacado de un análisis que desglosó la muestra según esas respuestas. El número de personas encuestadas que se definieron con estas identidades en cada región por separado es demasiado reducido para llevar a cabo un análisis preciso de las variaciones geográficas en las experiencias de estos grupos.

Los encuestados que se identificaron como discapacitados presentaron

UN MAYOR PELIGRO

de convertirse en blanco de los ataques de un adulto conocido.



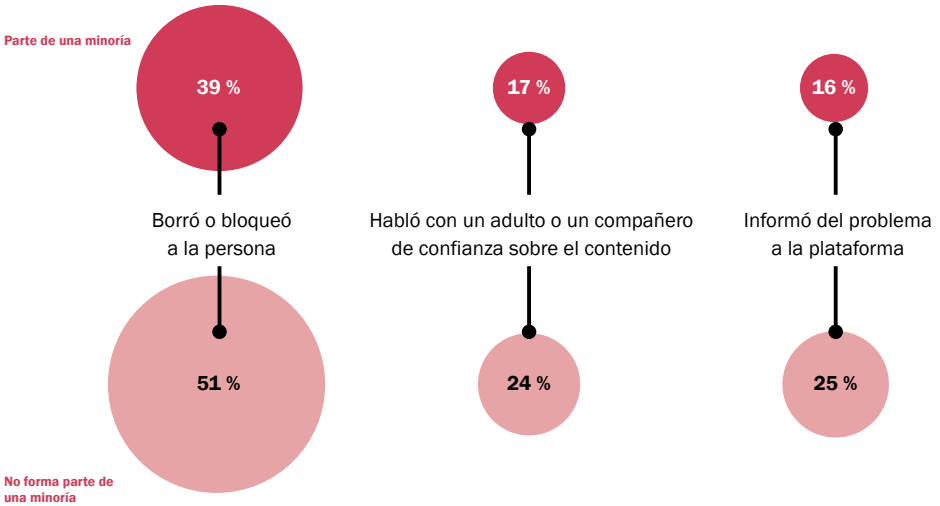
Porcentaje de personas encuestadas que sufrieron un daño sexual en línea por parte de un adulto que conocían (con y sin discapacidad).

Se considera una persona con discapacidad aquella que presenta una deficiencia o enfermedad (física o mental) que afecta su capacidad para llevar a cabo actividades cotidianas.

Los encuestados que se identificaron como racializados o minorías étnicas presentaron

UNA MENOR POSIBILIDAD

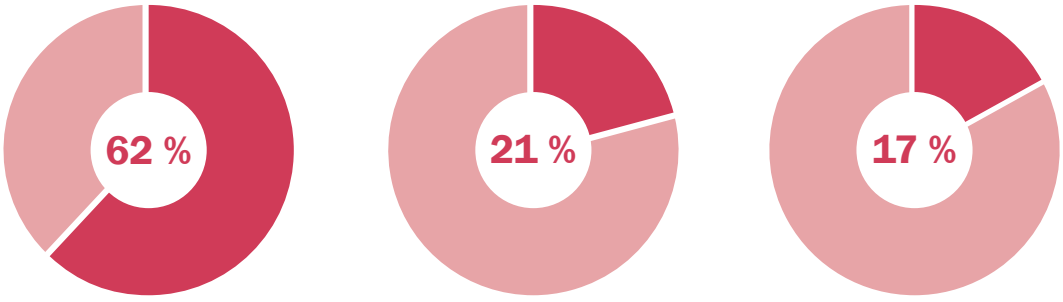
de tomar medidas en caso de que un adulto conocido o un desconocido intentase enviarles contenido sexual explícito.



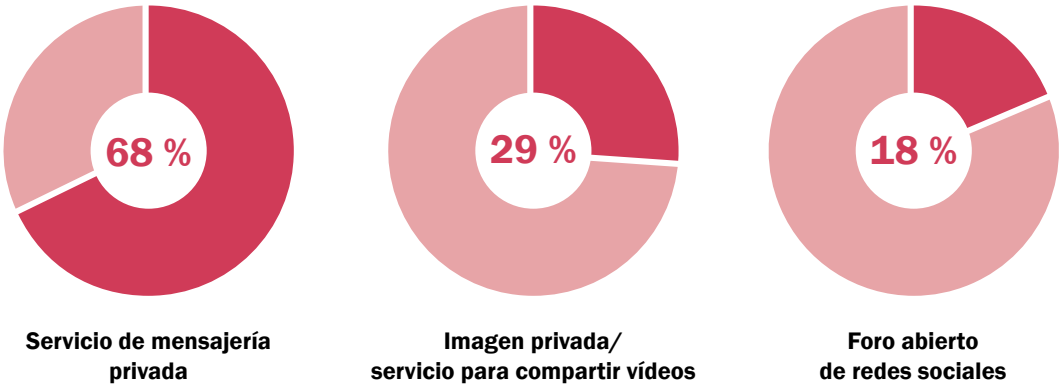
Porcentaje de encuestados que llevaron a cabo una determinada acción (formen parte o no de una minoría). Una minoría se define como una raza, nacionalidad o etnia diferente a la de la mayoría de las personas que viven en el país de la persona encuestada.

DOS TERCIOS **de los encuestados que recibieron material sexual explícito durante la infancia lo recibieron mediante un servicio privado de mensajería, generalmente a través de su dispositivo móvil personal.**

Dispositivos en los que la persona encuestada recibió el contenido



Plataformas donde la persona encuestada recibió el contenido



RESULTADOS CLAVE

La dimensión y el alcance de los daños sexuales en internet contra menores de edad hoy en día probablemente sea diferente. Las implicaciones éticas de encuestar a menores a través de una herramienta basada en internet nos ha impedido recopilar datos de participantes menores de 18.

¿Por qué los niveles son probablemente distintos hoy en día?

- El rápido aumento del uso de internet entre personas de todas las edades implica que más menores lo utilizan con regularidad y a edades cada vez más tempranas.
- Un mayor porcentaje de niños y niñas de todas las edades tiene acceso tanto a móviles propios como a móviles de adultos o de otros compañeros y utiliza un abanico más amplio de plataformas.
- La COVID-19 ha provocado que los niños pasen más tiempo conectados y que gente de todo el mundo se sienta más sola.
- Las plataformas digitales se han convertido para los menores en una nueva forma de explorar su sexualidad con sus iguales, pero estos espacios para el descubrimiento también abren la puerta a nuevas formas de abuso y explotación.

Debemos profundizar más en nuestras investigaciones para comprender hasta qué punto el dinámico panorama de internet, las redes sociales y las plataformas digitales están cambiando la forma en que los menores interactúan y lo que esto implica para su seguridad frente a las amenazas en línea. Nuestro estudio es un primer paso para describir la imagen general del problema e identificar qué investigaciones futuras tendrán mayor utilidad.

METODOLOGÍA

Este estudio se basa en datos recopilados a través de una encuesta online realizada a 5302 personas de entre 18 y 20 años que tenían acceso regular a internet* durante la infancia (cuando eran menores de 18 años) y que se llevó a cabo entre mayo y junio de 2021.

La encuesta se distribuyó en 21 idiomas en 54 países, que se agruparon en 12 subregiones** con un mínimo de 390 participantes cada una. La muestra global y la agrupación regional se usaron para el análisis del sexo y otras características demográficas de las experiencias.

Notas:

*El «acceso regular a internet» se define como alguien que usa internet personalmente (no que ve como otros lo usan) al menos una vez a la semana.

**Australasia, África Central, América Central, Asia Oriental, Europa del Este y la Comunidad de Estados Independientes, Oriente Medio y África del Norte, América del Norte, Sudeste Asiático, África del Sur, América del Sur, Asia Oriental y Europa Occidental.

NOTAS

i De acuerdo con la definición de «menor» de la Convención sobre los Derechos del Niño, «menor» en este estudio hace referencia a cualquier persona que tenga menos de 18 años.

ii El «acceso regular a internet» se define como un uso personal de internet (no ver cómo otros lo usan) al menos una vez a la semana. «Menor» se define como una persona de menos de 18 años. Para un análisis completo sobre cómo este método de muestreo puede afectar a los resultados, consultar el artículo completo.

iii Un conjunto de conductas dañinas consideradas factores de riesgo para la explotación y el abuso sexual infantil en internet, potencial o real.

iv El 54 % de los encuestados ha sufrido uno o más de los daños sexuales sobre los que se preguntó en esta encuesta.

05

Temas

COVID-19

La COVID-19 propició las condiciones ideales para la formación de una «tormenta perfecta» que alimentó el aumento de la explotación y el abuso sexual infantil en todo el mundo.[30]

Puede que pasen años antes de que sepamos la dimensión real de los abusos relacionados con la pandemia. Mientras tanto, los servicios de primera línea necesitan ayuda urgente para asistir a las nuevas víctimas ocasionadas por la COVID-19, además de las que ya conocíamos.

Si bien los confinamientos pueden haber acelerado la posibilidad de nuevas agresiones, el impacto a largo plazo de esta pandemia amenaza con reforzar los impulsores de la comercialización del abuso.

Muchos países han denunciado un incremento de la explotación y el abuso sexual infantil durante la COVID-19 (véase Figura 5). La encuesta Netclean 2020 de las fuerzas de seguridad a escala mundial también apuntó a que las fuerzas de seguridad estaban de acuerdo en que habían incrementado las tentativas de contactar con menores, así como el volumen de material sexual infantil «autogenerado» y la actividad en la Dark Web.[31] Algunas agencias de seguridad anticipan que todavía aumentará más el volumen de material detectado a medida que los agentes se vayan reincorporando a sus puestos de trabajo.[32]

Abordar este problema requerirá de inversión gubernamental para reforzar la capacidad de los servicios de primera línea y la colaboración del sector, con el objetivo de reducir la acumulación de denuncias.

El verdadero impacto de la COVID-19 es difícil de dilucidar, principalmente porque el aumento de las denuncias durante la pandemia no es necesariamente indicativo de un aumento de las agresiones. Los cambios en las prácticas laborales, incluyendo la obligatoriedad del trabajo remoto, afectaron negativamente a algunas de las agencias informantes clave. En algunos casos, los analistas tuvieron más dificultades a la hora de evaluar informes o ejercer de moderadores según los estándares establecidos, lo que provocó un aumento de «falsos positivos».[33] También puede que la mayor concienciación sobre este problema esté contribuyendo al aumento sostenido observado en 2021, ya que los medios de comunicación y las agencias policiales siguen poniendo de manifiesto picos alarmantes en las tasas de abuso denunciado.

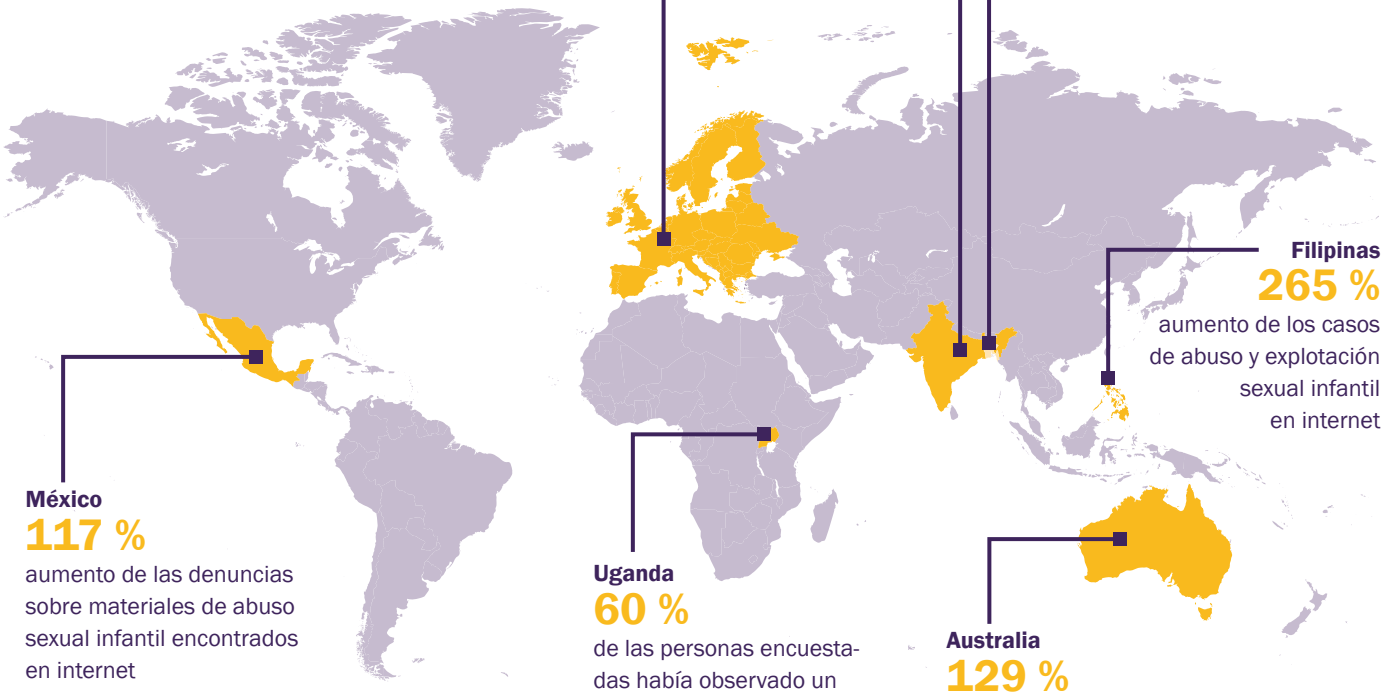
Figura 5: Aumento del abuso sexual infantil durante la COVID-19. [34 35 36 37 38 39 40]

NCMEC observó
un aumento del 106 %
de denuncias por sospecha de explotación sexual infantil en su CyberTipline global

Europa
50 %
aumento en algunos países del abuso sexual infantil en internet

India
95 %
aumento de las búsquedas por internet de material sobre abuso sexual infantil

Bangladés
40 %
aumento de las llamadas a teléfonos de asistencia para menores



Filipinas
265 %
aumento de los casos de abuso y explotación sexual infantil en internet

México
117 %
aumento de las denuncias sobre materiales de abuso sexual infantil encontrados en internet

Uganda
60 %
de las personas encuestadas habían observado un aumento de la violencia sexual contra menores de edad desde el principio del confinamiento

Australia
129 %
aumento de las denuncias sobre materiales de abuso sexual infantil encontrados en internet

En septiembre de 2020, el cierre de los colegios afectó a 827 millones de estudiantes en todo el mundo.[41]

Durante la pandemia, algunas iniciativas de prevención para agresores recibieron una mayor demanda de servicios de autoayuda.[42] [43] Al principio, surgió la preocupación de que las personas con el potencial de cometer abusos pudieran correr un mayor riesgo debido al «estrés, a la falta de asistencia social positiva, a las limitaciones para buscar ayuda y al aumento de la oportunidad» derivados de los confinamientos, «todo ello asociado con el peligro de cometer una agresión».[44] El aumento de la demanda de estrategias de autoayuda sugiere que dicha preocupación se ha confirmado hasta cierto punto y que los confinamientos pueden haber contribuido a reforzar las posibilidades de cometer una agresión para ciertos individuos.

Para muchos agresores declarados, los confinamientos proporcionaron más oportunidades de contactar con menores (debido a la posibilidad de estar más conectados en casa, por el cierre de los colegios) y una mayor autonomía para establecer relaciones. En una encuesta global realizada a los agentes de primera línea implicados en la protección de menores, el 72,8 % dijo que había existido al menos cierto aumento de actividad en las comunidades de abuso online durante la pandemia.[45]

El uso de «servicios ocultos (páginas web alojadas en una red proxy para que no pueda trazarse su ubicación) también se vio incrementado, lo que sugiere que más agresores han aprendido a ocultar sus actividades.[46] Además, hubo un incremento del abuso online como una forma de agresión sustitutoria para aquellos individuos que, circunstancias de normalidad, podrían haber intentado abusar de menores en persona.[47] Esto es especialmente preocupante, dado que algunos menores ahora corren un mayor riesgo de abuso transmitido en directo debido a las dificultades económicas provocadas o empeoradas por la COVID-19. Como señaló ECPAT: «A medida que las familias pierden ingresos, especialmente en el Sur Global, pueden considerar la transmisión en directo como una oportunidad».[48] Esto se debe principalmente a que la pandemia ha aumentado la demanda de streaming en directo como alternativa al abuso «en persona».[49] En este sentido, la pandemia también amenaza con reforzar los impulsores de comercialización del abuso a largo plazo. Ya hay pruebas de que los menores están reaccionando a su disminución de ingresos con la «autoproducción» de material sexual a cambio dinero.[50]

> ***El Banco Mundial calcula que la pandemia dejará entre 88 y 115 millones de personas más en la pobreza extrema, provocando que esta cifra alcance los 150 millones en 2021.[51]***

Los confinamientos agudizaron muchos factores de riesgo de abuso. La intervención inmediata para activar los escasos servicios de primera línea será fundamental para poder asistir a más víctimas.

Sin duda, los confinamientos habrán reducido las probabilidades de que algunos menores sufran abusos fuera del hogar (como en ámbitos institucionales), sin embargo, para muchos otros, habrán creado o intensificado vulnerabilidades (tales como la soledad o trastornos de salud mental[52]); incrementado el tiempo que pasaban conectados[53] (y por tanto expuestos a los depredadores[54]) e impedido el acceso a redes de apoyo (como adultos de confianza o amigos) que normalmente les hubieran podido proteger.[55] Es probable que el peligro de sufrir abuso sexual online durante la pandemia haya sido mayor para los niños que experimentan una convergencia de estos factores de riesgo.

Como se señala en el capítulo de Daños: *Producir material de abuso sexual infantil,* un porcentaje significativo del abuso sexual infantil lo perpetra un familiar. Los confinamientos por la COVID-19 habrán provocado que muchos menores se vean atrapados en casa con sus agresores. El sufrimiento de estas víctimas puede haberse prolongado debido a la falta de acceso a los canales de denuncia habituales durante la pandemia. En Paraguay, las denuncias de abuso sexual infantil se redujeron al 50 % durante el confinamiento, para volver a incrementarse una vez se relajaron las medidas, presumiblemente porque las víctimas (y sus adultos de confianza, como profesores y profesionales de la salud) pudieron salir de casa para denunciar los delitos.[56] En Jamaica, la disminución de las denuncias oficiales se veían contradichas por el creciente número de llamadas a teléfonos de emergencia, lo que sugiere que los menores podrían no haber tenido acceso a los canales habituales de denuncia y que «el abuso se produce con mayor probabilidad en el hogar».[57] Australia registró un descenso en las denuncias de maltrato infantil durante la primera fase de la pandemia, para luego observar un repunte cuando se relajaron las medidas.[58]

En 2020, se interrumpieron los servicios de protección de menores por la pandemia en 104 países, lo que representa una población total de 1,8 mil millones de menores.[59] En muchas regiones, la capacidad de vigilancia también se vio comprometida. Según el informe de Netclean de 2020, la capacidad de las fuerzas de seguridad para investigar la explotación y el abuso sexual infantil disminuyó durante la pandemia.[60] La Interpol indicó que llegaron menos denuncias, hubo más problemas para avanzar en las investigaciones ya existentes y se redujo el uso de la Base de Datos Internacional sobre Explotación Sexual de Niños.[61]

A medida que los países han ido saliendo de los confinamientos, las víctimas han empezado a denunciar los abusos, y es probable que este aumento intensifique los retrasos existentes en los servicios de primera línea. Sin una intervención gubernamental inmediata, el efecto dominó de la COVID-19 podría prolongar el sufrimiento de estos menores y reducir la tasa de resolución de casos, sobre todo si muchos gobiernos de todo el mundo desvían fondos de los servicios públicos para estimular la recuperación económica tras la crisis sanitaria.[62] [63] Estas actuaciones debilitarían la respuesta inmediata a la amenaza y la posibilidad de una prevención significativa en el futuro. En los países de menor renta, la situación podría agravarse todavía más si otras naciones siguen el ejemplo del Reino Unido y reducen la ayuda oficial para el desarrollo (ODA, por sus siglas en inglés),[64] cambiando sus prioridades de gasto. El impacto de estos recortes podría tener efectos a largo plazo, en futuras crisis sanitarias, incluida la proliferación de la explotación y el abuso sexual infantil.

05
Temas

Tecnología

El ritmo del cambio tecnológico sigue dificultando la respuesta a la explotación y el abuso sexual infantil en internet.

Sin embargo, en los últimos años las tecnologías de seguridad online han avanzado significativamente. Si se adoptan de manera más amplia, estas herramientas y técnicas podrían hacer posible el cambio de rumbo en la respuesta a la amenaza global.

En 1995, menos del 1 % de la población mundial eran usuarios activos de internet.[65] Hoy, esa cifra ha aumentado hasta un 59,5 %.[66] La media global de las velocidades de descarga también se está incrementando[67] y se espera que el número de dispositivos móviles activos alcance los 17,62 mil millones en 2024, lo que supone un incremento de 3,7 mil millones de dispositivos si lo comparamos con los niveles de 2020.[68] Algunas partes del mundo experimentan estos cambios a un ritmo considerablemente acelerado, como es el caso del continente africano (véase Figura 6). Los menores de 18 años ahora suponen uno de cada tres usuarios de internet en todo el mundo.69

Figura 6: Uso de internet en África. [70 71 72]

FOCO DE ATENCIÓN:
Uso de internet en África

África Subsahariana 2020-2025:

130 000 000
de usuarios de internet nuevos

70 %
de aumento del uso de smartphones

20 %
en el número de usuarios de internet cada año

4G
el despliegue en todo el continente acercará rápidamente a millones de jóvenes a internet

Como se señala en el Comentario General de las Naciones Unidas número 25 (véase *Glosario de términos*), el entorno digital facilita el acceso a una serie de derechos de los menores, puesto que ahora más que nunca las funciones sociales se apoyan en las tecnologías digitales. Las oportunidades educativas de estas tecnologías tienen el potencial de ser especialmente transformadoras. El aumento del número de dispositivos móviles se considera una gran oportunidad para llegar a las niñas de todo el mundo, que representan «dos tercios de la población infantil mundial que no asiste a la escuela primaria».[73] Para los menores, las ventajas sociales de estar conectados son muy amplias. Según la encuesta de la UE Kids Online de 2020, la mayoría «dice que les resulta más sencillo ser ellos mismos online, al menos a veces».[74] Esto puede resultar especialmente transformador para aquellos jóvenes cuya libertad de expresión se ve limitada de algún modo (debido a discapacidades o por vivir en un contexto sociocultural restrictivo).[75]

Para algunos menores, las ventajas de estar conectados se ven contrarrestadas por los efectos negativos, las experiencias perjudiciales y el abuso sexual.

Existen pruebas que sugieren que, para algunos menores, su presencia online les expone a interacciones sexuales [76] e imágenes de contenido sexual.[77 78] Mientras que algunos menores (un poco mayores) pueden percibirlo como oportunidades positivas para explorar su identidad sexual, para otros, como niños más pequeños, es probable que el impacto en su desarrollo sea negativo.[79] Como se explica en el capítulo de Daños: *Buscar o visionar materiales de abuso sexual infantil* o una exposición habitual a la pornografía está relacionado con el desarrollo de comportamiento sexual perjudicial (véase *Glosario de términos*) en adolescentes.[80 81]

El estudio Economist Impact que se encargó junto con este informe concluyó que, de los encuestados que afirmaron que les habían mandado material sexualmente explícito, el 62 % lo había recibido en su dispositivo móvil. En muchos países, los smartphones son el medio preferido de los menores para conectarse a internet.[82 83]

El incremento del acceso a internet mediante dispositivos móviles conectados contribuye a aumentar la sensación de los menores de estar atrapados, puesto que sus agresores se infiltran en todos los aspectos de sus vidas y se acaban convirtiendo en víctimas de abusos.[84] La encuesta de Thorn de 2021 sobre la juventud de los Estados Unidos reveló que muchos menores responden a las interacciones sexuales perjudiciales online restándole importancia a sus efectos y no hablando de ellas, tácticas que tienden a magnificar o amplificar el daño causado.[85]

Hay indicios positivos de que los activistas, incluyendo los propios menores y jóvenes, están comenzando a acusar la aparente «normalización» del abuso sexual. En el Reino Unido, a principios de 2021, los casos de «cultura de la violación» que emergieron en las escuelas inspiraron a los adolescentes a compartir sus experiencias de acoso sexual como parte del movimiento «Todos están invitados» (Everyone's Invited). Desde entonces, se han acumulado más de 50 000 testimonios, y en Estados Unidos ha ocurrido una reacción similar.[86] [87] [88] Si bien internet ha desempeñado un papel esencial en el incremento de la explotación y el abuso sexual, también brinda a los jóvenes una plataforma desde la cual exigir cambios.[89]

Muchas fuerzas policiales carecen de la capacidad necesaria para investigar la explotación y el abuso sexual infantil online.

Incluso agresores con mínimos conocimientos técnicos pueden complicar la detección de sus delitos con herramientas de anonimato como Tor y Virtual Private Networks (VPN), que ahora son de uso habitual y están incorporadas por defecto a algunos navegadores.[90] También el uso del cifrado o encriptación está cada vez más extendido (véase capítulo Daños: *Regulación, cooperación voluntaria y transparencia.*). En general, esto supone una traba significativa para investigar los delitos provocada por las tecnologías de fácil acceso. Los agresores en la Dark Web suponen un desafío distinto, pues los que están más avanzados tecnológicamente explotan todas las oportunidades que les ofrecen las nuevas herramientas para cometer sus agresiones y evitar ser detectados.

Se espera que la cifra de dispositivos móviles activos en el mundo alcance

17,62 MIL MILLONES

en 2024

El estudio Economist Impact que se encargó junto con este informe concluyó que, de los encuestados que afirmaron que les habían mandado material sexualmente explícito,

EL 62 %

lo había recibido en su dispositivo móvil.

Los agresores de la Dark Web buscan nuevas herramientas que les ayuden a cometer la explotación.

Los agresores en la Dark Web se están volviendo cada vez más sofisticados y se sienten cada vez más cómodos con las últimas tecnologías, que utilizan para crear y distribuir material de abuso sexual infantil. Para complicar las cosas, una generación emergente de agresores en la Dark Web con conocimientos tecnológicos está empleando y fomentando técnicas y servicios de seguridad avanzados para impedir ser detectados.

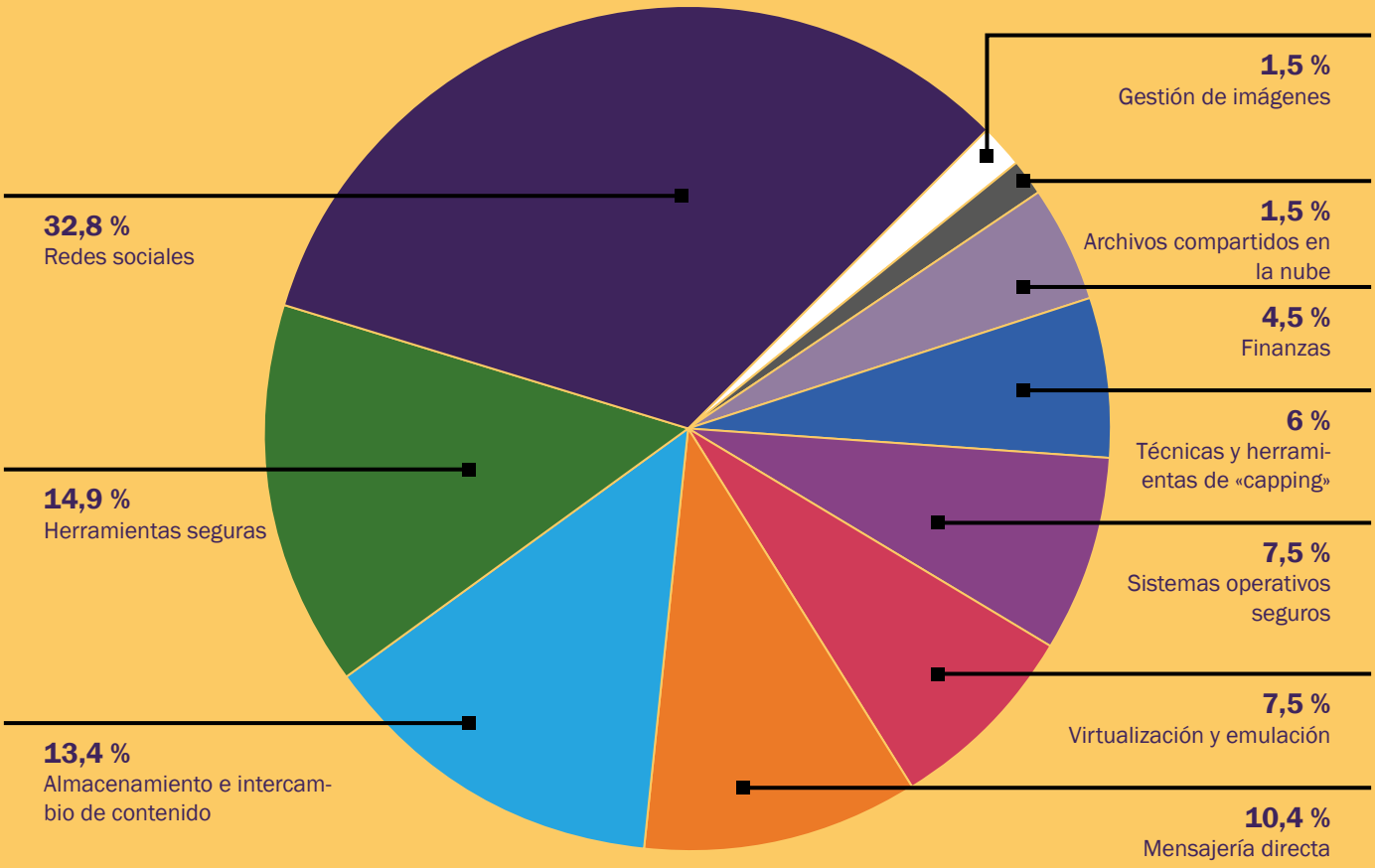
Lo que hace aún más difícil para las fuerzas del orden investigar y procesar estos delitos es que los agresores están continuamente buscando opciones y soluciones nuevas que faciliten su explotación a los menores. Resulta devastador que su caja de herramientas evolucione y se amplíe al mismo ritmo en que lo hacen las nuevas tecnologías online.

Los analistas de Crisp calcularon el interés del agresor en temas tecnológicos examinando detenidamente las conversaciones mantenidas en diversos foros de agresores en la Dark Web en febrero de 2021.

De los «temas de tecnología» discutidos en estos foros, casi un tercio estaban relacionados con las plataformas donde los agresores interactúan con menores o con usuarios vulnerables, junto con discusiones más amplias sobre «tradecraft» (véase *Glosario de términos*). Más preocupante aún es el hecho de que más de dos tercios de esas conversaciones giraban en torno a las herramientas técnicas de mensajería directa, al intercambio de fondos o en cómo adquirir y almacenar de manera segura contenido, tanto de manera local como en la nube, y también sobre las herramientas que pueden hacer más difícil la tarea de identificar y procesar a los agresores.

Para definiciones sobre temas tecnológicos, consulte *Glosario de términos.*

Figura 7: Temas sobre tecnología discutidos en los foros de agresores de la Dark Web.



Al igual que otros delitos habilitados por internet, la explotación y el abuso sexual infantil online supone un gran desafío para muchas agencias policiales. Deben hacer frente a una capacidad digital limitada, un personal insuficientemente cualificado y una carencia de herramientas para agilizar el proceso de investigación. Sri Lanka comunicó recientemente su falta de personal técnico en las unidades de investigación,[91] mientras que la policía tailandesa ha declarado que necesita más efectivos con formación en investigación sobre la Dark Web y pagos en criptomonedas relacionados con abusos.[92]

Algunos países incluyen los delitos de explotación y abuso sexual infantil en internet en el ámbito de las unidades de delitos cibernéticos, donde estos casos deben competir con delitos de gran volumen, a menudo complejos, como el fraude. En algunos lugares, la cooperación con proveedores de servicios de internet también se queda atrás. Según la Interpol, el incumplimiento de las órdenes policiales es un gran desafío a nivel mundial[93] Las discrepancias en las políticas de conservación de datos de las empresas también pueden complicar la recopilación de pruebas.

La causa de muchos de estos problemas es la subfinanciación crónica de la vigilancia policial. Es necesaria una inversión urgente para reforzar la capacidad de investigación de las fuerzas de seguridad de todo el mundo y desarrollar mecanismos de colaboración para enfrentarse de manera efectiva a las agresiones transfronterizas y tecnológicamente sofisticadas.[94]

Algunos marcos legales siguen sin ser adecuados para la era digital. Se corre el riesgo de que estas brechas creen una sensación de impunidad en torno al abuso sexual infantil online.

En las últimas décadas, ha habido una mayor consistencia en la forma de abordar el problema del abuso sexual infantil, catalizada por instrumentos internacionales tales como el Convenio de Lanzarote (véase *Glosario de términos*). Sin embargo, siguen existiendo un vacío. Desde 2006, el Centro Internacional para Niños Desaparecidos y Explotados realiza regularmente un informe sobre los materiales de abuso sexual infantil en los 196 países miembros de la Interpol. La primera encuesta reveló que la legislación era «suficiente» solo en 27 países. Asimismo, la última edición (de 2018) puso de manifiesto que 71 países seguían sin definir «material de abuso sexual infantil», mientras que solo 32 países obligaban a los proveedores de servicios de internet a denunciar estos delitos.[95]

El papel de la tecnología en los delitos de explotación y abuso sexual infantil arroja una cantidad ingente de desafíos específicos para la legislación.

Las discrepancias entre el tratamiento del abuso online y el abuso en persona son habituales y constituyen una de las razones por las que los agresores de internet operan con aparente impunidad. El análisis de un caso llevado a cabo por la organización benéfica International Justice Mission (IJM) puso de relieve que solo en Escocia, Canadá, Australia y Suecia se penaliza las transmisiones en directo del abuso «del mismo modo que las agresiones de contacto».[96] Muchos países no han definido su posición legal en cuanto al uso de material de abuso sexual infantil no pornográfico.[97] [98] Las repercusiones de este vacío pueden aumentar a medida que los agresores vayan diversificando sus métodos mediante nuevas tecnologías, como Imagen Generada por Ordenador (CGI, por sus siglas en inglés) (véase capítulo Daños: *Producir material de abuso sexual infantil*). Debido a estas limitaciones, existe el peligro de generar una sensación de impunidad que anime a los agresores a actuar, puesto que se ha observado que estos se dirigen más libremente a los niños de jurisdicciones con legislaciones más laxas.[99]

La buena noticia es que ahora existe tecnología para proteger a los niños y atrapar a los agresores. Ampliamente aceptadas, las herramientas y técnicas de seguridad online tienen el potencial de transformar la respuesta a la amenaza global.

En los últimos años, se han realizado avances significativos en tecnologías de seguridad online. Algunos ejemplos clave son:

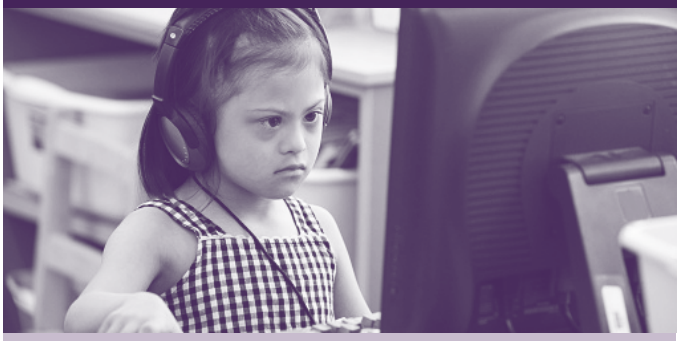
- Herramientas de detección de captación del tipo «seguridad por diseño» que reducen la oportunidad del agresor y fomentan comportamientos online seguros (véase capítulo Daños: *Captación de menores en internet con el propósito de explotación y abuso sexual*).
- Mecanismos de disuasión para impedir la agresión (véase capítulo Daños: *Buscar y consumir material de abuso sexual infantil*).
- Soluciones de «Hash-matching» (véase *Glosario de términos*) para detectar y eliminar material de abuso sexual infantil «conocido» y clasificadores utilizados para detectar material recién generado (véase capítulo Daños: *Compartir y/o almacenar material de abuso sexual infantil*).

El sector de tecnologías de seguridad, en constante expansión, ha desempeñado un papel fundamental en el desarrollo de muchas de estas tecnologías. Solo en el Reino Unido, donde las empresas de Safety Tech poseen colectivamente el 25 % de la cuota de mercado global, el sector ha experimentado una tasa de crecimiento anual estimada del 35 % desde 2016[100] y está en camino de conseguir unos ingresos brutos de mil millones de libras esterlinas para 2024 (véase Figura 8 a continuación).[101] Más de la mitad (52 %) de las empresas del Reino Unido tienen una presencia internacional consolidada.[102]

Al reducir las oportunidades del agresor y mejorar la protección de los menores, las tecnologías de seguridad online pueden fomentar una respuesta global a la explotación y el abuso sexual infantil en internet. Esto sin tener en cuenta el posible impacto de las herramientas y las técnicas que están todavía en vías de desarrollo, por ejemplo:

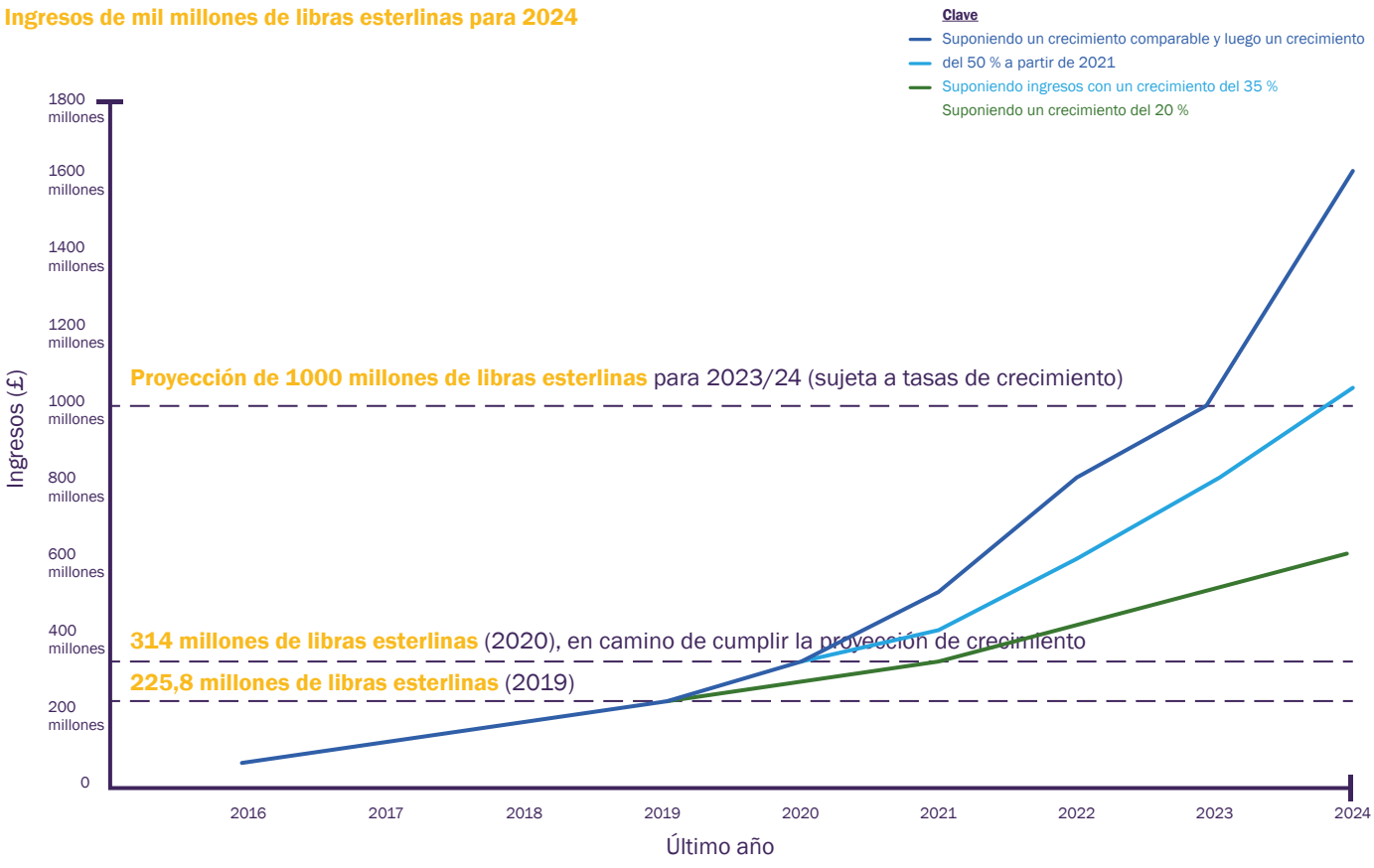
- La mejora en el reconocimiento facial, que podría acelerar la identificación de las víctimas menores de edad.[103]
- Análisis predictivos, que ya usan algunas autoridades para identificar a menores en peligro de abuso o para hacer posible una intervención temprana.[104]
- Herramientas para recopilar metadatos (véase *Glosario de términos*) que detecten posible material de abuso sexual infantil, incluso si el propio material no es reconocible.[105]
- Técnicas de «huella digital» de las cámaras, usadas para atribuir fotos o vídeos a un dispositivo concreto. En algunos países, estas técnicas ya se utilizan para optimizar y reforzar los procesos judiciales.[107]

¿QUÉ ES LA «TECNOLOGÍA DE LA SEGURIDAD»?



Los proveedores de tecnología de la seguridad desarrollan tecnología o soluciones para proporcionar experiencias online más seguras y proteger a los usuarios de contenidos, conductas o contactos perjudiciales.[106]

Figura 8: Gráfico que muestra el crecimiento previsto para el sector de la tecnología de la seguridad en el Reino Unido, reproducido con el permiso del Ministerio de Medios Digitales, Cultura y Deporte del Reino Unido. [108]



APPLE: AMPLIACIÓN DE LA PROTECCIÓN DE MENORES

Apple está considerando introducir funciones adicionales de seguridad infantil es Estados Unidos. Por ejemplo:

- Nuevas herramientas para dispositivos que advertirían a los niños y, en el caso de menores de 13 años, a sus padres o tutores cuando reciban o envíen fotos sexualmente explícitas, si los padres o tutores han decidido que se les notifique.
- Actualizaciones de Siri y Search para ayudar a los usuarios en caso de encontrarse en situaciones sexuales poco seguras, tanto online como en persona, y también para intervenir cuando los usuarios intenten buscar material de abuso sexual infantil, a fin de proporcionar recursos y advertencias dirigidas a prevenir el abuso.
- Utilización de la nueva herramienta NeuralHash para identificar el material de abuso sexual infantil «conocido» almacenado en la galería fotográfica de iCloud, al establecer coincidencias del contenido con una base de datos hash de imágenes de abuso sexual infantil. Si la coincidencia de funciones hash excede un umbral mínimo, se requerirá una revisión humana de confirmación antes de enviar un informe al NCMEC. Este proceso de emparejamiento es posible gracias a una tecnología de encriptación denominada «Private Set Intersection and Threshold Secret Sharing», que determina si hay una correspondencia sin revelar el resultado, a menos que, y hasta que, se alcance el umbral mínimo. Apple no puede obtener información sobre la cuenta de un usuario a menos que se haya detectado una colección de imágenes que coincidan con CSAM «conocido».

Fundamentalmente, las funciones podrían ser compatibles con el servicio iMessaging encriptado de Apple y demostrar su potencial continuo para contrarrestar la amenaza de explotación y abuso sexual infantil, incluso en entornos encriptados, mediante el uso de tecnologías a nivel de dispositivo y servidores sin vulnerar la protección de datos.

LA ALIANZA MUNDIAL PARA ACABAR CON LA VIOLENCIA CONTRA LOS NIÑOS: FONDO SAFE ONLINE

La iniciativa Safe Online forma parte de la Alianza Mundial para Acabar con la Violencia contra los Niños. Invierte en actuaciones de programación, generación de pruebas e innovación tecnológica para combatir el abuso sexual infantil en internet. Desde 2017, Safe Online ha invertido un total de 48 millones de dólares en 60 proyectos. En 2020, 10 millones de dólares de estos fondos se invirtieron en el diseño y la integración de soluciones tecnológicas.

Junto con las inversiones financieras para reforzar la respuesta al abuso sexual infantil online, la iniciativa Safe Online de la Alianza para Erradicar la Violencia fomenta el conocimiento y la colaboración con el objetivo de maximizar el uso de recursos colectivos y asegurar que las inversiones tengan un impacto más amplio.

Safe Online desempeña un papel crucial en la defensa y el fomento de la acción colaborativa para alinear los esfuerzos mundiales, regionales y nacionales y combatir los daños en internet contra los menores.

Esta perspectiva se apoya en el aumento de las inversiones de los gobiernos y del sector privado para ampliar las soluciones y mantener a los niños a salvo. Como ha señalado la Alianza para Erradicar la Violencia, la falta de inversión sigue siendo el mayor obstáculo para combatir la explotación y el abuso sexual infantil en internet.[109] Una implantación más amplia y consistente de las tecnologías es esencial para evitar que los agresores dirijan a los menores a plataformas sin mecanismos de seguridad integrados.

A medida que esta implantación aumente, el posicionamiento común internacional para legislar el uso de dichas tecnologías será cada vez más importante,[110] puesto que en muchos casos pueden plantear problemas éticos y de privacidad. Es necesario que las empresas asesoren a los gobiernos con el fin de desarrollar marcos legales que permitan una innovación responsable que ponga los derechos de los menores en el centro del diseño y el despliegue tecnológicos. Esto debe incluir la protección del derecho de los menores a su privacidad, a disponer de información adecuada para su edad y a la no discriminación en la aplicación de algoritmos de IA.[111] Los mecanismos para proteger a los niños más pequeños merecen una consideración especial para garantizar que no se vean privados de oportunidades debido a los peligros percibidos, entre otras cosas porque una baja alfabetización digital podría hacerles más vulnerables al abuso.[112]

05

Temas

Regulación, cooperación voluntaria y transparencia

El ritmo del cambio tecnológico continúa complicando la respuesta ante la explotación y el abuso sexual infantil en internet.

La proliferación de la explotación y el abuso sexual infantil online ha avivado el debate sobre la regulación de internet en los últimos años.

En espera de que más países tomen medidas para regular a los proveedores de servicios de internet, la cooperación voluntaria y la transparencia seguirán siendo vitales para coordinar una respuesta global.

El objetivo de la normativa es proporcionar un marco legislativo que permita armonizar la privacidad y la seguridad de los usuarios para conseguir un enfoque más consistente a la hora de enfrentarse a los daños online.

En los últimos tres años, se ha impulsado significativamente una reglamentación de servicios digitales y seguridad en internet. Entre los primeros países en buscar una solución legal se encuentran Australia, Alemania, Reino Unido, la Unión Europea e Irlanda (véase Figura 10).

Los sistemas de regulación efectivos siguen un ciclo de cuatro pasos (véase Figura 9).

La regulación de daños en línea es relativamente inmadura si la comparamos con la de otros sectores, como la aviación, la alimentación y los servicios financieros. La transparencia está limitada y tanto el compromiso voluntario como las medidas correctivas son inconsistentes. Sin embargo, la creciente concienciación de estos daños está generando una presión internacional cada vez mayor para que se adopten unas normas de transparencia y responsabilidad consistentes, y se apliquen unas medidas correctivas reguladas por un marco legislativo adecuado.

Figura 9: Pasos de un ciclo regulador efectivo.

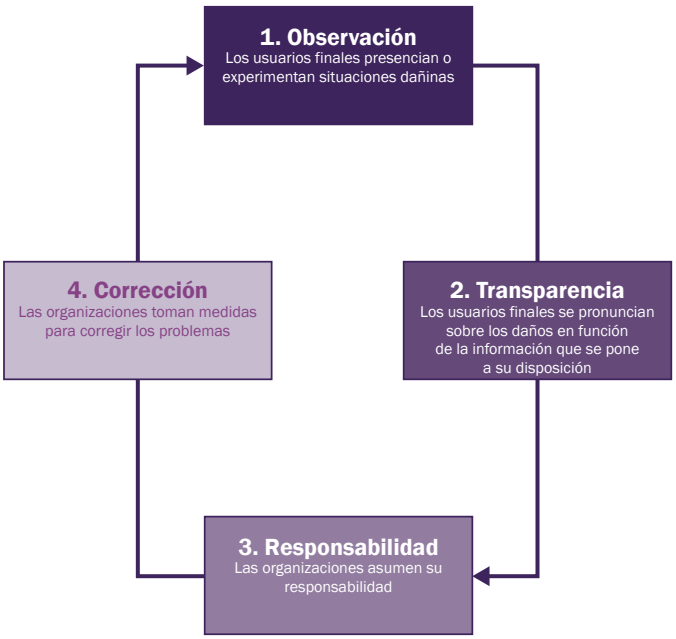
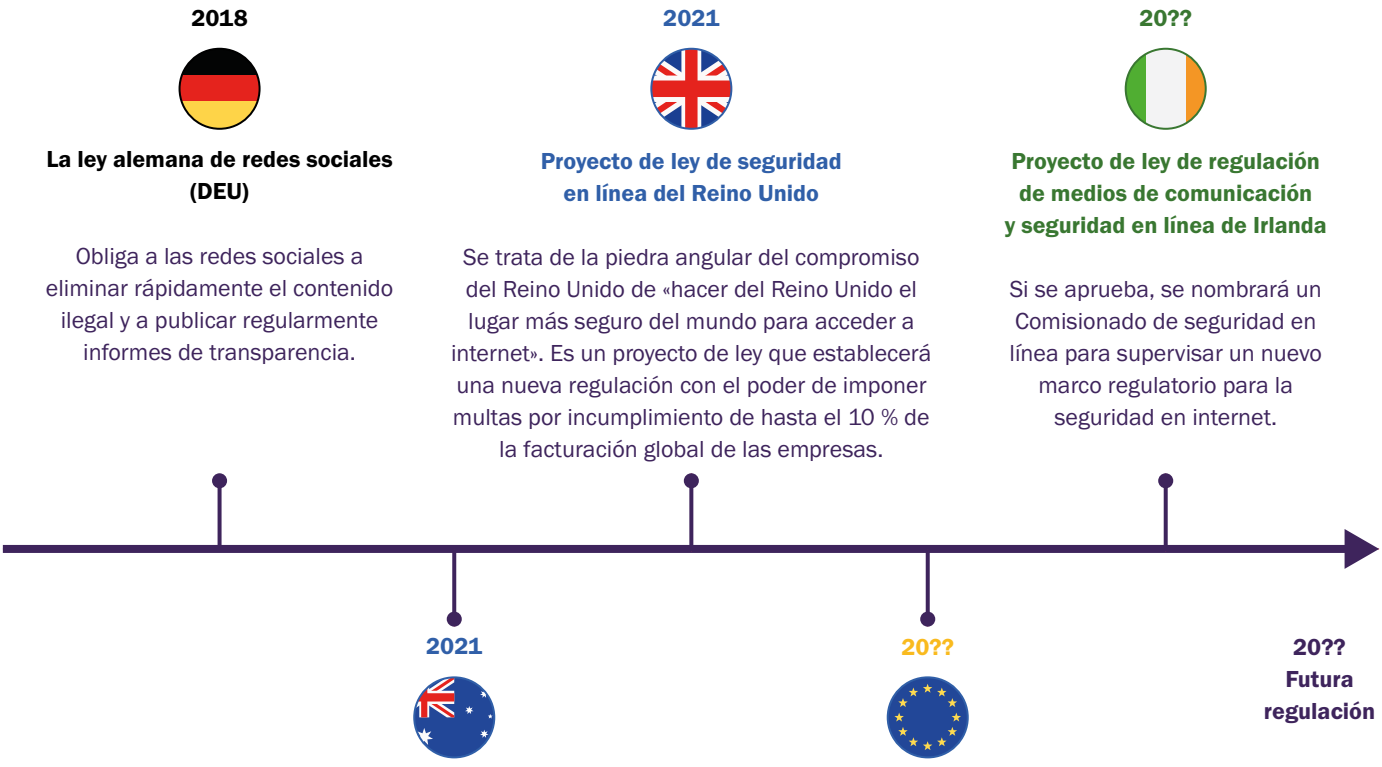


Figura 10: El camino hacia la regulación de internet. [113] [114] [115] [116] [117] [118]



En el mundo físico, los marcos legales ayudan a las empresas y a las autoridades a encontrar el equilibrio entre la privacidad y la seguridad individuales, pero en el ámbito de internet estas normas aún se están desarrollando. Al definir las responsabilidades de los proveedores de servicios de internet, se podría lograr un equilibrio más consistente para proteger a los usuarios de los daños, especialmente a los niños.[119]

El aumento del uso de cifrados de punta a punta (E2EE, por sus siglas en inglés) es un buen ejemplo del peligro de carecer de una normativa consistente en materia de seguridad y pone de manifiesto la necesidad de regular internet.

La encriptación y el E2EE son cada vez más populares debido a que los usuarios están cada vez más preocupados por la protección de sus datos y su privacidad en internet. El E2EE es una de las opciones de seguridad disponibles más efectivas. El Relator Especial de Naciones Unidas sobre la Libertad de Opinión y Expresión ha descrito el E2EE como «el pilar más importante para la seguridad digital en aplicaciones de mensajería» y puso de relieve su importancia para proteger a las minorías en «grave riesgo de ver sus derechos humanos violados y de sufrir acoso».[120] El E2EE ya está integrado en algunos servicios de mensajería y algunas grandes plataformas han anunciado que están en vías de implementar[121] o ampliar esta funcionalidad.[122]

¿QUÉ ES EL CIFRADO DE PUNTA A PUNTA (E2EE)?

Es una forma de encriptación en la que el contenido de los mensajes solo es visible para el emisor y el receptor. Descodificar el mensaje requiere de una clave de desencriptación privada que se intercambia entre las partes, de manera que si se intercepta el mensaje, ni el proveedor del servicio, ni las fuerzas de seguridad ni ninguna otra parte pueden verlo ni controlarlo.[123]

Sin embargo, el E2EE socava los esfuerzos por hacer frente a la explotación y el abuso sexual infantil en internet. La mayoría de las tecnologías de detección (por ejemplo, el «hash-matching», los algoritmos de detección de captación, los clasificadores para identificar el material de abuso sexual infantil) no pueden utilizarse en entornos con E2EE.

En Europa, la falta de consenso sobre el uso de tecnologías de detección automatizada ha servido curiosamente para descubrir las posibles consecuencias de no poder implementar dichas herramientas. El NCMEC experimentó una reducción del 58 % de los informes de la CyberTipline relacionados con la Unión Europea cuando algunas empresas dejaron de utilizar estas herramientas en diciembre de 2020, en cumplimiento con la directiva europea de privacidad electrónica.[124] [125] En mayo de 2021, se acordó una derogación temporal de la ley,[126] pero esto solo permite que la detección se reinstaure durante tres años. Como ha señalado la ECPAT,[127] es necesaria una respuesta legislativa a largo plazo para solventar este problema. Se espera que la implementación en la Unión Europea de una nueva estrategia para los derechos de la infancia[128] junto con los esfuerzos por fortalecer la lucha contra el abuso sexual infantil en internet[129] sienten las bases para encontrar una solución.

Dado que encubren la magnitud de la explotación y el abuso sexual infantil detectables en internet,[130] el aumento del uso del E2EE podría suponer una traba a la hora de exigir una mayor inversión para acabar con esta lacra.[131] También es probable que compliquen las investigaciones de los cuerpos de seguridad, ya que las solicitudes de órdenes judiciales que permiten el acceso a los dispositivos de los sospechosos (para tener pruebas de los delitos) podrían no incluir el contenido de las comunicaciones y se limitarían a incorporar metadatos (véase *Glosario de términos*) y otros indicadores que apuntarían a una «posible» actividad sospechosa.[132] Si bien las plataformas pueden utilizar dicha inteligencia para hacer un seguimiento de los sujetos de alto riesgo, como explica el Virtual Global Taskforce, los metadatos «generalmente no cumplen con los requisitos necesarios para solicitar una orden de registro».[133] La Agencia Nacional contra el Crimen (NCA) del Reino Unido destaca su investigación sobre el contumaz agresor, David Wilson, que usó perfiles falsos en redes sociales y engaño como mínimo a 500 niños para que le enviaran vídeos e imágenes sexuales y luego procedió a chantajearlos y amenazarlos. La NCA advirtió que el E2EE no solo habría reducido la probabilidad de que se detectaran los delitos de Wilson, sino que también habría impedido el acceso a los 250 000 mensajes que se usaron como prueba para condenarlo.[133] El mayor uso del E2EE también podría obstaculizar la detección de abusos en entornos no cifrados, al reducir el acceso al material necesario para formar a los clasificadores inteligentes y a otras herramientas de detección de contenido ilegal.[135]

Ya se están buscando soluciones para que las herramientas de detección sean compatibles con el E2EE. El cifrado «homomórfico» está emergiendo como una posible solución, porque permite analizar datos cifrados sin tener que descifrarlos primero.[136] Las investigaciones se centran pues en mejorar la eficiencia de la tecnología, para permitir su implementación a gran escala. Otras propuestas incluyen:

- La incorporación de herramientas de detección en navegadores y sistemas operativos (reduciendo la dependencia de plataformas para detectar abusos).[137]
- El uso de «enclaves» seguros como entorno protegido en el que descifrar, examinar y volver a cifrar el contenido para su posterior transmisión.[138]
- La creación de «firmas» digitales para el contenido en el punto de transmisión. Estas se transmitirían junto con el contenido cifrado, lo que permitiría a los proveedores de servicios de internet filtrar los mensajes en busca de firmas («hashes») de material conocido de abuso sexual infantil.[139] [140]

Ninguna de estas soluciones facilitaría directamente el acceso de las fuerzas de seguridad al contenido: la policía aún necesitaría los dispositivos de los sospechosos o de las víctimas para probar los delitos.[141] Sin embargo, podría existir una detección y eliminación de material de abuso sexual infantil más proactiva, en lugar de reactiva, gracias a los informes de usuarios o a las investigaciones policiales.[142] Los defensores de la privacidad podrían argumentar que estas medidas son desproporcionadas, dado que los beneficios del E2EE pueden considerarse mayores que la explotación y el abuso sexual infantil online para la mayoría de los usuarios.[143]

Por ello, la cooperación voluntaria y la transparencia son esenciales para establecer una regulación y dar coherencia a la respuesta global.

Al ayudar a las empresas a encontrar el equilibrio entre la privacidad y la seguridad de los usuarios, la regulación de internet podría mitigar parcialmente los inconvenientes que representa el E2EE para la detección de la explotación y el abuso sexual infantil en internet. En este sentido, las leyes tienen la posibilidad de mejorar la prevención. De hecho, el Centro Canadiense para la Protección de la Infancia considera que la regulación es fundamental para reducir los «altos niveles de reiteración de imágenes» y las «largas demoras en los tiempos de eliminación» mediante incentivos comerciales y legales «para evitar que estas imágenes salgan a la luz».[144]

La implementación de nuevas leyes para el uso de internet va a suponer grandes retos. Se trata de un territorio desconocido para muchos gobiernos y plantea preguntas difíciles, como por ejemplo:

- Cómo prevenir el daño sin restringir excesivamente la libertad de expresión.
- Qué constituye contenido «dañino» (el contenido ilegal es más fácil de definir).
- Cómo mitigar el peligro de que las leyes tengan un impacto comercial desproporcionado en las empresas más pequeñas.
- Cómo garantizar el cumplimiento de la regulación en diferentes jurisdicciones para las empresas con una base de usuarios internacional.[145]

La adaptabilidad y la colaboración con los proveedores de servicios de internet serán fundamentales durante la implementación de estas regulaciones, para aumentar las posibilidades de que las leyes aporten los beneficios esperados.

En última instancia, hará falta una solución global, ya que un acuerdo internacional es la única manera de reducir el riesgo de crear lo que el Comisionado de seguridad electrónica de Australia denomina como «una 'red divisoria' entre las diferentes leyes de distintos países y regiones». Estas inconsistencias a nivel mundial podrían obstaculizar la vigilancia efectiva,[146] debido a que las empresas o los propios usuarios de internet podrían adaptar sus actividades para sortear esta regulación. Es posible que «a medida que las grandes plataformas se pongan estrictas[...] se produzca un éxodo hacia espacios que más difíciles de escrutar y moderar».[147] La base de usuarios de algunas de las plataformas más grandes ya parece estar disminuyendo: a nivel mundial, el tiempo dedicado al uso de las cinco aplicaciones de redes sociales más descargadas se redujo en un 5 % en 2020.[148]

Mientras tanto, la cooperación voluntaria y la transparencia son complementos importantes de la regulación. Además de salvar las distancias que surgen entre los diferentes marcos normativos, la cooperación y la transparencia también brindan capacidad de respuesta para hacer frente a una amenaza de rápida evolución.

La transparencia de los proveedores de servicios de internet es fundamental para que entendamos mejor a qué nos enfrentamos y qué hace que una respuesta sea eficaz. A medida que las herramientas de detección y detención avanzan, la transparencia es cada vez más importante para establecer normas coherentes para su uso proporcional y para «aliviar el temor a abarcar de más y al uso indebido de la tecnología».[149]

La cooperación voluntaria internacional ha avanzado (véase Figura 11) junto con la innovación tecnológica. Hay que trabajar más para garantizar que las iniciativas sean inclusivas a nivel geográfico e involucrar a todo aquel que esté relacionado con el sector de los servicios de internet. Por ejemplo, ir más allá de las plataformas e incluir a los fabricantes de dispositivos y a los operadores de redes móviles.

Figura 11: Ejemplos de cooperación internacional voluntaria.

Principios voluntarios

Establecidos en la mesa redonda de «Five Country Ministerial Digital Industry» de 2019, los Principios voluntarios ofrecen un marco de referencia para que empresas de tecnología de todos los tamaños aborden la amenaza de la explotación y el abuso sexual infantil en línea.[150] Se puede consultar la lista de miembros de la Alianza y otras empresas que han respaldado dichos Principios **aquí**.

Alianza de confianza y seguridad digital

Marco para la industria establecido por nueve de las empresas tecnológicas más grandes del mundo en febrero de 2021. El alcance de la alianza es amplio y abarca la gestión de todos los contenidos y comportamientos dañinos en línea.[151]

Tecnología Coalición «Project Protect»

«Project Protect» ha creado un Fondo de Investigación e Innovación de varios millones de dólares para el desarrollo de herramientas que prevengan y erradiquen la explotación y el abuso sexual infantil en internet, liderado por las empresas globales que componen el consorcio Tech Coalition.[152]

El NCMEC informa de un descenso del 58 % de los informes de la CyberTipline relacionados con la Unión Europea desde que algunas compañías interrumpieron su uso en diciembre de 2020, en cumplimiento con la directiva europea en materia de privacidad electrónica.

06

Daños

Captación de menores en internet con el propósito de explotación y abuso sexual

A medida que más niños y niñas disfrutan de un mayor acceso a internet, existe también un peligro significativo de que la captación por internet siga creciendo, a menos que se implementen soluciones de protección.

En 2020, el NCMEC declaró un aumento del 97,5 % en la «incitación por internet»,[153] una categoría muy amplia de explotación que incluye la captación por internet. Según el NCMEC, en ella interviene «un adulto que se comunica con un supuesto menor vía internet con la intención de cometer un delito sexual o un secuestro».[154]

La encuesta que llevó a cabo Netclean en 2020 a 470 agentes de policía de 39 países también puso de manifiesto un aumento en los intentos de contactar con niños, lo que corrobora que la incidencia del acoso sexual en internet está aumentando.[155]

La captación a menudo puede provocar todo el espectro de daños comprendidos en la explotación y el abuso sexual infantil, como la producción de imágenes, la coacción, la extorsión y el abuso en persona, cuyas consecuencias pueden ser muy graves. Un estudio del NCMEC sobre los informes de extorsión sexual registrados entre 2014 y 2016 reveló que de las víctimas que habían experimentado una vivencia negativa, una de cada tres se había autolesionado o había intentado o amenazado con suicidarse.[156] Existen pruebas de que los traficantes también utilizan la captación por internet para reclutar a niños o niñas a los que explotar sexualmente con fines comerciales.[157]

Es difícil profundizar en la prevalencia de la captación por internet porque muchos países aún no la han definido en su legislación. Una evaluación comparativa del Economist Impact de 2020 para clasificar las respuestas de los distintos países al abuso sexual infantil reveló que, de 60 países analizados, solo 21 tenían una legislación que prohibiera la captación por internet con fines sexuales.[158] La ausencia de una definición legal complica la denuncia y la investigación tanto a nivel nacional como internacional. La captación aparece criminalizada en el «Convenio de Lanzarote» (Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual. Véase Glosario de términos).

Sin embargo, esta definición presupone que se realiza una propuesta para reunirse en persona, seguida de «actos materiales», por lo que debería actualizarse para incluir situaciones en las que el abuso se perpetra exclusivamente por internet.[159]

Las características del entorno digital han creado nuevos factores de riesgo para la captación por internet.

Un estudio de 2017 calculaba que, a los 12 años, el 50 % de los menores de todo el mundo ya tenían cuentas en redes sociales:[160] una huella digital que «ayuda a los depredadores a inmiscuirse en las vidas de los niños como paso previo a establecer contacto».[161] Los agresores también pueden usar información recopilada mediante funciones de geolocalización de imágenes o el «check in» en locales para que la víctima se sienta más acorralada o para poder ubicar físicamente al niño. Hasta cierto punto, internet también ha normalizado la comunicación con desconocidos: la encuesta de la UE Kids Online Survey de 2020 descubrió que estar en contacto con alguien desconocido en internet es una práctica habitual para el 37 % de los menores.[162]

Así, internet permite unas tácticas de captación que no pueden replicarse en el mundo real:

> ***«Para aquellos cuya intención es explotar a niños, lanzar una red de pesca lo más amplia posible es mucho más fácil hoy que hace 20 o 30 años. Pueden enviar mil solicitudes en cuestión de días y ser rechazados 999 veces. Solo necesitan que les acepten un chat o una solicitud de amistad para abrir la puerta".***
>
> Thorn, abril de 2021[163]

Un análisis de los informes de «Coacción y extorsión sexual de niños en internet» registrados por el NCMEC

2013 — 2016

ha revelado el uso de múltiples plataformas

42%

en muchos de los casos.

La forma en que los menores responden ante estas situaciones depende de una compleja interacción de factores. Desde principios de 2020, a estos factores se añade la experiencia individual de los menores con la COVID-19. Como advirtió la organización benéfica del Reino Unido NSPCC: «Los sentimientos de soledad provocados por la pandemia han llevado a algunos menores a buscar compañía y apoyo de desconocidos, lo que los hace más vulnerables a la captación."[164]

Internet ofrece diversas oportunidades para aquellos que intentan captar a menores.

Una táctica comúnmente empleada es el uso de múltiples canales para acceder a un grupo más amplio de potenciales víctimas y evitar ser detectados. Los agresores migran la conversación sistemáticamente de una plataforma pública a los mensajes privados, una técnica conocida en inglés como «off-platforming», que se traduce literalmente como «sacar de la plataforma». Por lo general, los intercambios se trasladan a aplicaciones que usan E2EE (lo que garantiza que las comunicaciones no serán controladas) o que carecen de herramientas integradas para detectar comportamientos depredadores. La mayoría de los delincuentes suelen migrar a plataformas nuevas con mecanismos de moderación y seguridad poco desarrollados. Un análisis de los informes de «Coerción y extorsión sexual de menores en internet» registrados por el NCMEC entre 2013 y 2016, reveló el uso de múltiples plataformas en el 42 % de los casos.[165] La encuesta del Economist Impact encargada junto con este informe descubrió que el 68 % de los encuestados que, de niños, recibieron material sexualmente explícito por internet, lo recibieron a través de un servicio de mensajería privado.

Los menores afirman que los captadores se acercan a ellos «a través de redes sociales, aplicaciones de mensajería instantánea, plataformas de transmisión en directo y servicios de chat de voz o texto integrados en los juegos multijugador en línea».[166] Las plataformas de videojuegos plantean un desafío complejo para la seguridad de los niños porque, en dichos entornos, las interacciones entre adultos y menores están relativamente normalizadas. La socialización en el videojuego se establece mediante el chat de audio y vídeo, así como por las plataformas que permiten a los jugadores transmitir sus partidas en directo mientras juegan. La Europol advierte que los menores «están más expuestos a posibles agresores a través de los videojuegos en línea»,[167] en parte como resultado de la COVID-19, a la que se le atribuye el imprevisto crecimiento de la industria del videojuego en un 50 % en 2021.[168]

FUNDACIÓN MARIE COLLINS: La historia de Olivia

A Olivia*, múltiples agresores la captaron por internet con fines sexuales en un período de dos años. Tenía 10 años cuando se descubrió el abuso. El agresor principal la captó a través de una aplicación de juegos para niños y niñas antes de trasladar la comunicación a aplicaciones más privadas.

Compartió los datos de Olivia con otros agresores, que empezaron a contactarla directamente mandándole enlaces a vídeos pornográficos para normalizar el comportamiento sexual y «enseñarle» lo que tenía que hacer. Eran hombres de diferentes países que se comunicaban a través de la Dark Web.

Olivia finalmente «confesó» el abuso dejando su dispositivo móvil desbloqueado, con correos electrónicos de los agresores a la vista para que los descubriera su padre. Estaba recibiendo cientos de correos de hombres distintos y ya no podía guardar más el secreto: tenía miedo y quería que las agresiones cesaran.

Este abuso tuvo grandes repercusiones en la salud mental de Olivia y su autoconcepto.

La Fundación Marie Collins (MCF) es una organización benéfica con sede en Reino Unido cuya misión es garantizar que todos los niños y jóvenes que hayan sufrido abusos sexuales reciban el apoyo necesario para recuperarse y vivir a salvo y seguros.[169]

*seudónimo

EL descubrimiento de las «palabras enmascaradas» de los agresores revela un contenido más dañino en las plataformas de videojuegos.

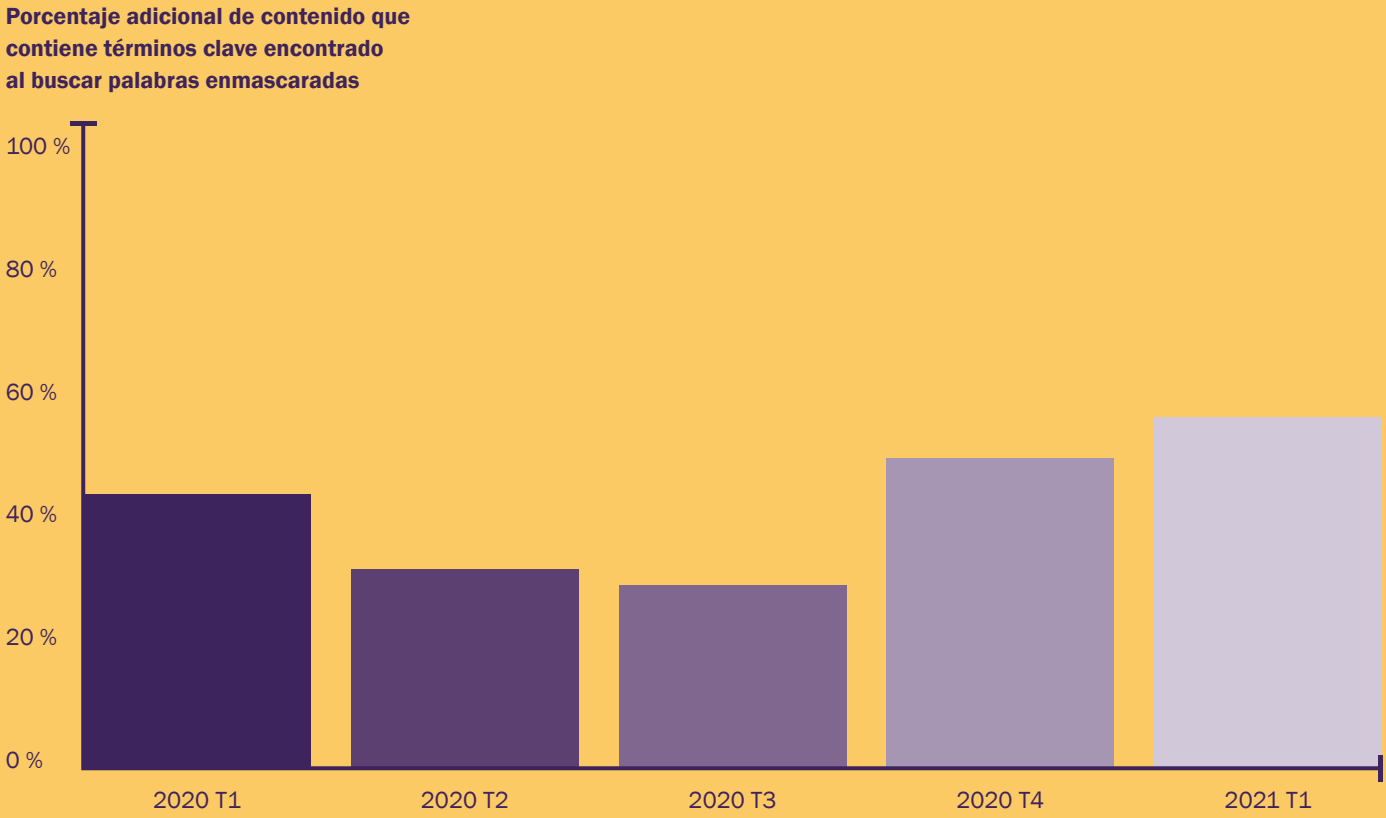
El anonimato y la ausencia de fronteras, junto con la facilidad de acceso a los espacios percibidos como seguros en internet, les da a los agresores la confianza para compartir material de abuso sexual infantil, así como tácticas y «tradecraft» para evitar su detección a través de redes de agresores.

Las salas de chat, las llamadas de voz y las plataformas de streaming en directo son nuevas formas de entrar en contacto con menores e iniciar el proceso de captación. Crisp llevó a cabo un análisis de conversaciones en la Dark Web en las que se mencionaban tres plataformas de videojuegos populares a nivel internacional, lo que ha destapado un diálogo abierto entre agresores, aparentemente para compartir consejos de captación. De 2019 a 2020, el número de conversaciones aumentó una media de un 13 % en todas las plataformas.

Crisp también ha observado que los agresores usan continuamente «palabras enmascaradas», es decir, palabras en las que algunas letras clave se reemplazan con números o símbolos para burlar los métodos de detección (por ejemplo, «8!rthday» en vez de «Birthday», lo que sería el equivalente a «cumpleañ0$» en vez de «cumpleaños»). Al identificar los intentos de los agresores por enmascarar palabras en las plataformas, Crisp identificó hasta un 50 % más de contenido con este tipo de términos, lo que llevó a la identificación de más contenido dañino y de quiénes estaban detrás del mismo.

La seguridad del usuario, ya sea en videojuegos o en cualquier red social o plataforma de contenido generado por los usuarios, depende de la capacidad de identificar rápidamente el contenido dañino y las estrategias para crearlo. La aplicación de métodos de inteligencia es esencial para identificar a los agresores e impulsar las actualizaciones de las políticas de prevención.

Figura 12: Se encontró contenido adicional cuando se identificaron términos enmascarados.



Existen soluciones para detectar la captación por internet, pero su adopción no está generalizada y los desafíos técnicos no desaparecen.

Ya se utilizan herramientas que utilizan inteligencia artificial para identificar y bloquear las conversaciones sobre captación infantil. Sin embargo, solo el 37 % de las empresas que respondieron a la encuesta de la Alianza Global de WeProtect/Technology Coalition implementan estas tecnologías.[170]

Detectar la captación por internet supone un gran reto, entre otras cosas, porque para crear herramientas para combatirla los desarrolladores necesitan tener acceso a «guiones» de chat con el fin de entrenar algoritmos. Si bien hay ejemplos de colaboración eficaz entre la policía, las plataformas y los desarrolladores, se podría simplificar el intercambio de datos para impulsar la innovación. Además, hay otros obstáculos que superar, como desarrollar herramientas que puedan funcionar en varios idiomas y sortear el uso de jerga y palabras en clave. Es necesario estar continuamente innovando para mejorar la precisión de estas herramientas, que además servirían también para minimizar las intrusiones injustificadas en la privacidad del usuario.

Las soluciones más efectivas son aquellas que pueden detectar conversaciones de alto riesgo y prevenir la captación antes de que ocurra. Sin embargo, esta tecnología es compleja, sobre todo porque «el chat puede evolucionar muy rápidamente[...] una conversación puede degenerar en contenido sexual en solo tres minutos».[171] Por otra parte, la mayoría de las herramientas de detección de captación no se pueden implementar fácilmente en entornos E2EE.

La incidencia de la captación por internet podría reducirse significativamente mediante entornos de internet «seguros por diseño».

La «seguridad por diseño» es una iniciativa del Comisionado australiano de seguridad electrónica, ahora conocida en todo el mundo, que establece la seguridad del usuario como «un principio de diseño fundamental que debe integrarse en el desarrollo de innovaciones tecnológicas desde el principio». [172]

Las soluciones de «seguridad por diseño» con mayor potencial para reducir el riesgo de captación por internet incluyen herramientas de estimación y verificación de edad. Esta tecnología es relativamente joven todavía,[173] pero podría usarse para excluir a los depredadores de los foros de menores y garantizar experiencias apropiadas para cada edad. Otros ejemplos incluyen controles parentales y filtros de contenido. Muchas plataformas convencionales ya incorporan algunas soluciones en este sentido, como por ejemplo:

- La plataforma de videojuegos **Roblox** tiene un software de seguridad incorporado que bloquea el contenido explícito y evita que los usuarios jóvenes compartan su información de contacto.[174]
- La red social **TikTok** ha introducido configuraciones predeterminadas de privacidad y seguridad para menores de 18 años.[175]
- **Instagram** está añadiendo funciones de seguridad para proteger a los adolescentes de los mensajes directos no deseados de adultos desconocidos.[176]
- **YouTube** ha desarrollado «Experiencias supervisadas» para niños menores de 13 años, lo que limita su capacidad para subir contenido, chatear o recibir comentarios, y ayuda a los padres a administrar el contenido al que acceden.[177]

Al limitar las oportunidades de los agresores e informar a los niños sobre los peligros a los que se enfrentan, estas funciones pueden reducir el riesgo de que los menores caigan víctimas de la captación por internet. También pueden aumentar la efectividad de otros mecanismos de seguridad, reduciendo el volumen general de incidentes y permitiendo un seguimiento y una protección más específicos.

YOTI: TECNOLOGÍA DE ESTIMACIÓN DE EDAD

YOTI es una plataforma de identidad digital global con sede en el Reino Unido que dispone de una tecnología de estimación de edad.

La IA de estimación de edad de YOTI analiza el rostro de un individuo y hace un cálculo estimado de su edad en 1 o 1,5 segundos, sin revelar ni almacenar ningún dato personal. Actualmente tiene una tasa de precisión media de 2,19 años en casi todas las franjas de edad y de 1,5 años para las personas de entre los 13 y los 25 años, lo que garantiza una moderación adecuada para los umbrales de edad del sector. También incluye al 13 % de la población mundial que no posee identificación con foto.

Hasta la fecha, la tecnología de estimación de edad de YOTI ha llevado a cabo más de 500 millones de controles de edad para organizaciones asociadas, incluyendo plataformas de streaming de vídeo en directo, comercio electrónico, webs para adultos, juegos de azar y operadores de telecomunicaciones.

Debemos aprender más sobre la captación por internet para prevenirla y detectarla de manera efectiva y continuada.

La efectividad de las actuaciones puede verse limitada si no se abordan las lagunas en el conocimiento y la investigación.

Todavía no comprendemos del todo la interrelación entre la captación en internet y la captación «en persona», y la dificultad de intervenir para prevenir el abuso, especialmente si el niño conoce al «captador» (como sucede en la mayoría de los casos de captación «en persona»).[178] En relación con esto, es necesario que mejoremos nuestro conocimiento sobre las vías delictivas que utilizan los captadores en internet, así como los factores de riesgo y protección que influyen en la probabilidad de que se abuse de un menor. Por ejemplo, los menores con discapacidades pueden ser más vulnerables, porque recurren a internet para compensar la falta de apoyo o de conexión que sufren en el mundo real.[179] Las respuestas a estas cuestiones pueden utilizarse para diseñar actuaciones potentes y personalizadas dirigidas a proteger a los niños y eliminar o reducir aún más las oportunidades de los agresores.

06 Daños

Producción de material de abuso sexual infantil

Cuando se documenta el abuso a un menor, el agresor también comete el delito de producción de material de abuso sexual infantil.

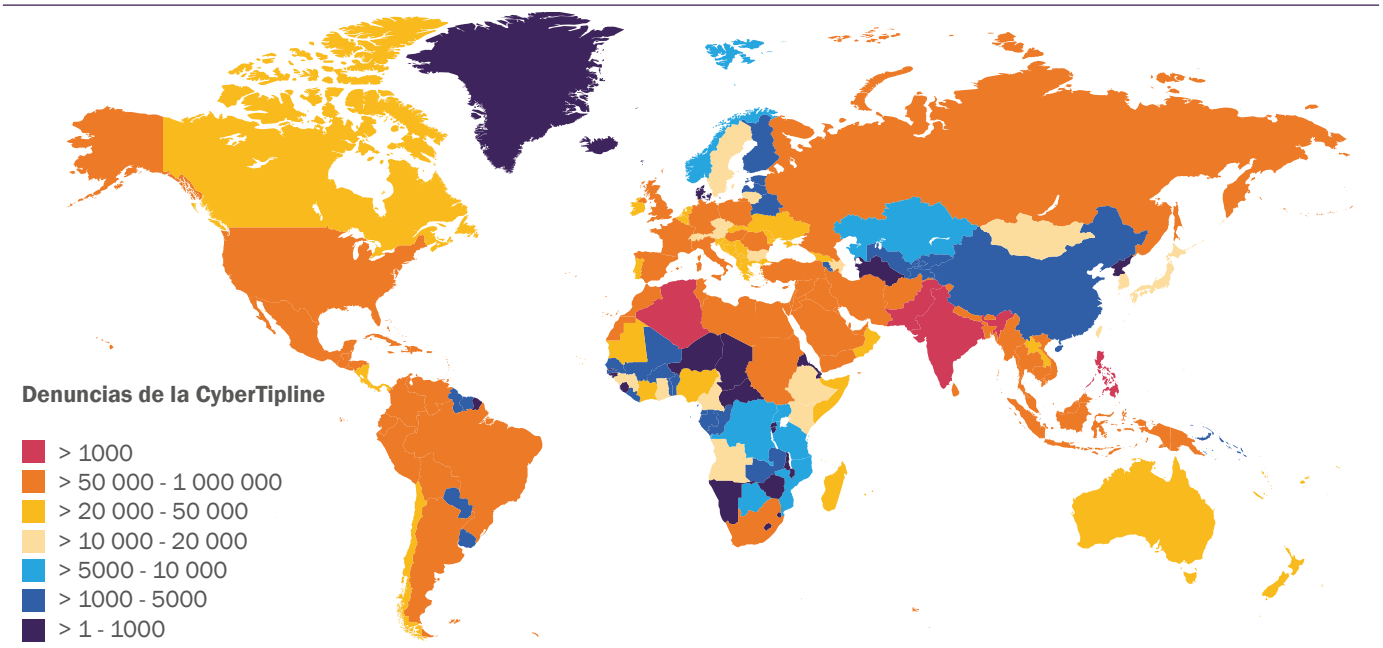
Los métodos de producción de los agresores están evolucionando, a menudo aprovechando las nuevas tecnologías.

Lo más probable es que la producción ocurra en todas las partes del mundo. Son niñas de todas las edades quienes más aparecen en las imágenes.

Un estudio conjunto de Thorn, Google y el NCMEC de 2019 concluyó que el 81 % de las denuncias por material de abuso sexual infantil proceden de Asia, África y Europa.[180] Las pruebas más recientes del NCMEC (véase Figura 13 a continuación) indican que estas mismas regiones, junto con el continente americano, siguen generando una gran cantidad de casos.

Por desgracia, estos datos ofrecen una visión intrínsecamente limitada de las tendencias globales. Por un lado, el país de procedencia de las denuncias puede no ser el mismo que el país de procedencia de las imágenes. Además, las denuncias solo transmiten el alcance del problema «conocido». Es muy probable que la producción sea (más) abundante en países con menos (o quizá ninguno) mecanismos para detectarla. Este dato viene respaldado por los resultados de la encuesta de Economist Impact, que concluyó que los menores están experimentando daños sexuales en internet en todas las regiones del mundo.

Figura 13: La procedencia de las denuncias de presunta explotación sexual infantil recibidos por la CyberTipline del NCMEC en 2020. Reproducido con el consentimiento del NCMEC. [181]



Como una muestra más de los sesgos geográficos, las pruebas indican que los menores de América del Norte y Europa Occidental tienen más probabilidades de ser identificados en las imágenes de abuso que los de Europa del Este y el Sudeste Asiático, quizá debido a los protocolos más avanzados de identificación de víctimas y denuncias.[182] Este patrón es un síntoma de las desigualdades que alteran el impacto local del abuso, cambiando la forma de la amenaza mundial.

En 2020, el INHOPE examinó 267 192 URL de contenido ilegal y el 93 % de las víctimas eran niñas.[183] La IWF, estrecho colaborador del INHOPE, declara el mismo porcentaje de contenido relacionado con niñas en las URL examinadas por su equipo.[184] Esto no implica necesariamente que las niñas sufran más abusos que los niños. Puede que el abuso a niños simplemente esté menos documentado. Sin embargo, sí puede sugerir que las niñas tienen más probabilidades de sufrir daños prolongados a consecuencia de la producción, el intercambio y la posterior distribución de sus fotografías.

El material de abuso sexual infantil lo producen a menudo familiares. Esto supone un enorme reto para la detección y prevención del delito.

Según la IWF, en el material sexual infantil «autogenerado» los niños aparecen predominantemente en una casa.[185] En el último año, se atribuye también una mayor producción en entornos domésticos a grupos delictivos que han adaptado sus formas de trabajar durante la COVID-19, »intensificando el uso de la comunicación en línea y la explotación en los hogares».[186] Sin embargo, la mayor parte de las imágenes se generan dentro de los hogares, porque los miembros de la familia suelen ser los productores del material de abuso sexual infantil:

- Un estudio de casos de abuso sexual infantil en Colombia destacó que los agresores suelen pertenecer a la familia nuclear del menor o a su círculo de confianza.[187]
- En México, el 73 % de los delitos de agresión sexual contra menores los cometen sus familiares y el 75 % de estos abusos suceden en la propia casa de la víctima.[188]
- Un estudio en Australia realizado con 150 víctimas adultas descubrió que el 42 % identificó a su padre biológico, adoptivo o a su padrastro como el principal abusador y productor de material de abuso sexual.[189]
- Un estudio de casos de abuso infantil en España puso de relieve que en el 80,2 % de los casos, el abusador pertenecía al círculo de confianza de la víctima y en el 32 % de los casos era su padre biológico.[190]

Departamento de Justicia de Estados Unidos: Página «BabyHeart», de la Dark Web

«BabyHeart» era una página de la web oscura dedicada al abuso de menores de cinco años. Estuvo disponible públicamente durante más de dos años, tiempo durante el cual se suscribieron cientos de miles de personas. Los agresores hablaban en la página sobre su preferencia por los niños y niñas de esa franja de edad porque parecía menos probable (o imposible) que denunciaran el abuso, por lo que se los consideraba de «menor riesgo». La mayoría de las imágenes compartidas en «BabyHeart» se habían producido, sin duda alguna, mediante el abuso de un familiar o de otros cuidadores, lo que pone en evidencia la importancia de que los mecanismos de prevención y detección no dependan de las denuncias de los menores y que no den por sentado que las familias son entornos seguros.[194]

Sufrir abuso sexual a manos de un miembro de la familia puede crear un trauma añadido muy complejo, sobre todo porque este tipo de abuso a menudo comienza cuando las víctimas son muy jóvenes y se prolonga más en el tiempo.[191] Las víctimas de abuso familiar también son menos propensas a hablar de ello, aunque en general todas las víctimas de abuso sexual infantil tienen problemas para informar del delito. Solo el 2 % de las denuncias de la CyberTipline del NCMEC proviene de los propios niños.[192]

A pesar de los importantes avances en el análisis de imágenes y las tecnologías de reconocimiento facial, las tasas de identificación de víctimas siguen siendo, en general, bajas. En abril de 2021, el Proyecto Arachnid del Centro Canadiense de Protección Infantil había procesado 126 mil millones de imágenes, el 85 % de las cuales pertenecen a víctimas que aún no han sido identificadas.[193] Los problemas para identificar a las víctimas subrayan la vital importancia de educar a comunidades enteras e invertir en sistemas de protección infantil para mejorar la detección del abuso, con el objetivo de identificar y proteger a las víctimas.

El Centro Australiano para Contrarrestar la Explotación Infantil ha identificado el «capping» como la tendencia delictiva actual más problemática, que genera aproximadamente

60%–70%

de los casos de la Unidad de Identificación de Víctimas.

En 2020, un «bot» de inteligencia artificial que operaba en Telegram generó

100,000

«deepfakes» pornográficos de mujeres y niñas reales.

Los métodos de producción de los agresores están evolucionando. Algunos funcionan de manera encubierta y puede que los menores no se den cuenta de que son víctimas.

El «capping» tiene una mayor incidencia desde hace algunos años. De hecho, algunas fuerzas de seguridad han notificado un incremento durante la crisis de la COVID-19.[195] [196] [197] Normalmente, esto implica la captación y la coacción sexual de menores y se ha relacionado con el aumento de material infantil «autogenerado». Los agresores van a la caza de niños y niñas en una gran variedad de plataformas y buscan ganarse su confianza para obligarlos a realizar actos sexuales que graban en vídeo, posteriormente comparten dichas grabaciones en foros de la Dark Web. Según la Europol, el número de mensajes e hilos encontrados en una sección para «cappers» de un foro de la web oscura se triplicó entre diciembre de 2019 y febrero de 2020.[198]

El Centro Australiano para Contrarrestar la Explotación Infantil ha identificado el «capping» como la tendencia delictiva actual más problemática, puesto que genera aproximadamente entre el 60 % y el 70 % de los casos de la Unidad de Identificación de Víctimas. El «capping» también demuestra el potencial de la «gamificación» (véase *Glosario de términos*) del abuso. Por ejemplo, existe una página de la Dark Web supervisada por fuerzas de seguridad que lleva a cabo concursos y «batallas de capping» mensuales, donde los «cappers» compiten unos contra otros en la publicación de imágenes de abusos.[199]

Si bien algunos menores son conscientes de que han sido víctimas de «capping», es posible que otros no lo sepan. La creación encubierta de material de abuso sexual infantil es una tendencia de producción muy extendida facilitada por una gran variedad de dispositivos digitales, entre los que se encuentran webcams (a veces pirateadas) y las cámaras de seguridad de los hogares y los colegios. En Corea del Sur, este fenómeno se conoce como «molka» y se lleva al siguiente nivel mediante la instalación de cámaras espía en objetos cotidianos, como bolígrafos.[200]

Tecnologías como las imágenes generadas por ordenador (CGI) pueden permitir una mayor diversificación de la producción e imponen cambios en la legislación.

Actualmente, los «deepfakes» y las «CGI» no suelen aparecer en las investigaciones sobre abuso infantil,[201] aunque es posible que se vayan popularizando. En 2020, un «bot» de inteligencia artificial que operaba en Telegram generó 100 000 «deepfakes» pornográficos de mujeres y niñas reales.[202] En relación con esto, la industria del cibersexo de realidad virtual para adultos ha experimentado un crecimiento significativo, en parte atribuido a los confinamientos por la COVID-19.[203] El comisionado australiano de Seguridad Electrónica ha expresado una gran preocupación por el potencial uso de la realidad virtual y otras «tecnologías inmersivas» como «una herramienta para el abuso sexual infantil en internet".[204]

Imágenes generadas por ordenador (CGI) y «deepfakes»

CGI es la creación de contenido visual estático o animado mediante un software de imágenes.[205] En el contexto del abuso sexual infantil, se trata de fotografías sexualizadas de menores total o parcialmente creadas de manera artificial o digital.[206] Un «deepfake» es una forma de CGI que utiliza inteligencia artificial (IA) para reemplazar a una persona por otra en fotos o grabaciones de vídeo.[207]

El problema clave de estas tecnologías son las escasas trabas para su uso y la verosimilitud de los resultados. Incluso los filtros simples integrados en aplicaciones populares pueden transformar el contenido con un simple clic. Algunos tipos de CGI podrían crear problemas a la policía a la hora de distinguir a un menor real de una persona artificial.[208]

Es poco probable que las CGI y las tecnologías asociadas lleguen a prevalecer en este ámbito tal como están las cosas, principalmente debido a la disponibilidad de material fotográfico de abuso sexual infantil en internet. De todas formas, deben tenerse en cuenta, sobre todo porque inciden en la necesidad de encontrar una posición acordada internacionalmente sobre una variedad de materiales no fotográficos que contribuyen a multiplicar la amenaza. Entre estos materiales se encuentran las CGI, los «deepfakes», el anime, las caricaturas y dibujos que representan abuso sexual infantil y las «muñecas sexuales» infantiles que se venden por internet.

Las CGI son dañinas porque «se sabe que se usan para la captación de menores[…] alimentan fantasías muy reales, fomentan la inclinación de los depredadores sexuales y contribuyen a mantener el mercado del material de abuso sexual infantil».[209] Existen muchas pruebas que respaldan esta creencia, por ejemplo el hecho de que este tipo de fotografías se encuentran a menudo junto con fotografías sexuales de menores.[210] Sin embargo, muy pocos países han reflejado esto en su legislación.[211]

Las CGI también se pueden utilizar como poderosas técnicas de detención, como ilustra el caso de «Sweetie», el personaje CGI de una menor que se utilizó para atrapar a más de 1000 depredadores.[212] Muchas redes de agresores exigen a los aspirantes que compartan material nuevo para poder inscribirse en grupos cerrados, por lo que también se podrían utilizar imágenes artificiales para ayudar a la policía a infiltrarse en estas comunidades. Es fundamental que se establezca una colaboración internacional en la aplicación de la ley para evitar conflictos a la hora de utilizar estas tácticas de manera más amplia, y también es necesario llegar a un consenso sobre las implicaciones éticas del uso de tecnología para tales fines.[213]

06

Daños

Buscar o visionar material de abuso sexual infantil

Los intentos de acceso a material de abuso sexual infantil van en aumento. Abordar tanto el lado de la «oferta» como el de la «demanda» es fundamental para una prevención sostenible a largo plazo.

A la mayor parte del material de abuso sexual infantil se accede a través de la internet superficial, aplicaciones E2EE o mediante el intercambio/difusión en red de pares (P2P, por sus siglas en inglés).

Solo se necesitan tres clics para encontrar contenido de abuso sexual infantil en internet.[214] A la mayor parte del material se accede a través de la internet superficial o mediante redes P2P.[215] Según la Interpol, este último modo era el más utilizado hasta 2020.[216]

Se ha comprobado que muchas personas condenadas por ver material de abuso sexual infantil hicieron pocos o ningún intento por ocultar sus huellas,[217] aunque evidentemente esta muestra está algo sesgada. Como se destaca en el Capítulo Tema: *Tecnología*, un porcentaje de los agresores utiliza herramientas y métodos avanzados para evitar ser detectados. Una de las técnicas documentadas consiste en crear aplicaciones que dirigen a los usuarios a grupos de mensajería privados usados para compartir imágenes.[218] Según la Europol, la distribución de imágenes de abuso sexual infantil «normalmente se lleva a cabo en plataformas de redes sociales".[219]

Los agresores suelen utilizar plataformas y aplicaciones E2EE, entornos que combinan la accesibilidad de la internet superficial con un alto nivel de seguridad. Como se destaca en el «Informe sobre la evaluación de la amenaza de la criminalidad grave y la delincuencia organizada de 2021» de la Europol, «el uso generalizado de herramientas de cifrado, incluidas las aplicaciones E2EE, ha reducido la detección» de los agresores de menores.[220] El uso de aplicaciones supone retos importantes para las fuerzas de seguridad, ya que la policía debe infiltrarse en grupos de mensajería privados para obtener pruebas de las agresiones. Una vez dentro, muchas agencias policiales se limitan a la recopilación manual de datos. La Child Rescue Coalition lidera el desarrollo de una solución para agilizar la obtención de pruebas en aplicaciones de dispositivos móviles en tiempo real. La herramienta está diseñada para que la usen agentes infiltrados a fin de mejorar de manera significativa la eficiencia de las operaciones encubiertas, reduciendo la necesidad de recopilar datos manualmente. La colaboración continua con las fuerzas de seguridad internacional es fundamental para maximizar su impacto y garantizar una mejor identificación y protección de las víctimas.[221]

La Dark Web oculta el contenido más extremo y permite que las comunidades de agresores compartan material y estén en contacto.

Dark Web (web oscura)

La información y las páginas a las que solo se puede acceder a través de las denominadas «redes superpuestas», como las redes privadas virtuales (VPN) y las redes de intercambio de archivos de redes de pares (P2P), que ocultan el acceso público. Los usuarios necesitan un software especial para acceder a la Dark Web, ya que está encriptada y la mayoría de sus páginas se alojan de forma anónima.[222]

En general, la actividad en la Dark Web ha aumentado en un 300 % en los últimos tres años.[223] La web oscura es, según se informa, un centro de contenido más reciente[224] y extremo[225] que pone a disposición del usuario material de explotación y abuso sexual infantil.

Las comunidades de agresores de la Dark Web han persistido y evolucionado durante más de una década y no representan una nueva dimensión de la amenaza. Sin embargo, lo que sí ha cambiado es la disponibilidad de soluciones de anonimato como Tor y VPN, que ahora son de uso común e incluso vienen integradas en algunos navegadores de forma predeterminada.[226]

Tor

«Tor» es una red privada de código abierto que permite a los usuarios navegar por la web de forma anónima. El sistema utiliza una serie de nodos por capas para ocultar direcciones web, datos de internet y el historial de navegación. [227]

Actualmente, solo se necesitan unos conocimientos técnicos mínimos para ocultar la actividad en internet. Para las fuerzas de seguridad, el desafío es ir un paso por delante de los agresores, quienes tienen más conocimientos técnicos y pueden permanecer en el anonimato para evitar ser descubiertos.[228 229 230]

Aumentan los intentos de acceder a material de abuso sexual infantil. Existen pruebas que hacen pensar que existe un vínculo entre el consumo habitual de contenido sexual adulto extremo y el consumo de material de abuso sexual infantil.

En 2020, tres de las organizaciones miembro de la IWF detectaron 8,8 millones de intentos de descarga de material de abuso sexual infantil en un solo mes.[231] Durante los confinamientos por la COVID-19 en la India, hubo un aumento del 95 % en las búsquedas de material de abuso sexual infantil.[232] Según el Consejo de Derechos Humanos de la ONU, la demanda de material de abuso sexual infantil también aumentó hasta en un 25 % durante la pandemia en algunos estados miembros de la Unión Europea.[233]

Se estima que, siendo conservadores, el 1 % de la población masculina mundial es pedófila (atracción sexual por niños y niñas prepúberes).[234] Muchas de estas personas buscan y miran material de abuso sexual infantil para satisfacer sus deseos sexuales.[235] Es fundamental potenciar la capacidad policial para identificar a estos agresores y gestionar los peligros derivados, incluida la posibilidad de que acaben cometiendo abusos contra menores en persona.

Hay muchas otras vías que llevan a consumir material de abuso sexual infantil. Según la Fundación Lucy Faithfull, solo el 15 o el 20 % de los agresores con los que trabajan actualmente son pedófilos «en el sentido de que los menores prepúberes son su principal interés sexual».[236] Varios estudios han establecido un vínculo entre el consumo de material de abuso sexual infantil y la exposición habitual a la pornografía adulta extrema, ya que este material puede, supuestamente, llegar a insensibilizar y crear una necesidad de buscar estímulos cada vez más fuertes para lograr excitarse sexualmente.[237 238] Hay dos áreas particularmente problemáticas: la llamada «pornografía con temática de abuso»[239] y la pornografía que busca representar a personas adultas como menores. La primera hace que sea más fácil para los espectadores «dar el siguiente paso para ver un abuso real», mientras que la segunda ha sido descrita por los agresores como una puerta de entrada al consumo de material de abuso sexual infantil.[240]

El vínculo con el consumo de pornografía extrema es preocupante también porque la exposición de los menores a contenido sexual para adultos ha aumentado drásticamente en la era digital. Algunos estudios en varios países de Asia Oriental sugieren que el 50 % de los menores y jóvenes han estado expuestos a «medios sexualmente explícitos», mientras que en Estados Unidos, Australia y varios países europeos se habla de tasas de exposición del 80 % o más.[241] El consumo frecuente de pornografía para adultos o pornografía violenta desde una edad temprana se asocia con el consumo de material de abuso sexual infantil.[242]

La forma en que se guía a los usuarios para interactuar con el contenido en línea contribuye también a facilitar los caminos hacia la delincuencia. El medio principal para incitar a los usuarios a participar en las redes sociales es la recomendación de contenido, para lo que, en general, existen dos modelos: el primero es el modelo algorítmico de «gráfico social», que presupone los intereses de un usuario, priorizando las actividades de sus contactos. El segundo es el modelo de «gráfico de intereses», que deduce los intereses de un usuario en función de su actividad e interacciones. Para los usuarios que buscan de manera inapropiada contenido que involucre a menores, dichos algoritmos pueden reforzar su comportamiento al recomendar una y otra vez fotografías y vídeos con la misma temática.[243] [244] Esto, junto con un alto número de visualizaciones de vídeos e hilos de comentarios preocupantes, que a menudo escapan a la detección de los moderadores,[245] puede provocar que estos usuarios superen sus inhibiciones internas y cometan un abuso.[246] [247] Algunas plataformas importantes afirman tener mecanismos de detección y políticas de moderación para identificar estos comportamientos.[248] La rapidez y eficacia de estas medidas es fundamental, porque, tal como explica el Centro Nacional de Investigación Social del Reino Unido, «la insensibilización/desinhibición y validación en internet de otros agresores son a menudo razones que impulsan a consumir material de abuso sexual infantil o a pasar a la agresión de contacto».[249]

La interrupción de las búsquedas de material de abuso sexual infantil puede disuadir a los agresores, pero el impacto de estas intervenciones es difícil de calcular.

El vínculo entre la visualización de contenido y el abuso en persona es evidente y pone de relieve por qué la interrupción de las búsquedas de imágenes es tan importante.

La mayoría (60 %) de las empresas tecnológicas encuestadas por la Alianza Global de WeProtect/Technology Coalition confirmaron que emiten mensajes de disuasión.[250] El filtrado de búsqueda es un mecanismo muy común, utilizado principalmente por los motores de búsqueda. Las consultas de los usuarios tienen referencias cruzadas con una lista de contenido que se debe bloquear, por lo que si se establece una coincidencia, no se devuelven resultados. En algunos casos, también se envía una advertencia a la persona que realiza la búsqueda. El año en que lo implementaron Google y Microsoft, el número total de búsquedas web de imágenes de abuso se redujo en un 67 %.[251]

Un estudio financiado por el gobierno australiano descubrió que los mensajes de advertencia enviados a los usuarios que buscaban «pornografía casi ilegal» en internet hicieron que abandonaran hasta en un 25 % de los casos.[252] Del mismo modo, la campaña «Stop It Now!» de Lucy Faithfull en el Reino Unido y el Proyecto de Prevención Dunkenfeld en Alemania demostró que la disuasión puede incentivar a los (potenciales) agresores a buscar ayuda.[253] La Fundación Oak se comprometió recientemente a financiar un nuevo proyecto de investigación para identificar y evaluar iniciativas de prevención de agresores y ayudar a implementarlo a través de un hub en internet para legisladores y profesionales.[254]

FUNDACIÓN LUCY FAITHFULL: COLABORACIÓN CON MINDGEEK (PORNHUB)

La Fundación Lucy Faithfull (la Fundación) es una organización benéfica del Reino Unido que trabaja para prevenir el abuso sexual infantil, incluyendo la asistencia a adultos y jóvenes que han cometido agresiones sexuales o corren el peligro de hacerlo. En febrero de 2021, la Fundación se embarcó en una colaboración con Mindgeek para enviar mensajes de disuasión en su página web de pornografía para adultos, Pornhub. Los mensajes se muestran cuando los usuarios realizan búsquedas que indican intentos de encontrar vídeos sexuales con menores. Mindgeek ya había reconocido la necesidad de incluir mensajes de disuasión en sus sitios de contenido para adultos porque había observado intentos de búsqueda de material de abuso sexual infantil mediante términos de búsqueda prohibidos.

Los mensajes de disuasión advierten sobre la ley y el daño causado a los menores con la creación y el consumo de este tipo de materiales. También orientan a los usuarios hacia la ayuda que necesitan para evitar cualquier comportamiento ilegal, incluyendo «Stop It Now! Get Help» («¡Detente, pide ayuda!»), una intervención autodirigida en línea para personas preocupadas por su comportamiento sexual en internet. Entre febrero y principios de mayo de 2021, los mensajes de disuasión llevaron a más de 35 000 usuarios de todo el mundo a «Stop It Now! Get Help». Aunque es una cifra relativamente pequeña en comparación con los volúmenes de tráfico generales de Pornhub, demuestra el importante papel que desempeñan estos mensajes en la educación y la intervención, como destaca la Fundación Lucy Faithfull.

El principal obstáculo para la disuasión radica en la dificultad para medir su eficacia. En los ejemplos citados, se logró mediante el seguimiento de las actividades de búsqueda de ayuda y el uso de los materiales de ayuda. Es una medida limitada, sobre todo porque es imposible saber con certeza si se ha llegado a impedir la infracción y cómo se ha hecho. También hay dudas sobre su impacto a largo plazo, con el tiempo, los usuarios podrían volverse insensibles a las advertencias o simplemente visitar otras páginas.

Los mecanismos de disuasión son una parte fundamental de una respuesta más amplia que hace frente a las diversas vías de consumo de material de abuso sexual infantil.

La importancia de los esfuerzos para eliminar el material de abuso sexual infantil de internet es indiscutible. Sin embargo, si no trabajamos también con los agresores (potenciales) para abordar la «demanda», siempre existe el riesgo de que persistan en encontrar nuevas formas de acceder a las imágenes y evitar ser descubiertos. La necesidad de equilibrar el esfuerzo entre «oferta» y «demanda» se pone de relieve en una iniciativa actual de la IWF. El instituto, que eliminó 153 600 páginas web de abuso sexual infantil solo en 2020,[255] se asoció con la Fundación Lucy Faithfull para desarrollar el chatbot ReThink con el apoyo de la Alianza para Erradicar la Violencia. La herramienta se dirigirá a los usuarios que busquen material de abuso sexual infantil y les indicará los servicios de apoyo para intentar disuadirlos antes de que cometan un delito.[256] Las iniciativas de disuasión también son importantes desde una perspectiva social más amplia, porque «se centran en cambiar el comportamiento de los adultos», no el de los niños y, al hacerlo, mandan «un mensaje claro acerca de quién es el responsable de prevenir el abuso sexual infantil».[257]

SUOJELLAAN LAPSIA RY: PROYECTO REDIRECTION

Suojellaan Lapsia Ry es una organización no gubernamental finlandesa que ayuda a proteger a los menores en todos los entornos a través de programas de apoyo, investigación y formación.[258]

Su proyecto ReDirection, apoyado por la Alianza para Erradicar la Violencia, comenzó en septiembre de 2020 y terminará en septiembre de 2022. Se trata de una iniciativa de investigación para recopilar información con el objetivo de asesorar en el desarrollo de nuevas y mejores formas de detener y disuadir a los agresores. Esta investigación distribuyó una encuesta de 30 preguntas, «Help us to help you» («Ayúdanos a ayudarte»), a través del navegador de la Dark Web «Ahmia», que procesa unas 20 000 búsquedas diarias. La encuesta se publicó automáticamente en respuesta a más de 20 000 búsquedas de material de abuso sexual infantil en el transcurso de tres meses. Se completaron más de 3100 encuestas.

Partiendo de los resultados de la investigación, Suojellaan Lapsia planea diseñar un nuevo programa de autoayuda para los usuarios que buscan y consumen material de abuso sexual infantil. El objetivo es identificar a las personas en riesgo de cometer una agresión y orientarlas hacia los servicios de ayuda y apoyo.

Comprender mejor las vías disponibles para el consumo de material de abuso sexual infantil será clave para desarrollar una respuesta eficaz. Este capítulo ha explorado solo dos motivaciones importantes: el interés sexual por los menores y la insensibilización causada por la exposición habitual a contenido sexual extremo. Es poco probable que las actuaciones de disuasión, por efectivas que sean, lleguen a desalentar a los individuos más decididos, de ahí la importancia de que se desarrollen y apliquen leyes para identificar agresiones persistentes y potencialmente sofisticadas. Asimismo, podría decirse que no es pertinente ni factible pedir cargos penales para el creciente volumen de delitos de consumo relacionados con la insensibilización y la desinhibición en internet.

06

Daños

Compartir y/o almacenar material de abuso sexual infantil

El volumen de material de abuso sexual infantil disponible en internet está aumentando. Los métodos para compartir y almacenar contenido están evolucionando.

De 2019 a 2020, el número de denuncias de la CyberTipline del NCMEC relacionadas con material de abuso sexual infantil aumentó en un 63 %.[259] En el mismo período, la IWF también advirtió un aumento del 16 % de las denuncias de material de este tipo tanto en la internet superficial como en la web oscura.

Esta cifra incluye denuncias de miembros de la sociedad y las conclusiones del equipo de la IWF tras una búsqueda activa en internet. Estos datos parecen indicar que el volumen de material de abuso sexual infantil en internet está aumentando.[260]

A escala mundial, una gran parte de las denuncias hacen referencia a material «conocido» que se ha vuelto a compartir (y no a material de «primera generación», véanse las definiciones a continuación). La red internacional de líneas directas de denuncia INHOPE calcula que el 60 % del contenido marcado como sospechoso en 2020 era «conocido».[261]

Material «conocido» y «de primera generación»

El material de abuso sexual infantil «conocido» es contenido que ha sido previamente detectado y clasificado por las autoridades policiales o los moderadores. El material «de primera generación» es contenido «nuevo» que no se había detectado ni clasificado con anterioridad.

Los vídeos representan un porcentaje cada vez mayor del contenido detectado: la cantidad de archivos de vídeo reportados al NCMEC se multiplicó por diez entre 2017 y 2020 (Figura 14).

Durante el mismo período, el número de archivos de imágenes se duplicó. Dado que muchos cuerpos de policía y agencias de investigación no tienen suficiente ancho de banda para procesar imágenes, esta tendencia podría dificultar la detección, a menos que se mejoren los equipos, especialmente a medida que la capacidad de almacenamiento de los dispositivos va en aumento.[262]

Los servidores de imágenes son las páginas que más se usan para compartir material de abuso sexual infantil.[264] Esto incluye las redes sociales, que se utilizan a menudo para difundir material a través de cuentas falsas que luego se eliminan rápidamente.[265] Actualmente no existe un mecanismo formal y establecido para que las plataformas compartan legalmente los identificadores asociados a dichas cuentas, lo que permite a los agresores saltar libremente de una plataforma a otra y de un servicio a otro, operando con relativa impunidad.[266]

El uso de «servicios ocultos» para distribuir material de abuso sexual infantil aumentó en un 155 % de 2019 a 2020.[267] Se trata de páginas web alojadas dentro de una red proxy (como «Tor», véase su definición en el glosario), de modo que no se puede rastrear su ubicación.[268]

Si bien algunos agresores siguen acumulando material en dispositivos como ordenadores portátiles, teléfonos móviles y memorias USB,[269] hay indicios de que cada vez hay menos colecciones personales y los agresores prefieren el acceso al contenido «bajo demanda» mediante el uso de «servidores de archivos»,[270] es decir, servicios de internet que permiten subir archivos para acceder a ellos en remoto.[271]Los enlaces a archivos con contenido de abuso sexual infantil se publican en varias páginas y, a menudo, se utilizan como parte del intercambio entre redes de pares.

Esto supone una serie de retos en cuanto a la aplicación de la ley, ya que el material a menudo se publica y se aloja en diferentes jurisdicciones, lo que complica la recopilación de pruebas.[272] El volumen de material que un agresor tenía en su poder había sido siempre uno de los factores utilizados para evaluar el peligro que representaba, pero esto ya no siempre es indicativo de dicho riesgo.[273]

Las aplicaciones para compartir en la nube favorecen el incremento de interacciones con contenido dañino.

Los agresores dependen de la facilidad de uso, la seguridad y la privacidad de las aplicaciones para compartir archivos en la nube donde almacenar y distribuir fotografías y vídeos ilegales. El almacenamiento en la nube permite compartir material de abuso sexual infantil con solo publicar un enlace en un foro, una plataforma o mediante mensajería directa, para así llegar a más agresores más rápidamente.

El estudio de Crisp desvela que los casos de participación o interacción de los usuarios con contenido dañino relacionado con la explotación y el abuso sexual infantil se dispararon a casi 20 millones en el primer trimestre de 2021, más de 5,5 millones más que en el primer trimestre de 2020.

En los cinco trimestres desde enero de 2020 hasta marzo de 2021, Crisp evaluó 1340 elementos que contenían enlaces para compartir contenido considerado de alto riesgo por contexto y por las comunidades donde se compartía. Aquellos enlaces con contenido dañino, tuvieron un número de interacciones que oscilaba entre 20 y 12 746 en casos extremos. Compartir en múltiples ubicaciones y foros a nivel mundial aumentó en gran medida el número total de interacciones con dichos enlaces.

Los perpetradores suelen utilizar el intercambio de archivos en la nube para compartir fotografías y vídeos de manera eficiente tanto con agresores nuevos como conocidos. Para garantizar que el contenido sea accesible durante el mayor tiempo posible, los agresores más diligentes utilizan múltiples plataformas en la nube simultáneamente y esconden la verdadera naturaleza de los enlaces dañinos detrás de una cortina de humo con referencias a otras actividades ilegales (menos graves) o a usos legítimos de intercambio de archivos para evitar ser detectados.

Figura 15: Interacciones del usuario con contenido dañino.

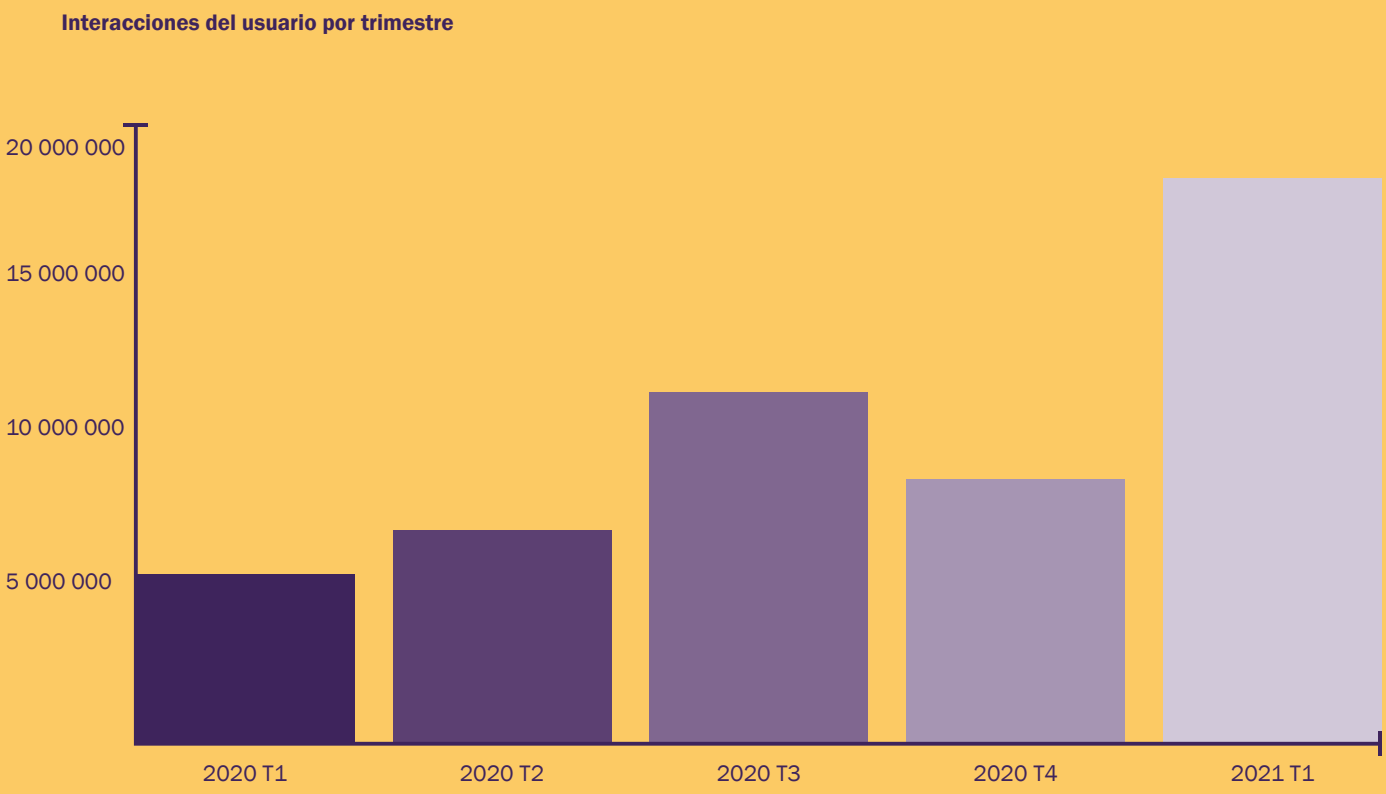


Figura 14: Aumento de material fotográfico versus vídeo de abuso sexual infantil, reproducido con permiso del NCMEC. [263]

Datos sobre tendencias del NCMEC: aumento de imágenes y vídeos de abuso sexual infantil		
Año	Imágenes	Vídeo
2020	33 600 000	31 600 000
2019	27 700 000	41 200 000
2018	23 200 000	22 200 000
2017	17 000 000	3 400 000

En cualquier caso, que el material se comparta de nuevo «vuelve a victimizar y, por lo tanto, a empeorar y avivar todavía más el daño psicológico de la persona que ha sufrido el abuso», impidiendo que pase página, ni siquiera si el agresor es detenido y condenado.

El hecho de volver a compartir material empeora el daño causado.

Una parte significativa de las denuncias de material de abuso sexual infantil están provocadas por el hecho de difundir imágenes ya «conocidas». Facebook ha declarado que más del 90 % de las denuncias que remitió al NCMEC entre octubre y noviembre de 2020 estaban relacionadas con personas que compartían contenido previamente detectado.[274] Un estudio de las denuncias remitidas al NCMEC entre 2011 y 2014 encontró que, de una muestra de 2598 imágenes, se «habían intercambiado activamente» (denunciado al NCMEC cinco veces o más) un 7 % que implicaban a un único agresor y una víctima, y un 12 % con múltiples víctimas o agresores.[275] En cualquier caso, que el material se difunda de nuevo «vuelve a victimizar y, por lo tanto, a empeorar y avivar todavía más el daño psicológico de la persona que ha sufrido el abuso»,[276] impidiendo que pase página, ni siquiera si el agresor es detenido y condenado.[277] A medida que se intensifica el intercambio de información en internet, las políticas «opcionales» de notificación a las víctimas (como las que existen en Estados Unidos) serán cada vez más necesarias para garantizar que el daño no se refuerce involuntariamente cada vez que la policía o las agencias de investigación vuelvan a destapar las imágenes.[278]

Otros problemas relacionados con el hecho de volver a difundir fotografías comprenden el acoso y la persecución de víctimas específicas, una actividad que también permite a los agresores conectarse con personas de ideas afines.

Facebook ha declarado que más del

90 %

de las denuncias que remitió al NCMEC entre octubre y noviembre de 2020 estaban relacionadas con personas que compartían contenido previamente detectado.

Un estudio de las denuncias remitidas al NCMEC entre 2011 y 2014 encontró que, de una muestra de

2598

imágenes se «habían intercambiado activamente» (denunciado al NCMEC cinco veces o más).

Los agresores vuelven a traumatizar a los supervivientes usando perfiles falsos.

Los agresores crean perfiles falsos en internet que se apropian indebidamente de las identidades de las víctimas y los supervivientes conocidos, una táctica que vuelve a victimizarlos. Estas cuentas fraudulentas, que suelen adoptar los nombres de los supervivientes y usan imágenes de cuenta o perfil no dañinas, aparecen en la internet superficial en distintas redes sociales.

Las comunidades de agresores usan estas cuentas para conectar con agresores afines, principalmente para intercambiar contactos. Esto puede conducir a tácticas de explotación comercial, «tradecraft», y la aparición de material de abuso sexual infantil en lo que se considera «espacios seguros» de internet.

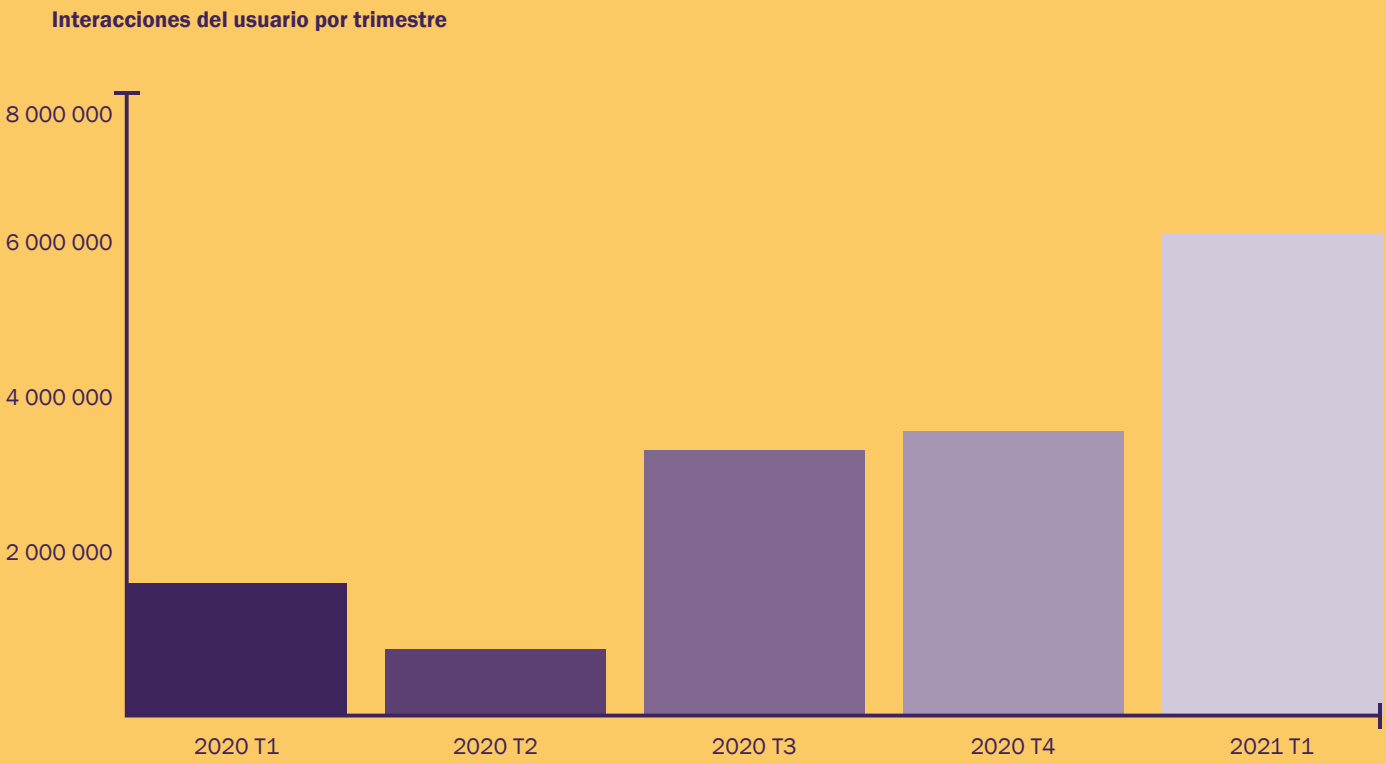
Cada vez más agresores utilizan estas cuentas para transmitir públicamente sus preferencias o intereses y promocionar páginas web comerciales que distribuyen imágenes de abusos.

Crisp ha detectado una tendencia alarmante, las interacciones de los usuarios con perfiles falsos desde el primer trimestre de 2020 hasta el primer trimestre de 2021se han multiplicado por tres.

Por ejemplo, entre enero de 2020 y marzo de 2021, Crisp identificó 3324 archivos que hacían referencia a supervivientes conocidos o a páginas web comerciales. Cada uno de estos archivos dañinos generó de media más de 2000 interacciones («me gusta», comentarios, etc.), lo que provoca un efecto multiplicador y llega a muchos más agresores.

La mayoría de las cuentas presentan discusiones entre agresores y confirman el consumo de este tipo de material. La mayoría hacen referencia a agresiones que tuvieron lugar una década antes de la creación de los perfiles falsos. Esta reavivación de un abuso sexual pasado tiene el efecto de volver a traumatizar a los supervivientes, que vuelven a perder el control de sus identidades en las redes sociales.

Figura 16: Interacciones con contenido que hace referencia a supervivientes conocidos o a páginas web comerciales.



CENTRO NACIONAL PARA MENORES DESAPARECIDOS Y EXPLOTADOS (NCMEC):
La historia de Ella

Un miembro de su familia abusó sexualmente de Ella* desde los cinco años y durante siete años. El abusador de Ella sacó fotos y vídeos del abuso y los distribuyó por internet. El NCMEC rastreó la ubicación del abuso hasta una zona al oeste de Estados Unidos y remitió el caso a la policía local. La policía localizó y rescató a Ella y su agresor fue declarado culpable y sentenciado.

Aunque el agresor se encuentra ahora en la cárcel, las imágenes y vídeos de Ella siguen circulando por internet y otros agresores continúan acosándola. Su cuidador describió el trauma de esta manera: «Se cree que, cuando el agresor va a la cárcel, todo ha acabado, pero no es así... Al principio, estaba extrañamente agradecida por las fotos, porque gracias a ellas lo cogieron. Pero las imágenes siguen ahí, no desaparecen. Decenas de miles de personas las han visto... incluso 10 años después».

A lo largo de los años, Ella ha recibido miles de notificaciones del gobierno sobre casos relacionados con sus fotografías y vídeos. Incluso ya de adulta, esta revictimización hace que Ella tenga una necesidad continua de terapia.

Ella ahora está aprovechando su experiencia para ayudar a otras personas y asesora a supervivientes, contribuyendo al desarrollo de recursos del NCMEC y creando nuevos servicios y programas de ayuda.

El Centro Nacional para Menores Desaparecidos y Explotados (NCMEC) es una organización privada sin ánimo de lucro. Su misión es encontrar a menores desaparecidos, reducir la explotación sexual infantil y prevenir la victimización de los niños y las niñas.

*seudónimo

Facebook analizó el material compartido entre 2019 y mediados de 2020 y concluyó que el 75 % era «no malicioso». Según la clasificación de Facebook, esta difusión de material está motivada, supuestamente, por despecho, humor o venganza.[279] Resultaría útil contar con una mayor transparencia en la clasificación de la difusión «no maliciosa» y las taxonomías establecidas por otras plataformas y así adaptar estrategias para frenar esta tendencia. Una actitud proactiva de los proveedores de servicios de internet es esencial para plantar cara a estos comportamientos y mitigar el riesgo de que el abuso sexual infantil en internet se normalice e incluso se trivialice.

El material de abuso sexual infantil se distribuye con fines de lucro. Detectar este tipo de difusión representa retos únicos.

Según la IWF, aunque la cantidad de páginas web comerciales con material de abuso sexual infantil disminuyó ligeramente (-4 %) respecto al año anterior,[280] la mayoría (61 %) de los dominios analizados en 2020 eran de naturaleza comercial.[281] La IWF continúa vigilando los nuevos medios de monetización de contenido, como los programas de afiliación que permiten a los creadores ganar dinero cada vez que se hace clic en un enlace para acceder a material de abuso sexual infantil.[282]

También ha habido un aumento drástico en el uso registrado de criptomonedas para comprar material de abuso sexual infantil. El importe total de los pagos en Bitcoin y Ethereum, a direcciones vinculadas con proveedores de este tipo de contenido, fue de 930 000 dólares en 2019, un aumento del 212 % con respecto a 2017.[283] Existe una correlación entre esta tendencia y el mayor uso de servicios comerciales ocultos para acceder a contenidos. El número de este tipo de servicios ha aumentado desde 2016[284] y solo aceptan pagos en criptomonedas.[285]

Este intercambio comercial puede suponer retos únicos, ya que los distribuidores a menudo implementan técnicas para frustrar los intentos de detectar y eliminar imágenes. En 2020 se observó un aumento de «páginas web comerciales disfrazadas». Estas páginas evitan ser detectadas mostrando imágenes ilegales solo cuando se accede a ellas mediante «rutas digitales» específicas desde otras páginas. Otras webs comerciales utilizan técnicas que incluyen el denominado «top level domain hopping» para sobrevivir cuando la página original se elimine, lo que consiste en modificar el dominio de una página mientras se conserva su nombre de marca, de modo que todavía pueda ser localizada.[286]

Se necesita más creatividad y una implementación más amplia de herramientas para detectar y frenar la difusión continuada de imágenes.

Es posible detectar eficazmente el material «conocido» mediante dos técnicas relacionadas denominadas «hash» y «hash-matching», que han acelerado significativamente la identificación y eliminación de material de abuso sexual infantil en internet.

Hashing y hash-matching

El «hashing», también conocido como la función resumen, es un proceso que se utiliza para transformar datos de cualquier tamaño en datos de longitud fija mucho más cortos. La secuencia acortada representa los datos originales y se convierte en la firma única del archivo, o su «valor hash».

El «hash-matching» es el proceso mediante el cual se comparan los valores hash del material de abuso sexual infantil conocido, que se encuentra en las bases de datos, con el «hash» del material recién descubierto para así determinar si el contenido ya ha sido denunciado anteriormente. Si es el caso, el proceso para eliminar dicho contenido generalmente se simplifica y, a menudo, se automatiza.[287]

Existen ciertas bases de datos que facilitan el «hash-matching». Una de las más importantes es la de la Interpol, que almacena más de 2,7 millones de «hashes» de material de abuso sexual infantil y que utilizan 64 fuerzas policiales en todo el mundo.[288] Otras son la base de datos de imágenes de abuso infantil del Reino Unido, la lista de hash de la IWF y la CyberTipline del NCMEC.

El «hash-matching» tiene ciertas limitaciones. Cuando se detectan imágenes «conocidas», el host tiene que identificarlas y emitir un aviso de eliminación. A veces, es complicado rastrear la ubicación del servidor del alojamiento, lo que puede retrasar su eliminación.[289] En algunos países se añade el problema de que se ignoran los avisos de eliminación.[290] Es fundamental que los gobiernos, la industria y las fuerzas de seguridad de todo el mundo acuerden una buena colaboración continuada para garantizar una eficacia sostenida de las operaciones.

También es clave que se implemente de manera más amplia la tecnología para mejorar su impacto: aunque la mayoría de los encuestados por la Alianza y Tech Coalition confirmaron que usan el «hash-matching» tanto de imágenes (87 %) como de vídeo (76 %) para eliminar de forma proactiva el material de abuso sexual infantil de sus plataformas,[291] muchas organizaciones aún no contribuyen a las bases de datos existentes con «hashes» ni referencias cruzadas.[292]

La detección y eliminación basadas en hash se pueden optimizar mediante la combinación de listas de hash existentes. Sin embargo, esto se complica debido a las distintas formas de clasificar el material de cada país. La Interpol aplica una etiqueta de referencia para el material considerado ilegal en todos los países y muchas de las fuerzas de seguridad aliadas la utilizan.[293] Sin embargo, es más difícil lograr un consenso global para clasificar las imágenes que revisten menor gravedad. Una mayor colaboración internacional podría mejorar la detección y eliminación de duplicados e incrementar significativamente el impacto general de las tecnologías.[294] [295]

La detección y eliminación de material de abuso sexual infantil de «primera generación» plantea una problemática distinta. Existen herramientas para detectar contenido nuevo, pero están relativamente menos desarrolladas y son técnicamente más complejas que el «hash-matching». Los denominados «clasificadores» de contenido utilizan algoritmos que el aprendizaje automático alimenta para identificar y categorizar el material de abuso sexual infantil. La dificultad para calcular las edades de los menores de las imágenes,[296] y evaluar la gravedad de dichas imágenes, genera más falsos positivos de los que puede cribar el «hash-matching», lo que aumenta la necesidad de intervención humana.[297] Por tanto, debemos mejorar el índice de precisión, reducir la carga de los moderadores e incrementar la aceptación de estas soluciones efectivas y seguras. También debemos trabajar para descubrir cómo los clasificadores y el «hash-matching» podrían funcionar eficazmente con E2EE.

GOOGLE: CONTENT SAFETY API

Content Safety API es una herramienta desarrollada por Google y que proporciona de manera gratuita a las ONG y empresas privadas para respaldar su tarea de proteger a menores. Utiliza inteligencia artificial para ayudar a las organizaciones a priorizar aquellas imágenes que potencialmente contienen abusos para que sean revisadas por humanos, si el contenido no es material «conocido». La identificación rápida de imágenes nuevas aumenta a su vez la velocidad de identificación y la protección de las víctimas, y además reduce la presión sobre los moderadores y revisores.

La herramienta ya ha procesado más de dos mil millones de imágenes y ha contribuido a mejorar la detección y denuncia de material de abuso sexual infantil por parte de algunas empresas, como Yubo, Plugon y Facebook, y varias ONG, como Safernet Brasil.

06 Daños

Material sexual infantil «autogenerado»

El volumen de material sexual infantil «autogenerado» ha aumentado durante la pandemia de la COVID-19.

El material infantil «autogenerado» representa un porcentaje cada vez mayor del contenido de abuso sexual infantil. Esto plantea retos muy complejos para los legisladores y exige una respuesta matizada.

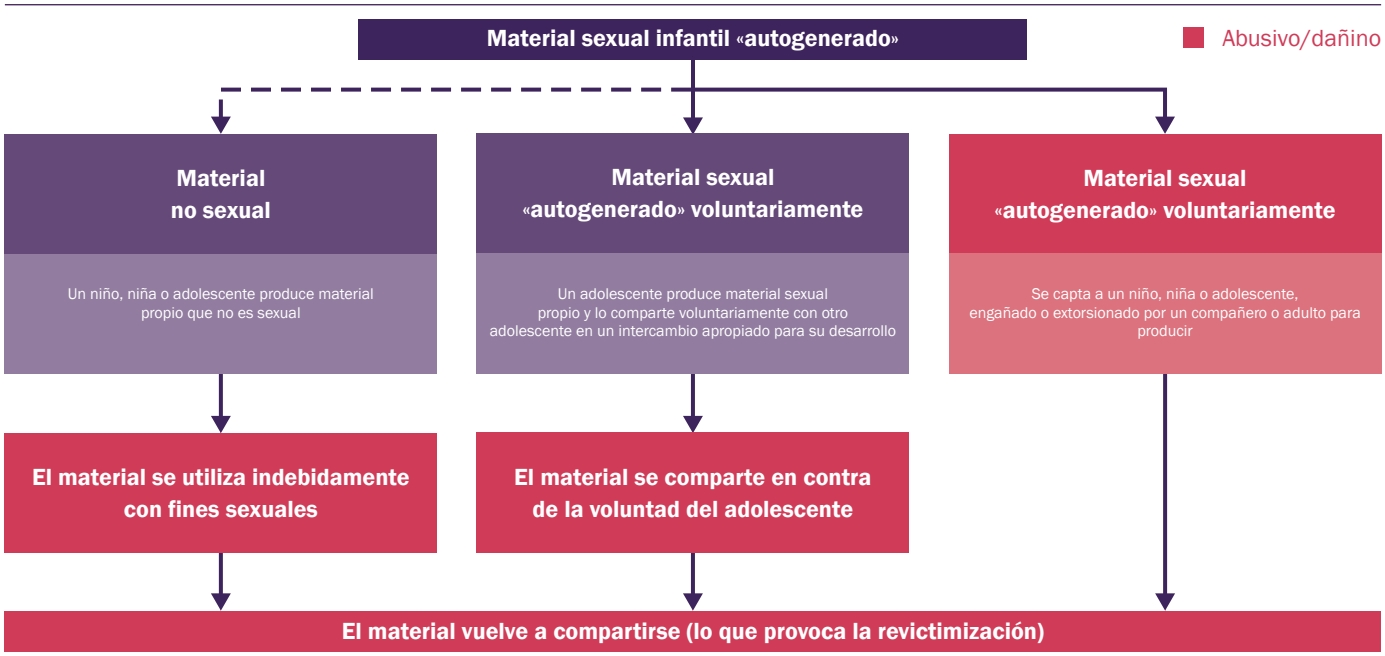
La IWF presentó un estudio transversal del contenido «autogenerado» en su Informe Anual de 2012.[298] En 2017, la ECPAT también lo describió como una «tendencia actual» y atribuyó el creciente volumen de material «autogenerado» a la cantidad mercantilizada de imágenes «recién producidas, nunca antes vistas», lo que las convierte en una «moneda» muy valiosa para los agresores.[299]

Recientemente, el volumen de material «autogenerado» se ha disparado drásticamente.

La IWF recibió 68 000 denuncias de material sexual «autogenerado» en 2020, un aumento del 77 % con respecto a 2019. En general, el contenido «autogenerado» representó el 44 % de las denuncias realizadas por la IWF en 2020.[300]

Este aumento se ha atribuido en parte a la «tormenta perfecta» creada por la pandemia de la COVID-19, que llevó a los menores a pasar más tiempo conectados y redujo las oportunidades de los agresores para cometer abusos «en persona», lo que provocó un aumento de las agresiones en línea y la demanda de imágenes.[301]

Figura 17: Principales categorías de material sexual «autogenerado» y los daños asociados.



Las razones que llevan a la «autoproducción» son complejas y variadas.

Hay tres categorías generales de material «autogenerado» (véase Figura 17):

- El material no sexual es contenido «autogenerado» que no es propiamente de naturaleza sexual, pero del que los agresores se apropian indebidamente para utilizarlo con intenciones de explotación y abuso sexual infantil en línea.[302] Aunque las víctimas pueden no estar al corriente, dicho material es dañino principalmente porque permite que los agresores se mantengan activos. En algunos casos, también se causa un daño directo a las víctimas al manipular las imágenes para que parezcan sexuales, chantajeándolos después con la amenaza de compartirlas.[303]
- El material «autogenerado» voluntariamente suele compartirse entre adolescentes. Esta categoría comprende solo la «autoproducción» de adolescentes, porque los niños y las niñas más pequeños no pueden dar su consentimiento y, por lo tanto, su «autoproducción» no puede considerarse «voluntaria». Por norma general, en estos casos el daño se produce cuando las imágenes se comparten (o se vuelven a compartir) en contra de los deseos del menor. En 39 estudios en los que participaron 110 380 jóvenes de entre 12 y 17 años, el 12 % afirmó haber reenviado una imagen sexual «autogenerada» sin permiso.[304] El estudio de Economist Impact realizado junto con este informe también reveló que el 29 % de los encuestados reportaron que se habían compartido imágenes o vídeos sexualmente explícitos suyos sin su consentimiento. Al mismo tiempo, también se puede causar daño a los destinatarios y destinatarias si reciben material «autoproducido» voluntariamente sin que ellos lo hayan solicitado.[305]
- La «autogeneración forzada» consiste en la captación de menores para que generen imágenes sexuales y está relacionada con el «capping».[306] Los menores involucrados en la «autoproducción forzada» pueden no verse a sí mismos como víctimas y pueden considerar que sus acciones son voluntarias.

Los caminos que conducen a la «autoproducción» son variados y suponen un reto para los servicios de ayuda. Si bien el contenido de la imagen y el vídeo puede ajustarse a la definición legal de «material de abuso sexual infantil» y, por tanto, es posible abrir un proceso legal en contra, la intención que motiva la creación o el envío de tales imágenes puede no ser tan evidente. Comprender el contexto de la producción y la difusión es fundamental para garantizar una respuesta adecuada en todo momento y, por ello, siempre es necesario que se estudie caso por caso.

INTERNET WATCH FOUNDATION
Material sexual «autogenerado» entre hermanos

La Internet Watch Foundation (IWF) es una organización de protección infantil que utiliza la tecnología para encontrar y eliminar material de abuso sexual infantil de internet.[307]
En 2020, la IWF constató un aumento alarmante en el volumen de material «autogenerado» en internet.[308] Dentro de estos materiales, los analistas observaron una tendencia particularmente inquietante: depredadores que engañaban a menores para que implicaran a otros menores en la «autoproducción».

El análisis de las imágenes sexuales «autogeneradas» denunciadas ante la IWF entre septiembre y diciembre de 2020 reveló que:

511
imágenes y vídeos incluían a hermanos

65 %
de los casos, uno o ambos menores tuvieron contacto sexual directo con el otro

46 %
de este material se clasificó como contenido de Categoría A, que engloba las formas más graves de abuso sexual infantil

En muchos casos, los menores habían sido manipulados o coaccionados por adultos para transmitir en directo la actividad sexual, y los vídeos y las capturas de pantalla se habían compartido en diversas plataformas web. Algunos adultos se habían hecho pasar por menores y, a veces, hacían pasar el abuso por un juego o una «apuesta». Los niños implicados rara vez parecieron entender la naturaleza sexual de lo que se les obligaba a hacer.

Aunque hay indicios de que compartir imágenes sexuales no es una práctica aislada entre los jóvenes (véase Figura 18), algunos menores se sienten más presionados a hacerlo, lo que los hace más vulnerables a la coerción y/o al riesgo de que se comparta el material sin su consentimiento.

HAMOGELO:
La historia de María

María* tiene 15 años y vive en Grecia. Empezó a hablar con Yannis*, un joven de 20 años, a través de una aplicación de citas que empezó a usar por curiosidad y aburrimiento. Debido a las restricciones del confinamiento no podía ir al instituto ni participar en sus actividades habituales.

Yannis le preguntó cómo era su vida durante la pandemia, parecía interesado en lo que ella le contaba y compartía sus inquietudes. Hablaban todos los días y, poco a poco, fueron cogiendo confianza.

Al final, Yannis forzó a María para que le mandara fotografías de carácter sexual «autogeneradas». La convenció de que era un paso normal en su «relación» y que sería su secreto. Con el tiempo, Yannis le pidió más y más fotografías, y también vídeos.

María intentó negarse, pero Yannis la amenazó con publicar las imágenes en las redes sociales. Desesperada, buscó ayuda por internet y encontró el teléfono de asistencia de Hamogelo, el 1056.

Este teléfono le proporcionó apoyo y asesoramiento de manera anónima y le infundió fuerzas para explicar el problema a sus padres. Juntos volvieron a llamar al teléfono de asistencia y el caso se derivó a la división de ciberdelincuencia de la policía griega, que finalmente arrestó a Yannis.

Hamogelo, o «La sonrisa del niño», es una organización griega que ayuda a menores que se enfrentan a situaciones de violencia, abuso, extorsión, pobreza o problemas de salud. Hasta la fecha, han ayudado a más de 1,7 millones de niños y familias.

*seudónimos

Una encuesta reciente reveló que los adolescentes flamencos que se identificaban como LGBTQ+ recibían más presiones para compartir imágenes de naturaleza sexual que sus compañeros heterosexuales.[309] Un estudio sobre adolescentes, «sexting» y los riesgos asociados realizado por la organización benéfica británica Internet Matters también concluyó que los «grupos vulnerables» (menores con una o más discapacidades físicas, cognitivas o sociales) tienen muchas más probabilidades de recibir presiones o ser chantajeados para que compartan desnudos.[310] El acoso sexual en forma de solicitudes persistentes de material «autogenerado» parece ser una práctica bastante frecuente en algunos países. Una encuesta realizada por la oficina no ministerial de educación de menores del Reino Unido (OFSTED) encontró, en una muestra de 900 jóvenes, que el 80 % de las niñas habían recibido presiones para compartir imágenes sexuales de sí mismas «muchas veces» o «algunas veces». Otras posibles causas para la «autoproducción» incluyen un historial previo de abusos, participación en «comportamientos más arriesgados en internet y en el mundo real» y el uso frecuente de chats.[311] [312]

Según la IWF, las niñas en la adolescencia temprana tienen muchas más probabilidades de aparecer en este tipo de imágenes: el 95 % del contenido sexual «autoproducido» reportado a la organización en 2020 incluía a niñas de 11 a 13 años.[313] Sin embargo, otros estudios sugieren que una cantidad igual o mayor de niños también «autogeneran» estos contenidos:

- Una encuesta de Estados unidos a 1000 jóvenes de entre 13 y 17 años concluyó que uno de cada diez niños (una de cada cinco niñas) había compartido sus propios desnudos.[314]
- Una encuesta realizada por internet a 1001 jóvenes de entre 13 y 17 años del Reino Unido reveló que un número similar de niños y niñas se habían fotografiado a ellos mismos completamente desnudos.[315]
- Una encuesta realizada con 500 jóvenes de entre 13 y 24 años del valle de Katmandú, en Nepal, concluyó que el 18 % de los niños y el 5,2 % de las niñas reportaron haberse fotografiado desnudos.[316]

Hace falta una investigación más exhaustiva para comprender hasta qué punto el género es un factor de riesgo y si influye en los distintos tipos de daño relacionados con el material sexual «autogenerado» por los menores (por ejemplo, producción forzada versus «autoproducción» voluntaria). Otros peligros que pueden desembocar en la «autoproducción» están vinculados al uso de internet de los menores. El aumento del uso de dispositivos móviles[317] limita la capacidad de supervisión de los padres que, junto con la facilidad de acceso a plataformas y contenido para adultos (debido a la falta de controles de verificación de edad o a controles que se evitan fácilmente),[318] favorece las condiciones para la «autoproducción», incluso en ausencia de otras causas que contribuyan al riesgo.

La pobreza derivada de la COVID-19 puede provocar un aumento de la «autogeneración» a cambio de dinero.

La «autoproducción» con fines comerciales es aquella que se realiza cuando los menores crean imágenes o vídeos sexuales de sí mismos para ganar dinero. En todo el mundo están creciendo las denuncias de «autoproducción» con fines comerciales. En Filipinas, las autoridades han descubierto casos de adolescentes que crean grupos en redes sociales con el fin de vender imágenes y vídeos sexuales «para financiar gastos de formación en línea». Uno de estos grupos llegó a tener 7000 miembros antes de que se desmantelara.[319] En Camboya, algunos jóvenes (en su mayoría niñas) utilizan su material sexual para vender productos cosméticos en internet. Las encuestas realizadas a jóvenes camboyanos sugieren que esta actividad puede culminar en un abuso sexual grave.[320] El NCMEC ha puesto de relieve casos de menores desaparecidos que luego se descubrió que vendían su material sexual en plataformas bajo suscripción y se encontraron pruebas de un vínculo con la explotación y la trata organizadas. [321]

Independientemente de las circunstancias, se puede afirmar que prácticamente todos los casos de «autoproducción» con fines comerciales son perjudiciales para el menor y lo más probable es que el material producido sea ilegal. Este problema requiere una respuesta urgente y mesurada por parte de los legisladores. La encuesta de Netclean de 2020 sobre la aplicación de la ley a nivel mundial confirmó que algunos países ya habían experimentado un aumento de la «autoproducción» a cambio de dinero durante la pandemia, mientras que otros predijeron un mantenimiento de la tendencia a medida que las condiciones económicas empeoraran, como un medio para los menores «de ganar dinero para cosas que de otro modo no podrían sufragar".[322]

El daño causado por el material «autogenerado» abarca también el acoso, el intercambio de información y la culpabilización de las víctimas.

La IWF ha sido testigo de algunos casos en que los agresores que consumen contenido «autogenerado» intentan identificar y localizar a las víctimas con la intención de obligarlas a crear más contenido.[323] En otros casos, es posible que estos agresores sean conocidos por el menor, puesto que, al igual que ocurre con el «abuso en persona», a menudo son «personas en las que los menores confían y de las que dependen».[324] Ambos factores pueden crear una sensación de inevitabilidad del abuso, que se amplifica cuando se vuelven a compartir las imágenes. En 2014, la IWF analizó más de 3800 imágenes y vídeos sexuales «autogenerados» y descubrió que el 90 % se había «obtenido de la ubicación de carga original y se estaba redistribuyendo en páginas web de terceros».[325]

Es probable que el daño causado por el material «autogenerado» se vea agravado por la tendencia a culpar a la víctima. Según una encuesta de Thorn, el 60 % de los menores culpan a la víctima cuando se vuelve a compartir material «autogenerado», mientras que el 55 % de los cuidadores también cree que la víctima es la principal o la única culpable de que este material se haya vuelto a compartir.[326] Estas actitudes socavan las posibilidades de que los menores den un paso al frente y presenten testimonios y denuncias, ya que alimentan su estigma.

Las iniciativas para facilitar las denuncias y las soluciones tecnológicas pueden frenar el aumento de material «autogenerado», pero la prevención exige un enfoque más matizado.

La campaña «Report Remove» se lanzó en el Reino Unido en 2020 para facilitar que los menores denunciaran anónimamente el material «autogenerado» y solicitaran su eliminación.[327] Este tipo de iniciativas reducen las barreras que los menores pueden encontrar a la hora de denunciar su caso. Los controles a nivel de dispositivos que evitan fotografiar y grabar vídeos sexuales también pueden ser un «parche» eficaz para frenar el aumento de la «autoproducción». Un ejemplo es el detector de amenazas en imágenes y vídeos «SafeToWatch» (véase el estudio de caso en la página siguiente). Estas soluciones plantean un dilema sobre el derecho a la privacidad que deberá ser cuidadosamente considerado a la hora de aceptarlas e implementarlas.

La prevención sostenible a largo plazo requerirá enfoques muy mesurados, basados en las experiencias complejas de los niños y los jóvenes que batallan con el autodescubrimiento en la era digital. Dado que compartir imágenes sexuales «autoproducidas» es una práctica relativamente común y no siempre supone un daño, centrarse en exceso en sus posibles efectos negativos podría «suscitar consejos que serían rechazados, puesto que no se corresponden con las experiencias habituales de los jóvenes».[328] La educación será clave para evitar que los niños y las niñas sufran coacciones y deban afrontar las consecuencias negativas de la «autoproducción voluntaria». Las iniciativas educativas deben contribuir a fomentar un desarrollo sexual saludable y una mayor comprensión del consentimiento.[329] Un ejemplo de una de estas iniciativas es la campaña «Send me a pic» («Envíame una foto») de la NCA, cuyo objetivo es favorecer un diálogo constructivo con los jóvenes sobre el intercambio de desnudos.

SAFETONET: SAFETOWATCH

SafeToNet es una empresa de seguridad tecnológica que utiliza la inteligencia artificial y el análisis de comportamiento para contribuir a proteger a los menores en internet. SafeToNet considera que deben integrarse características de diseño seguras en los dispositivos y sistemas operativos.

La última innovación de SafeToNet es SafeToWatch, un detector de amenazas en fotografías y vídeos que puede interrumpir la creación de material de abuso en tiempo real y en origen. Utiliza varias entradas, como la de audio y vídeo, para evaluar el entorno digital y aplica un conjunto de algoritmos para permitir la detección en tiempo real de material de abuso sexual infantil. SafeToWatch funciona de la misma manera tanto si el contenido lo está emitiendo en directo un tercero como si es «autogenerado» por el propio menor. La detección de estas imágenes desencadena inmediatamente la restricción de cámaras y micrófonos, lo que puede provocar que una aplicación, o todo el dispositivo, deje de ser operativo, evitando así que se haga la foto o el vídeo. Las imágenes no se conservan, respetando el derecho de los menores a la privacidad. A diferencia de las herramientas de detección a nivel de plataforma, la tecnología se puede implementar fácilmente en entornos cifrados de extremo a extremo. Para que SafeToWatch y otras innovaciones similares tengan éxito, es fundamental tener un acceso fiable a los datos gubernamentales y policiales para entrenar algoritmos y optimizar la efectividad de estas soluciones.

SafeToNet ha adquirido 77 tiendas de telefonía móvil en Alemania para llevar la ciberseguridad a pie de calle.[330]

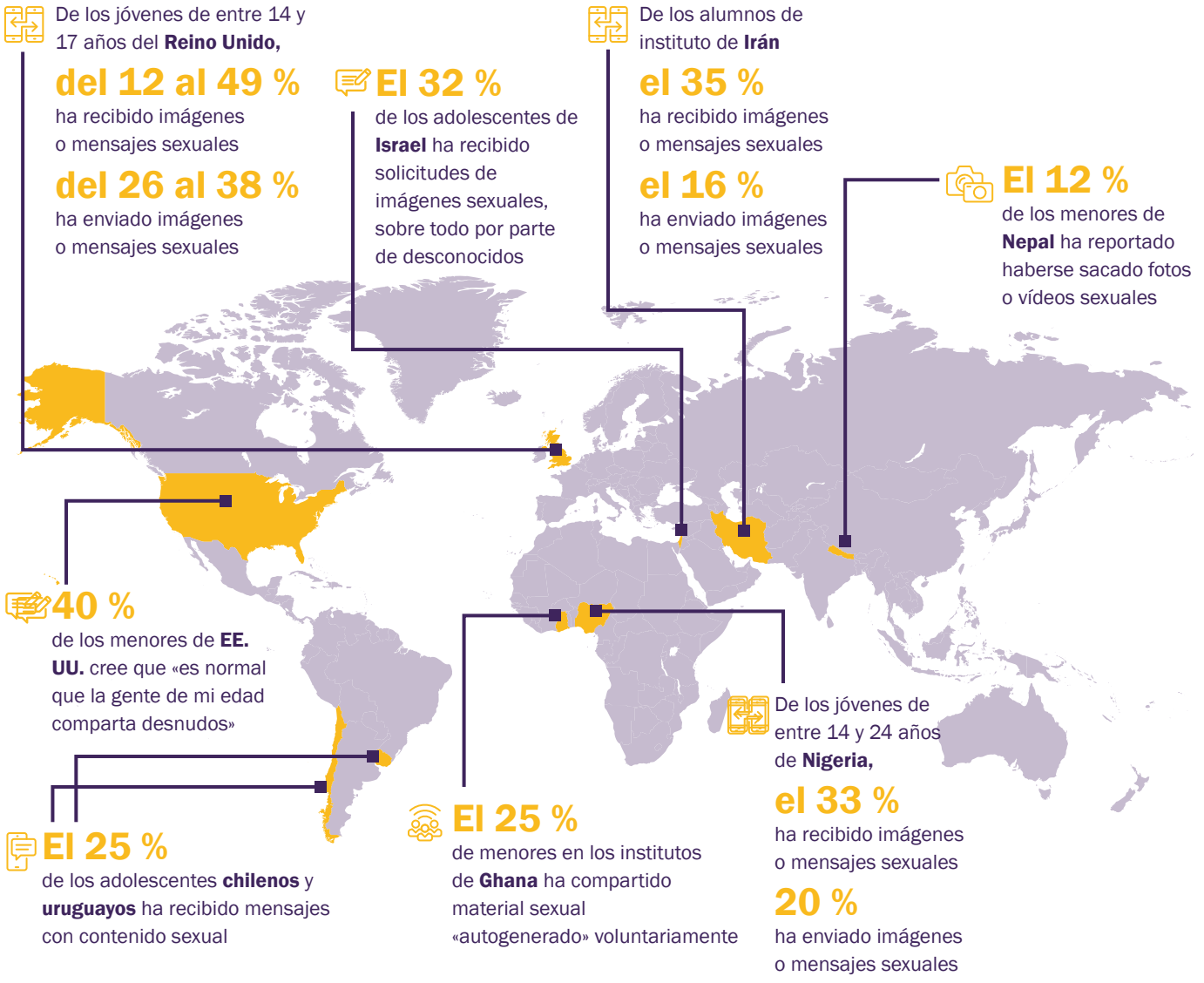
En algunos países, los cambios en la legislación permitirían una respuesta más eficaz y centrada en los menores en materia de material sexual «autoproducido» voluntariamente.

Algunos marcos legales requieren una reforma urgente para prevenir la criminalización continua de los menores por comportamientos que posiblemente formen «parte integral del descubrimiento normal de su sexualidad».[331]

En este sentido, en algunas regiones de Australia se ha despenalizado el «sexting» entre iguales.[332] Según el Convenio de Lanzarote, esto es posible, puesto que en sus términos se contempla una «exención» para tipificar como delito el abuso sexual infantil entre menores si se cumplen determinados aspectos. Esta guía puede ayudar a los países a establecer una respuesta adecuada para los niños y adolescentes que participan en la generación, el consumo o el intercambio de contenido «autogenerado».[333] En el Reino Unido, el número de jóvenes que pasaron por un proceso judicial en relación con material sexual «autogenerado» se duplicó entre 2007 y 2016.[334] Recientemente, el gobierno aconsejó a los profesionales de la educación que «no se criminalice a los niños y los jóvenes por 'compartir desnudos y semidesnudos'».[335]

Sin embargo, algunos jóvenes cruzan la línea y adoptan una conducta sexual dañina y de abuso. Como destaca UNICEF, «los compañeros son responsables en muchos casos de los actos de abuso sexual contra otros niños y adolescentes».[336] Esta situación deja también al descubierto un vacío de actuación, porque «las intervenciones se han diseñado principalmente para tratar con agresores adultos».[337] El problema del material sexual «autogenerado», que en muchos casos es un daño causado por compañeros, demuestra la importancia de adoptar estrategias que aborden las necesidades de los menores que sufren abusos y que participan en comportamientos sexuales perjudiciales contra otros compañeros.[338]

Figura 18: ¿Hasta qué punto es habitual el intercambio de imágenes y mensajes sexuales entre los jóvenes? [339 340 341 342 343 344 345 346]



06 Daños

Transmitir en directo explotación y abuso sexual infantil

El streaming en directo es cada vez más común, propiciado por la conectividad y la disponibilidad en el mercado de dispositivos económicos.

La transmisión en directo puede implicar el abuso «en persona» de uno o más menores emitido por internet, o un menor o menores obligados a llevar a cabo actos sexuales frente a una cámara web, generalmente a cambio de dinero.

El streamaing en directo es cada vez más común, propiciado por la conectividad y la disponibilidad en el mercado de dispositivos económicos. A menudo se manifiesta como un delito transfronterizo que requiere una respuesta internacional coordinada.

A diferencia de la transmisión en directo «autogenerada» (véase capítulo Daños: *Material sexual infantil «autogenerado»*), este tipo de abuso normalmente lo facilita un tercero. Aunque hay casos en que la víctima y los abusadores se encuentran en la misma localidad, la mayoría de los delitos traspasan las fronteras nacionales. Como explica la ECPAT, este tipo de abuso «tiende a aprovechar las desigualdades económicas, por lo que delincuentes de países desarrollados acceden a víctimas de países en vías de desarrollo».[347] Este problema ilustra el daño causado por las desigualdades globales en un mundo cada vez más conectado.

Según la Interpol, el streaming en directo de pago está aumentando.[348] Hay indicios que sugieren que esta tendencia se está agravando con la pandemia. En Filipinas, descrita por UNICEF como el «epicentro mundial del tráfico de abusos sexuales en directo»,[349] se registró un aumento del 265 % de casos durante la cuarentena de marzo a mayo de 2020. Save the Children ha establecido un vínculo entre este tipo de abuso y el agravamiento de la pobreza, lo que sugiere que las dificultades económicas creadas por la COVID-19 están impulsando a más personas a transmitir en directo por dinero.[350]

El streaming implica varios delitos. La mayoría de las víctimas identificadas se encuentran en el Sur global, pero el abuso tiene lugar en muchas otras regiones del mundo.

En una transmisión en directo, se considera que tanto los que organizan la explotación como los que manejan y consumen el contenido son abusadores. Las personas que organizan el abuso pueden pertenecer a grupos criminales organizados, pero también pueden formar parte del círculo de confianza de la víctima. A través del análisis de casos de transmisión en Filipinas, la IJM denunció que la mayoría de los agresores (el 69 %) eran familiares adultos o conocidos cercanos de las víctimas que actuaban por motivaciones económicas.[351] El hecho de que los «facilitadores» de la transmisión en directo actúen principalmente por un interés económico diferencia este delito de muchas otras formas de abuso sexual infantil.

Los datos indican que las personas que «consumen» abusos transmitidos en directo son predominantemente de Europa, América del Norte y Australia.[352] Estos agresores buscan contenidos de abuso transmitido en directo desde regiones del mundo «con altos niveles de pobreza, medidas de protección infantil domésticas limitadas y fácil acceso a los menores».[353] La acción penal contra los agresores «que demandan este tipo de material» ha tendido a centrarse solo en el consumo, lo que contribuye a restar importancia a su implicación en el delito. Como explica la IJM, hay quienes defienden que se debería procesar a estas personas por traficantes, ya que «abusan de su poder económico» al pagar por la explotación, delito que encajaría en la definición de trata de personas establecida en el Protocolo de Palermo.[354]

La mayoría de las víctimas de transmisiones en directo identificadas viven en el Sudeste Asiático, sobre todo en Filipinas,[355] pero también hay víctimas en países como Europa, Rusia y Estados Unidos.[356] Esto destaca la importancia de evitar una tipificación limitada del streaming en directo como un delito que solo afectaría a niños y jóvenes de países con bajos ingresos.[357] Además de causar un gran trauma y sufrimiento a las víctimas, según un estudio de casos en el Sudeste Asiático, la transmisión en directo también podría representar para los niños y las niñas «una puerta de entrada a la explotación sexual fuera de línea por motivos económicos».[358]

INTERNATIONAL JUSTICE MISSION: La historia de Ruby

A los 16 años, Ruby* fue privada de su libertad y los agresores online la obligaron a hacer todo lo que le decían mientras transmitían en directo el abuso sexual.

La pesadilla de Ruby comenzó cuando un traficante le envió un mensaje privado a través de las redes sociales proponiéndole un trabajo de dependienta en una tienda de ordenadores. El traficante se ganó su confianza. Le ofreció alojamiento y comida gratis mientras trabajara para ellos. También corrió con los gastos del viaje para que se reuniera con él y su cómplice. Ruby pronto descubrió que el trabajo no era lo que le habían prometido. Quiso marcharse, pero no podía hacerlo hasta que saldara lo que se había convertido en su «deuda» del viaje, cosa que se volvió casi imposible debido a que sus «ingresos» servían para pagar los productos sobrevalorados que le vendía el propio traficante. Incluso intentó escapar, pero la amenazaron con un cuchillo.

Ruby describe el abuso con sus propias palabras:

«Me pagaban por cada espectáculo asqueroso que hacía frente a la cámara del ordenador con un cliente. Y, mientras hacía todos esos espectáculos asquerosos, perdí toda la autoestima que me quedaba, hasta el punto de darme asco a mí misma.»

Es como estar encerrada en una habitación oscura sin un rayo de luz. La vida no tiene ningún sentido.

«Haces espectáculos asquerosos todos los días, una y otra vez y, luego, después de hacerlos, te vas a dormir y repites la misma rutina todos los días. Es como si no tuviera fin».

La IJM ayudó a las autoridades filipinas a actuar gracias a un aviso de la Oficina de Investigaciones de Seguridad Nacional de Estados Unidos (HSI) para identificar la ubicación de Ruby y rescatarla, junto con cinco niñas más. La pareja que dirigía la operación fue declarada culpable y condenada y la IJM ayudo a Ruby a recuperarse. Ruby explica así su proceso de recuperación: «No fue nada fácil. Me llevó años, necesité años para recuperarme de esas experiencias tan dolorosas, tan traumáticas. Por las noches, cuando alguien apagaba de repente la luz, me levantaba de la cama, no podía dormir si apagaban la luz, me aterraba la oscuridad. Y esto duró muchos años».

Hoy, Ruby es libre, está a salvo y planea licenciarse en derecho con la esperanza de ayudar a otras niñas que se encuentren en circunstancias similares.

La International Justice Mission es una ONG que colabora con sistemas judiciales locales de todo el mundo para acabar con la violencia contra personas que viven en la pobreza. A través de su Centro para erradicar la explotación sexual infantil en internet, fortalece los sistemas de protección contra la producción de material de abuso sexual infantil, incluidas las transmisiones en directo.

*seudónimo

Que los límites entre la transmisión en directo y la trata sean cada vez más difusos complicará aún más las investigaciones de estos delitos.

A nivel mundial, un tercio de las víctimas de trata detectadas son menores. De estos, el 72 % de las niñas y el 23 % de los niños son objeto de trata con fines de explotación sexual.[359] La trata de menores habitualmente implica formas de abuso en línea y se ha relacionado con el aumento del volumen de material de abuso sexual infantil. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) destaca el caso de los traficantes de Tailandia, «que explotan sexualmente a un gran número de menores y producen varios cientos de miles de imágenes para su distribución por internet».[360]

Es probable que cada vez sea más difícil separar el streaming en directo del tráfico de personas, debido a que muchos traficantes están trasladando su modelo de negocio a internet para eludir el impacto de las restricciones de la COVID-19.[361] Como se pone de relieve en el informe sobre la trata mundial de la UNODC de 2021, las ventajas que representan las tecnologías de internet para los traficantes son significativas, sobre todo porque, en general, «permiten llegar a un público más amplio que con la trata tradicional».[362] Existen indicios de que la transmisión en directo se ha vuelto cada vez más popular debido a la pandemia, como una alternativa al abuso sexual infantil en persona.[363] Podría decirse que los traficantes de internet están bien posicionados para aprovechar esta mayor demanda de «servicios remotos».

Cuando la transmisión en directo forma parte de la trata de menores, puede suponer retos adicionales que complican las investigaciones. Por ejemplo, en Filipinas, UNICEF descubrió que los casos de trata que presentan explotación por internet «se confunden con casos de delitos informáticos», un problema que puede suponer retrasos en la derivación de los casos.[364] Las víctimas de la trata también suelen ser más difíciles de identificar, precisamente debido a que se solapan con otras formas de abuso.[365]

A nivel mundial, un tercio de las víctimas de trata detectadas son menores. De estos,

UN 72 % DE LAS NIÑAS Y **UN 23 % DE LOS NIÑOS**

son objeto de trata con fines de explotación sexual.

Se necesita una colaboración más proactiva entre la policía y los proveedores de servicios financieros y de internet para mejorar la detección de abusos transmitidos en directo.

Técnicamente es posible interrumpir la emisión en directo. Como se describe en el Capítulo Daños: *compartir y/o almacenar material de abuso sexual infantil*, existen clasificadores para detectar el material de abuso sexual infantil. Sin embargo, la mayoría de los abusos transmitidos en directo se emiten en línea dentro de «conversaciones» privadas que no están sujetas a la revisión ni a la filtración del moderador. A menos que un agresor la grabe, la transmisión no suele dejar rastro. La falta de pruebas también dificulta la condena por estos delitos, un reto que se agrava con la ausencia de legislación que penalice esta práctica.[366] Los consumidores de abusos vía streaming en directo, generalmente no necesitan una gran sofisticación técnica (la mayoría de las transmisiones en directo se producen en la internet superficial),[367] posiblemente porque perciben que la probabilidad de ser detectados y condenados es baja.

Algunos usuarios podrían considerar que la supervisión de conversaciones privadas para detectar transmisiones en directo es una violación de la privacidad justificable, pero incluso si se aceptaran estos mecanismos y algunos proveedores de servicios de internet los implementaran, los agresores podrían simplemente migrar a cualquiera otra plataforma E2EE, cada vez más abundantes. Esta función, que oculta el contenido de las comunicaciones, hace imposible detectar las emisiones de esta naturaleza, por lo que una vez más se pone de manifiesto la necesidad imperiosa de diversificar los métodos de interrupción.

Muchos consideran que los indicadores financieros son las «pistas» más eficaces para identificar los abusos transmitidos en directo. Se han llevado a cabo colaboraciones con el sector financiero que han obtenido resultados muy positivos. Por ejemplo, en 2017 una iniciativa logró la casi total eliminación del uso de tarjetas de crédito para adquirir contenido de abuso sexual infantil online en Estados Unidos.[368] El Centro Australiano de análisis e informes de transacciones también aprovechó con éxito su asociación público-privada con Fintel Alliance para bloquear transacciones vinculadas con la explotación infantil.[369]

Asimismo, muchas agencias policiales y proveedores de servicios financieros colaboran para investigar delitos de transmisión en directo. Sin embargo, aún se puede adoptar un enfoque más proactivo. Como expone la IJM, dado que las empresas «normalmente cumplen» cuando las fuerzas de seguridad les solicitan información, es importante que también «identifiquen, informen e interrumpan de manera proactiva[…] las transferencias de dinero en tiempo real».[370] El potencial de una colaboración tan estrecha puede verse obstaculizado por la diversificación continua de los servicios financieros. Un mayor uso de las criptomonedas también podría crear dificultades, ya que, aunque es posible rastrear este tipo de pagos, no todas las agencias policiales poseen los conocimientos necesarios.[371]

En 2020, el Grupo Egmont (un consorcio de unidades de inteligencia financiera mundial) llevó a cabo un estudio sobre cómo la inteligencia financiera puede combatir el streaming en directo. El estudio destacó algunos inconvenientes, como la dificultad para distinguir las transacciones de los pagos por contenido sexual para adultos de las actividades fraudulentas u otros delitos. En general, concluye que sería bueno «combinar información financiera» con otras fuentes a través del intercambio de datos entre organismos judiciales y el sector privado.[372] Los resultados del proyecto demuestran la importancia de la coordinación multisectorial para abordar de manera efectiva el abuso transmitido en directo. Estableciendo los marcos adecuados para permitir el intercambio legal de datos, la información de los proveedores de servicios de internet podría suponer un complemento muy potente para la inteligencia financiera. Esto podría incluir, por ejemplo, «señales» (metadatos e indicadores de comportamiento) que apunten a una actividad potencialmente perniciosa por parte de los usuarios.

La prevención continuada de la transmisión en directo requiere la educación y el empoderamiento de la comunidad, la mejora de la capacidad policial y una mayor coherencia del tratamiento global.

Un análisis de UNICEF de casos de abuso sexual infantil por internet en Filipinas encontró que la familia o la comunidad de la víctima facilita en muchos casos la transmisión en directo y que ciertas creencias culturales la «justifican». Por ejemplo, la idea de que no se causa ningún daño si no se llega a tocar al menor, así como la expectativa de que los menores ayuden económicamente a sus familias.[373] Este contexto complica la protección de los menores (ya que, en estas circunstancias, puede que ni siquiera reconozcan el abuso) e impone una responsabilidad mayor para las agencias de protección, ya de por sí sobrecargadas. La educación y el empoderamiento de la comunidad son por tanto fundamentales a la hora de prevenir la transmisión en directo, aumentando la conciencia del daño que este tipo de abuso supone, erradicando una serie de creencias perjudiciales y fomentando prácticas de protección. Las iniciativas que dan voz a los menores también son cruciales para que puedan denunciar el abuso y buscar ayuda.

Actualmente, no existe una definición acordada internacionalmente para el delito de transmisión en directo de explotación y abuso sexual infantil. Y aunque en muchos países este delito se englobaría dentro de las disposiciones relativas a la explotación sexual infantil,[374] esto sigue representando un inconveniente para la colaboración en la aplicación de la ley y limita la capacidad de desarrollar líneas de investigación consistentes. También implica que los agresores pueden librarse de la pena en virtud de la cláusula de «doble criminalidad», que establece que la conducta debe estar penalizada tanto en el país de origen del delincuente como en el país donde se cometió el delito.[375]

En algunos países, las limitaciones para investigar también reducen las probabilidades de detectar y condenar a los delincuentes. Por ejemplo, en Australia, el 90 % de los procesos judiciales por streaming en directo que culminan con éxito se apoyan en tácticas encubiertas, pero en Camboya las investigaciones encubiertas no están permitidas por la ley.[376] En México, el desconocimiento de los legisladores acerca de este tema obstaculiza los esfuerzos para combatir este tipo de delito, lo que impide que haya consenso integral sobre los métodos de detección e investigación.[377]

Actualmente, no existe una definición acordada internacionalmente para el delito de transmisión en directo de explotación y abuso sexual infantil.

07

Recomendaciones

La Evaluación de la amenaza global de este año demuestra que la dimensión de la explotación y el abuso sexual infantil en internet sigue creciendo.

Las siguientes recomendaciones permitirían a los gobiernos, la sociedad civil, las comunidades y los proveedores de servicios de internet aprovechar la evolución positiva para mejorar la respuesta y la prevención ante las amenazas. Estas recomendaciones van de la mano del marco de Respuesta Estratégica Global de la Alianza Global de WeProtect.[378]

La explotación y el abuso sexual infantil en internet es un problema global que requiere una colaboración internacional continua y un diálogo transversal. La Alianza responde a esta necesidad facilitando el compromiso entre los gobiernos, el sector privado y la sociedad civil, a la vez que genera un compromiso político y desarrolla enfoques prácticos para lograr que el mundo digital sea seguro para los menores.

Para más información, visite: www.weprotect.org

Tema	Recomendación
Financiación	**Los gobiernos, el sector privado y la sociedad civil** deben destinar fondos suficientes para hacer frente a la amenaza de la explotación y el abuso sexual infantil en internet. Los niveles actuales de inversión no son proporcionales a la dimensión y el alcance del problema, ni son suficientes para abordar globalmente este peligro[379]
Normativa/legislación	**Los gobiernos** deben establecer leyes que tipifiquen como delito todas las agresiones relacionadas con la explotación y el abuso sexual infantil en internet basándose en los marcos internacionales aprobados, para así evitar la criminalización de los propios menores. **Los gobiernos** deben invertir en reforzar los sistemas de protección infantil para prevenir y responder a la explotación y el abuso sexual de menores en todos los contextos. **Los gobiernos** deben considerar opciones legislativas para reforzar la respuesta a la explotación y el abuso sexual infantil en internet. Las leyes deben establecer estándares para las denuncias del sector, la eliminación rápida de material de abuso sexual infantil y el uso legal y transparente de las herramientas de detección de material de esta naturaleza. Se debe buscar el consenso internacional a fin de mejorar la colaboración global para combatir esta amenaza.

Justicia penal	**Los gobiernos** deben invertir en mecanismos de disuasión y rehabilitación para ayudar a aquellos que están en peligro de perpetrar una agresión o ya la han perpetrado, para que cambien o controlen sus conductas. **Los gobiernos** deben financiar unidades especializadas en el cumplimiento de la ley para formar y mantener al día a expertos en este tipo de amenazas, y así mejorar los resultados de las investigaciones en su país. Los gobiernos también deben invertir en la definición de competencias policiales internacionales para fortalecer la colaboración en los delitos transfronterizos y tecnológicamente sofisticados. **Los gobiernos** y las fuerzas de seguridad deben consultar con sus homólogos internacionales para desarrollar respuestas consistentes dirigidas a investigar delitos transfronterizos y resolver los retos de investigación más comunes (por ejemplo, recopilar pruebas dispersas en múltiples jurisdicciones).
Servicios de apoyo a la víctima y empoderamiento	Para reducir el trauma de la victimización repetida, **los legisladores** deben trabajar junto con **la industria** para establecer normas que eliminen rápidamente el material de abuso sexual infantil de internet, reduzcan el riesgo de que las imágenes se vuelvan a compartir y diseñen formularios de denuncia adaptados para menores, independientes de los procesos de justicia penal. **Los gobiernos** deben invertir en servicios de asistencia a las víctimas y en la capacitación de los servicios de protección infantil para que el personal sepa cómo gestionar el trauma, cómo apoyar a las víctimas y adaptar ese apoyo para asistir a menores de grupos marginados. **Todas las partes involucradas** deben considerar una colaboración segura y adecuada con los supervivientes de abuso sexual infantil para que asesoren en el diseño y la evaluación de servicios, políticas y apoyo efectivos.
Tecnología	**Los proveedores de servicios de internet** deben adoptar un enfoque de «seguridad por diseño» que incluya la evaluación del impacto de todos los productos y servicios desde la perspectiva de los derechos del menor. Los proveedores de servicios de internet deben identificar y, según corresponda, advertir, expulsar y denunciar a los actores que representen un riesgo para los menores. **Los proveedores de servicios de internet** deben publicar informes de transparencia periódicamente, detallando las acciones que toman para reducir el peligro para los menores en internet y los mecanismos que utilizan para hacer un seguimiento de su efectividad. **Los desarrolladores de tecnologías de seguridad en internet** deben seguir trabajando para mejorar la precisión de las herramientas de estimación de la edad, los clasificadores para detectar contenido de abuso sexual infantil desconocido (incluido el contenido transmitido en directo) y las soluciones de detección de abuso sexual infantil en entornos cifrados. Se debe utilizar el código abierto (con los controles adecuados) para fomentar la colaboración entre las partes involucradas y ayudar a establecer una normativa consistente para las tecnologías de seguridad.
Social	**Los gobiernos** deben incorporar en los planes de estudio escolares la seguridad en internet, como complemento a programas más amplios que también abarquen, por ejemplo, conductas sexuales saludables y conductas sexuales nocivas. **Todas las partes implicadas en la respuesta**, incluyendo a los padres, los cuidadores y las organizaciones de la sociedad civil, deben educar a su comunidad sobre el peligro y los efectos del abuso sexual infantil, y también qué se puede hacer para prevenirlo.
Investigación y conocimiento	**Los gobiernos, las organizaciones de la sociedad civil y los proveedores de servicios de internet** deben invertir en investigación para: • Comprender mejor qué motiva una agresión y cuál es la eficacia de los programas de disuasión, autoayuda y tratamiento de agresores. • Comprender mejor los factores que provocan un aumento del material sexual «autogenerado» por menores y las características del desarrollo social y sexual de los adolescentes. • Comprender los factores de riesgo y de protección que pueden aumentar o reducir el peligro de que un menor se convierta en víctima, incluidos aquellos factores específicos de los grupos marginados. • Comprender mejor hasta qué punto la tecnología facilita la explotación y el abuso sexual de niños y niñas de todo el mundo. • Destacar cómo se manifiesta la amenaza en los países del Sur global (puesto que el escenario del problema está más documentado actualmente en el Norte global).

08

Agradecimientos

La Alianza Global de WeProtect quiere agradecer a las siguientes organizaciones e individuos su apoyo en el desarrollo de la Evaluación de la amenaza global de 2021:

COMITÉ DIRECTIVO

Signy Arnason
Canadian Centre for Child Protection

Rinchen Chopel
South Asia Initiative to End Violence Against Children

Sean Coughlan
Fundación Human Dignity

Toby Dagg
INHOPE/Oficina del Comisionado de Seguridad Electrónica

Deborah Denis y Donald Findlater
Fundación Lucy Faithfull

Edward Dixon
Rigr AI

Nicole Epps
Fundación World Childhood

Alexandra Evans
TikTok

Guillermo Galarza
Centro Internacional para Niños Desaparecidos y Explotados

Alexandra Gelber
Departamento de Justicia de Estados Unidos

Susie Hargreaves
Internet Watch Foundation

Afrooz Kaviani Johnson
UNICEF

Almudena Lara
Google

Daniela Ligiero
Together for Girls

Remy Malan
Roblox

David Miles
Facebook

Uri Sadeh
Interpol

Michael C. Seto
University of Ottawa Institute of Mental Health Research at the Royal

John Starr and **Melissa Stroebel**
Thorn

Nena Thundu
African Union

*Queremos agradecer especialmente a los miembros de la junta de la **Alianza Global de WeProtect,** y también a **Getty Images***

OTROS COLABORADORES

Apple
Arpan
Australian Centre to Counter Child Exploitation
Ministerio del Interior australiano
Policía federal de Australia
Camera Forensics
ChildSafeNet
Child Rescue Coalition
Crisp
DLT Risk Ltd.
Ethel Quayle
Europol
La Alianza Mundial para Erradicar la Violencia Contra los Niños
(Alianza Erradicar la Violencia)
Dr. Hany Farid
Hamogelo
International Justice Mission
LOCATE
Fundación Marie Collins
Microsoft
Centro Nacional para Niños Desaparecidos y Explotados (EE. UU.)
National Crime Agency (Reino Unido)
Netsweeper
Palantir
Policing Institute for the Eastern Region (UK)
Project VIC International
SafeToNet
SafeBAE
Scotiabank
Sentropy
Stuart Allardyce
Suojellaan Lapsia Ry
Terre des Hommes
The Technology Coalition
Ministerio del Interior del Reino Unido
Departamento de Cultura, Comunicación y Deporte del Reino Unido
Videntifier
Walk Free
YOTI
ZiuZ Forensic BV

El apoyo brindado en el desarrollo del informe, en cuanto miembro del Comité Directivo o Colaborador, no implica que se esté de acuerdo (total o parcialmente) con el contenido de este informe. La investigación y el desarrollo de este informe corre a cargo de Chloe Setter, Natalia Greene, Nick Newman y Jack Perry.

09

Glosario de términos

Término	Definición
Abuso sexual infantil	Implicar a un niño o una niña (cualquier persona menor de 18 años) en actividades sexuales que él o ella no comprende del todo, para las que no está preparado/a a nivel de desarrollo y para las que no puede dar su consentimiento informado.[380] Esta es la definición de abuso sexual infantil adoptada por la Alianza Global de WeProtect («la Alianza»), y se basa en las directrices de la Organización Mundial de la Salud (OMS).
Explotación sexual infantil	Una forma de abuso sexual infantil que implica cualquier abuso o intento de abuso a una persona que se encuentra en una posición de vulnerabilidad, desequilibrio de poder o confianza. Esto incluye, aunque no se limita a, aprovecharse económica, social o políticamente de la explotación sexual de otra persona,[381] lo cual puede cometerse de manera individual o en grupo. Lo que distingue la explotación sexual infantil del abuso sexual infantil es la noción subyacente de intercambio que está presente en la explotación.[382] Ambos conceptos se solapan de manera significativa, porque la explotación es a menudo una característica del abuso y viceversa.[383]
La explotación y el abuso sexual infantil en internet	La explotación y el abuso sexual infantil que la tecnología, es decir, internet u otras comunicaciones inalámbricas, facilita parcial o totalmente. Este concepto también se conoce como OCSEA (por sus siglas en inglés) y como explotación y abuso sexual infantil «facilitado por la tecnología».
Material de abuso sexual infantil (CSAM)	Cualquier contenido visual o de audio de naturaleza sexual que involucre a una persona menor de 18 años,[384] ya sea real o no. **Nota sobre terminología alternativa:** algunas organizaciones distinguen entre material de abuso sexual infantil y material de explotación sexual infantil (por ejemplo, el Grupo de Trabajo Interagencial sobre la Explotación Sexual de Niños define «material de explotación sexual infantil» como una categoría más amplia que abarca «material que representa abuso sexual infantil y otro contenido sexualizado que representa a menores»). Algunas organizaciones también utilizan el término alternativo «pornografía infantil». La posición declarada de la Alianza es abstenerse del uso de este término, ya que se considera que «material de abuso sexual infantil» recoge con mayor precisión la naturaleza atroz de la violencia sexual contra los menores y protege la dignidad de las víctimas. Hay determinado material sexual «autogenerado» que también constituiría material de abuso sexual infantil, dependiendo de las circunstancias de su producción (ver Material sexual infantil «autogenerado»).

Término	Definición
Material de abuso sexual infantil conocido	Aquel material de abuso sexual infantil que ya ha sido previamente detectado y clasificado por las fuerzas de seguridad o los moderadores.
Material de abuso sexual infantil de «primera generación»	Aquel material de abuso sexual infantil que no ha sido previamente detectado y clasificado por las fuerzas de seguridad o los moderadores.
Material de abuso sexual infantil no fotográfico	Esto incluye dibujos animados con imágenes generadas por ordenador o ilustraciones que representan gráficamente a menores en una situación de abuso sexual.[385] [386]
Material sexualizado de menores	Material que no representa un abuso sexual de un menor, pero que se utiliza con fines sexuales. Un ejemplo podría ser un vídeo de menores haciendo gimnasia que se consuma de forma inapropiada para una gratificación sexual. La sexualización no siempre es un criterio objetivo y el elemento crucial para juzgar estas situaciones es la intención de la persona de sexualizar a un menor en una imagen o de hacer uso de una imagen con fines sexuales.
Producción de material de abuso sexual infantil	La creación de material de abuso sexual infantil mediante imágenes, vídeo o grabación de audio en persona, la creación de contenido textual o material visual no fotográfico (por ejemplo, generado por ordenador), o la manipulación de material de abuso sexual infantil ya existente para crear nuevas imágenes.
Buscar y/o consumir material de abuso sexual infantil	Buscar material de abuso sexual infantil en internet y verlo o intentar verlo.
Compartir y/o almacenar material de abuso sexual infantil	Descargar, almacenar, alojar, subir y compartir material de abuso sexual infantil.

Término	Definición
Captación de menores en internet con el propósito de explotación y abuso sexual	Un individuo establece una relación, se gana la confianza y conecta emocionalmente con un menor o un joven con el fin de manipularlo, explotarlo y abusar de él o ella (sirviéndose, parcial o totalmente, de internet u otras redes inalámbricas).[388] No siempre existe la intención de conocerse en persona. Nota sobre terminología alternativa: algunas organizaciones utilizan el término «incitación en línea» (como define el NCMEC[389]) cuando se refieren a este concepto.
Material sexual infantil «autogenerado»	Contenido de naturaleza sexual, incluyendo imágenes y vídeos de desnudos totales o parciales, que los propios menores han producido. El material sexual infantil «autogenerado» no es un daño por sí mismo (puede producirse de manera voluntaria y compartirse como parte de un intercambio apropiado para el desarrollo personal, por ejemplo, si se da entre adolescentes), pero hay situaciones en las que sí causa un perjuicio, principalmente: • Cuando se coacciona a un menor o adolescente para que produzca material sexual «autogenerado» • Cuando el material sexual «autogenerado» de manera voluntaria se comparte en contra de los deseos del adolescente Este informe se centra en analizar las características y los límites de la «autoproducción» perjudicial. Esta expresión aparecerá entrecomillada durante todo el informe para evitar dar a entender que existía una predisposición voluntaria del menor o joven implicado. Aunque el contenido pueda coincidir con la definición de material de abuso sexual infantil, es muy probable que la intención no sea clara por lo que no se puede dar por sentado en ninguna circunstancia.
Transmitir en directo explotación y abuso sexual infantil (streaming en directo)	Transmitir abusos y explotación sexual infantil en tiempo real a través de internet
Imágenes generadas por ordenador (CGI)	En el contexto de abuso y explotación sexual infantil, se refiere a imágenes sexualizadas de menores total o parcialmente creadas de forma artificial o digital.[390]
«Deepfake»	Una forma de CGI que usa inteligencia artificial para reemplazar la imagen de una persona por otra en fotos o vídeos grabados.[391]
«Capping»	Los agresores graban imágenes de abuso y explotación sexual de menores y las transmiten en directo.[392] El «capping» también puede referirse a los agresores que capturan imágenes inofensivas de menores pero las utilizan con fines sexuales (estas imágenes constituirían imágenes sexualizadas de menores).
«Gamificación» del abuso	La aplicación de elementos lúdicos (por ejemplo, puntuación, competición, reglas de juego) para fomentar la participación en el abuso y la explotación.

Término	Definición
Menor que muestra un comportamiento sexual dañino	Una persona menor de 18 años que exhibe comportamientos que no son apropiados para su desarrollo, conductas que pueden ser perjudiciales para sí misma, para otras personas y/o abusivas para otros menores jóvenes o adultos.[393]
Factores de riesgo	Factores a nivel individual, relacional, comunitario y social que pueden hacer que un menor sea más propenso a sufrir abusos y explotación sexual.
Factores de protección	Factores a nivel individual, relacional, comunitario y social que pueden reducir el riesgo de que un menor sea víctima de abusos y explotación sexual.
Revictimización	Cuando una víctima debe enfrentarse a un nuevo abuso o agresión sexual después de haber sufrido un abuso o agresión anterior.[394] Esto incluye la redistribución y visualización de sus imágenes por internet: una sola imagen de una víctima se puede compartir cientos o miles de veces.[395] La revictimización puede se causada por el mismo agresor de la victimización inicial o por uno diferente.
Tráfico de menores	El reclutamiento, transporte, traslado, acogida o recepción de un menor con fines de explotación.[396]
Norte global	Los países del G8, Estados Unidos, Canadá, todos los estados miembros de la Unión Europea, Israel, Japón, Singapur, Corea del Sur, Australia, Nueva Zelanda y cuatro de los cinco miembros permanentes del Consejo de Seguridad de las Naciones Unidas, excluida China.[397]
Sur global	África, América Latina, Oriente Medio y la parte de Asia en vías de desarrollo. Esto incluye tres de las cuatro economías avanzadas de los países BRIC (excluida Rusia): Brasil, India y China.[398]
Internet superficial	La parte de la web que está disponible para el público en general y a la que se puede acceder con los motores de búsqueda estándar.[399]
Internet profunda	La parte de la web cuyo contenido no está indexado por los motores de búsqueda web estándar pero incluye muchos de los usos comunes de internet, como el correo electrónico, banca en línea y los servicios de suscripción. El contenido se puede ubicar y acceder a él a través de un enlace directo o dirección IP y puede requerir una contraseña u otro acceso de seguridad además de la dirección web pública.[400]
Dark Web (web oscura)	La capa de información y páginas a las que solo se puede acceder a través de las llamadas «redes superpuestas» (como las redes privadas virtuales o VPN y las redes de intercambio de archivos de entre pares o P2P), que dificultan el acceso público. Los usuarios necesitan un software especial para acceder a la Dark Web porque está encriptada en gran medida y la mayoría de sus páginas están alojadas de forma anónima.[401]

Término	Definición
Tecnologías de seguridad (Safety Tech)	Soluciones para facilitar experiencias online más seguras y proteger a los usuarios de contenidos, contactos o conductas perjudiciales.[402]
Seguridad por diseño	La integración de los derechos y la seguridad de los usuarios en el diseño y la funcionalidad de los productos y servicios de internet desde su concepción.[403]
Red de pares (P2P)	En una red P2P, los «pares» son sistemas informáticos que están conectados entre sí a través de internet. Los archivos se pueden compartir directamente entre sistemas de la red sin la necesidad de un servidor central. En otras palabras, cada ordenador de una red P2P se convierte en un servidor de archivos y también en un cliente.[404]
Red privada virtual (VPN)	Una solución que, a través de internet, establece una conexión encriptada desde un dispositivo a una red, conocida como túnel.[405]
Hashing	Un proceso mediante el cual se crea un «hash» binario mediante un algoritmo matemático que transforma datos de cualquier tamaño en datos de longitud fija mucho más cortos. La secuencia corta pasa a representar los datos originales y se convierte en la firma única de este archivo, o su «valor hash», que a menudo se conoce como huella digital.[406]
«Hash-matching»	Un proceso que usa las bases de datos de material «hash» de abuso sexual infantil para detectar cuándo se vuelve a compartir dicho material, comparando su «valor hash» con el de archivos ya conocidos.[407]
Clasificación por inteligencia artificial (IA) o moderación de IA	Sistemas de moderación automatizados o parcialmente automatizados que identifican contenido dañino siguiendo ciertas normas para interpretar muchos ejemplos diferentes de lo que es y no es contenido dañino.[408]
Encriptación o cifrado	El proceso de codificación de información en una forma alternativa que solo pueden descifrar personas autorizadas que posean la clave de decodificación.[409]
Cifrado de extremo a extremo	Es una forma de encriptación en la que el contenido de los mensajes solo es visible para el emisor y el receptor. Descodificar el mensaje requiere de una clave de descifrado privada que se intercambia entre las partes, de manera que si se intercepta el mensaje, ni el proveedor del servicio, ni las fuerzas de seguridad ni ninguna otra parte pueden verlo ni controlarlo.[410]
«Servicios ocultos»	Páginas web alojadas dentro de una red proxy (como Tor), por lo que no se puede rastrear su ubicación.[411]
Metadatos	Datos que describen otros datos.[412] La hora y la duración de una llamada telefónica (a diferencia del contenido de la comunicación en sí) son ejemplos de metadatos.
Tor	Una red privada de código abierto que permite a los usuarios navegar por la web de forma anónima. El sistema utiliza una serie de nodos por capas para ocultar la dirección web, los datos de internet y el historial de navegación.[413]

Término	Definición
Herramientas seguras	Software o aplicaciones utilizadas para propiciar el anonimato en internet, dado que ocultan la ubicación y la identidad del usuario.
Sistemas operativos seguros	El uso de sistemas operativos que se pueden arrancar desde un USB. Debido a que no se guardan en el disco duro, una vez que se apagan, todo se elimina. El software de cifrado se puede utilizar para proteger el contenido de un archivo y partes de la unidad a las que solo se puede acceder con la clave de decodificación del usuario.
Tradecraft	Una serie de técnicas de encubrimiento y estrategias de evasión en constante evolución que los agresores utilizan para evitar ser detectados, así como sus técnicas y estrategias para identificar e involucrar a los menores.
Virtualización y emulación	Las máquinas virtuales permiten ejecutar un sistema operativo que se comporta como un ordenador completo e independiente en una ventana del escritorio. Algunos emuladores pueden crear una interfaz de smartphone virtual en un ordenador, lo que permite al usuario instalar y usar aplicaciones en su ordenador que de otro modo no estarían disponibles. Los emuladores se utilizan a menudo junto con herramientas de «capping», ya que pueden evitar que se envíe una notificación de «captura de pantalla» a la víctima y el agresor puede utilizar el software de «capping» instalado en su ordenador para capturar imágenes más nítidas.
Convención de las Naciones Unidas sobre los Derechos del Niño	Un tratado internacional de derechos humanos que consta de 54 artículos que abarcan todos los aspectos de la vida de un menor y establecen los derechos civiles, políticos, económicos, sociales y culturales a los que los menores de todo el mundo tienen derecho. También explica cómo los adultos y los gobiernos deben trabajar juntos para asegurarse de que todos los menores puedan disfrutar de sus derechos.[414] [415]
Observación general 25 del Comité de los Derechos del Niño de las Naciones Unidas	Una guía autoritativa que establece cómo se aplican los derechos de los menores en el entorno digital. Ayuda a los países a comprender qué pasos son necesarios para respetar, proteger y cumplir los derechos del niño en el entorno digital.[416]
Principios voluntarios para combatir la explotación y el abuso sexual de menores	Conjunto de principios que tienen como objetivo proporcionar un marco para combatir la explotación y el abuso sexual infantil en internet y fomentar la acción colectiva. Fueron desarrollados por gobiernos de cinco países (Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos), asesorados por un amplio grupo de partes interesadas, incluido un grupo líder de representantes de la industria.[417]
Modelo de Respuesta Nacional de la Alianza Global de WeProtect (MNR)	Un marco que proporciona orientación y apoyo sobre el MNR a los países y organizaciones para ayudarlos a cumplirlo. Este modelo se centra en asesorar a los países para que desarrollen su respuesta a la explotación sexual infantil en internet.[418]
Respuesta Estratégica Global de la Alianza Global de WeProtect (GSR)	Un marco que proporciona orientación y apoyo sobre la GSR a los países y organizaciones para ayudarlos a cumplirlo. Esta respuesta se centra en mejorar la colaboración global en materia de explotación sexual infantil en internet.
Convenio del Consejo de Europa sobre la protección de los menores contra la explotación y el abuso sexual (también conocido como el «Convenio de Lanzarote»)	Un convenio que exige la tipificación como delito de todo tipo de agresiones sexuales contra menores. Establece que los países de Europa y de fuera de Europa adoptarán una legislación específica y tomarán medidas para prevenir la violencia sexual, proteger a los menores y condenar a los agresores. El «Comité de Lanzarote» es el organismo designado para controlar que las partes implementen adecuadamente el Convenio de Lanzarote e identifican las buenas prácticas.[419]
Directiva europea de privacidad electrónica	Legislación relativa al procesamiento de datos personales y a la protección de la privacidad en el sector de las comunicaciones electrónicas.[420] La Directiva no contiene una base legal explícita para que se continúe con las prácticas voluntarias actuales para detectar, denunciar y eliminar el abuso sexual infantil.[421]

10

Anexo A:

Resultados de la encuesta de Alianza Global de WeProtect y Technology Coalition de empresas tecnológicas

RESUMEN DE LOS RESULTADOS

Muchas de las empresas a las que se encuestó tienen capacidad para detectar el abuso y la explotación sexual infantil en internet, así como mecanismos de denuncia, pero existen oportunidades para mejorar la colaboración y centrarse más en la disuasión y la prevención.

	Reportando	Detección	Disuasión y prevención	Desarrollo de herramientas	Transparencia reportando
Resultados clave	La mayoría de los informes son al menos parcialmente automatizado, y casi todas las empresas tener alguna forma de mecanismo de presentación de informes	La mayoría de las empresas están usando herramientas basadas en hash para detectar tanto la imagen como video abuso sexual infantil materia. Uso de clasificadores avanzados para detectar video y contenido de transmisión en vivo, es menos común a pesar de	Medidas de prevención como la disuasión mensajería y niño los recursos de seguridad son ampliamente proporcionado, pero estos son menos comunes que el uso de hash-based detección, a pesar de su potencial para prevenir abuso antes de que ocurra	Muchas empresas utilizan herramientas desarrolladas por otros, pero es menos común para ellos desarrollar herramientas internamente y compártelos	La mayoría de las empresas no aún publicar transparencia informes. Sin embargo, de empresas que lo hacen, gran mayoría publica datos específicos sobre el niño abuso sexual y explotación
Recomendaciones	Diversificar la presentación de informes caminos para ganar más imagen holística de la amenaza	Comparta información y inteligencia (por ejemplo, hashes y palabras clave) para ayudar mantente por delante de lo que es un espacio en rápida evolución	Invertir en disuasión y medidas de prevención, y diversificar el focalización de la seguridad en línea recursos para evitar sobre-realianza en uno grupo, para ayudar a prevenir abuso antes de que ocurra	olabora y comparte herramientas en la industria para ayudar a maximizar su beneficio. Garantizar marcos regulatorios empoderar en lugar de obstaculizar las empresas utilizando herramientas clave	Desarrollar universal reportar marcos a asegurarse de que los datos sean consistente y animar más empresas para hacerlo disponible públicamente

METODOLOGÍA

Entre febrero y marzo de 2021, la Alianza Global de WeProtect y la Technology Coalition hicieron una encuesta de 20 preguntas a los miembros de sus respectivas industrias para entender hasta qué punto las empresas tecnológicas se habían implicado en iniciativas para combatir la problemática del abuso sexual infantil en internet. En total, respondieron 32 empresas cuyo tamaño oscila entre menos de 250 empleados y más de 5000.

LIMITACIONES

La muestra es pequeña en comparación con el tamaño del sector tecnológico mundial y es más representativa de las empresas con sede en el Norte global. Sin embargo, se podría decir que la gran variedad de tamaños y tipos de empresa que han participado proporciona una muestra representativa de la industria. Debido a que la encuesta es completamente anonimizada y se muestran los resultados en conjunto, no ha sido posible analizar las respuestas de un encuestado a varias preguntas distintas. Esto limita las posibles de comparación entre las respuestas, por ejemplo, para diferentes tamaños de empresa. Por último, algunas de las preguntas pueden no haber sido relevantes para algunos encuestados, pero esto se intentó mitigar al incluir la opción «no relevante» y al permitir que se saltaran preguntas.

RESULTADOS TOTALES

Denuncias:

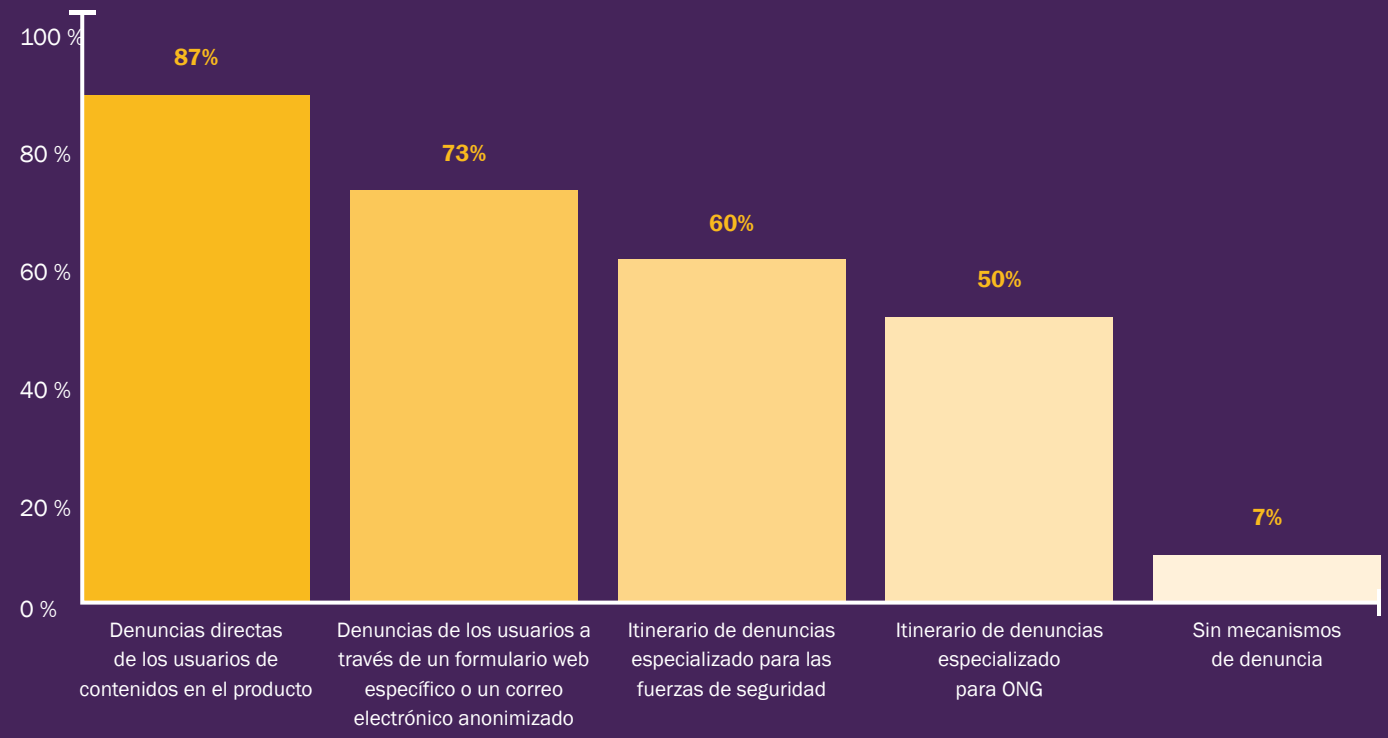
El 84 % de las empresas encuestadas cuenta con procesos al menos parcialmente automatizados para denunciar el abuso sexual infantil en internet, lo que sugiere que la gestión de denuncias es relativamente eficiente.

GESTIÓN DE DENUNCIAS
84%
PARCIAL O TOTALMENTE AUTOMATIZADA

Esta pregunta no se centraba en los mecanismos concretos de detección proactiva que puedan tener las empresas, por lo que no proporciona una imagen completa al respecto. Sin embargo, se sabe que el mecanismo de denuncias más popular para las empresas son las denuncias directas de los usuarios, y que el menos popular es el que se deriva a ONG y fuerzas de seguridad, lo que sugiere que puede haber margen para una mayor colaboración intersectorial. La diversificación de las vías de presentación de denuncias también evitará una dependencia excesiva de las denuncias de los usuarios, lo que, dado que las tasas de denuncias de casos propios son bajas, puede ayudar a proporcionar una imagen más completa de las agresiones.

Figura 19: Mecanismos que facilitan las empresas para poder denunciar.

¿Qué mecanismos ofrecen las empresas para facilitar la denuncia de material de abuso sexual infantil?

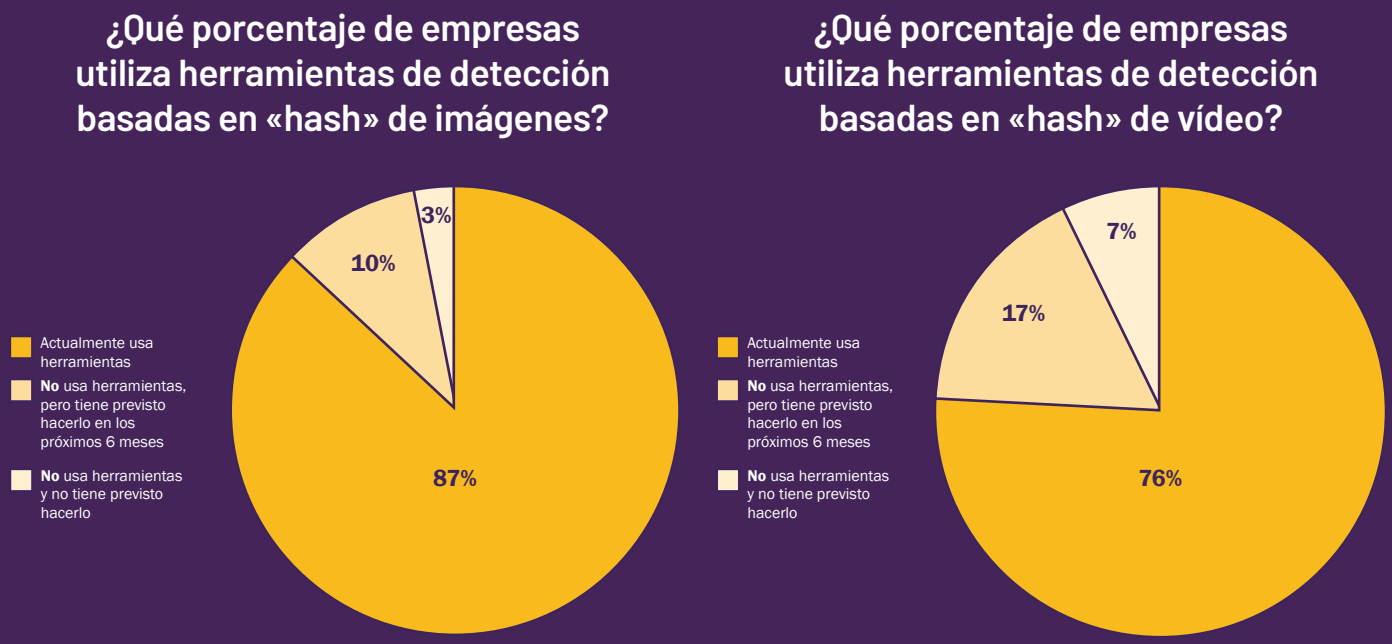


DETECCIÓN

Detección basada en «hash»

La mayoría de los encuestados utiliza herramientas basadas en «hash» para detectar material de abuso sexual infantil en las imágenes y vídeos de sus plataformas. La mayoría de los que aún no utilizan herramientas basadas en «hash» planean implementarlas en los próximos seis meses, como se muestra en la Figura 20 a continuación.

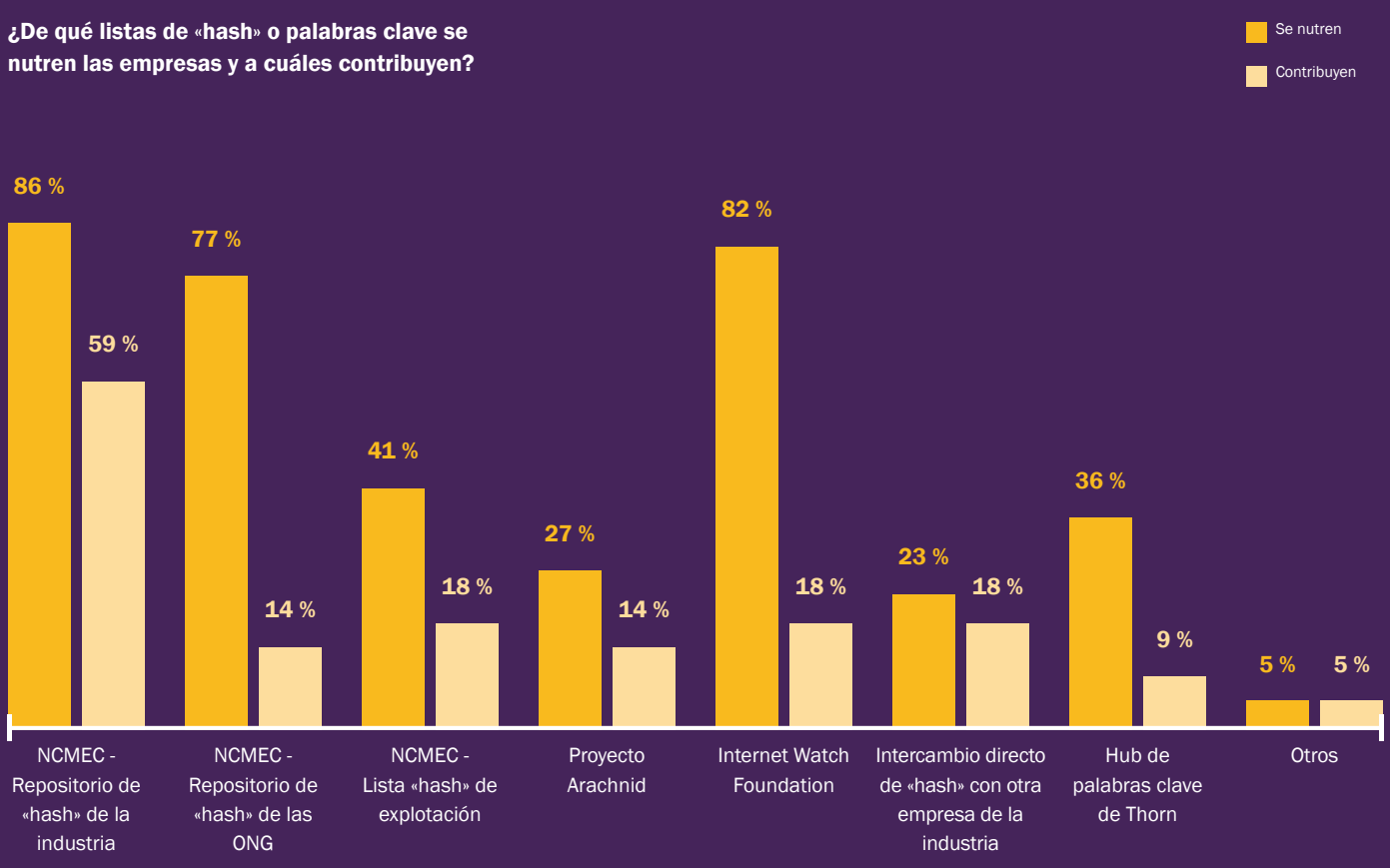
Figura 20: Uso de herramientas de detección basadas en «hash» de las empresas.



Para utilizar de forma eficaz las herramientas de detección basadas en «hash», las empresas necesitan acceder a «hashes» de material conocido de abuso sexual infantil. Otro elemento importante para la detección es la capacidad de bloquear términos de búsqueda relacionados con el abuso sexual infantil, para lo cual las empresas necesitan acceder a listas de palabras clave.

La mayoría de las empresas utilizan «hash» y palabras clave de al menos un repositorio, como se muestra en la Figura 21 a continuación. Sin embargo, muchas menos aportan sus propias «hash» o palabras clave. Suponiendo que las empresas no detecten simplemente contenido conocido, el intercambio limitado de inteligencia externa puede afectar a la capacidad de afrontar esta amenaza en constante evolución.

Figura 21: Uso de listas de «hash» o palabras clave por parte de la empresa.

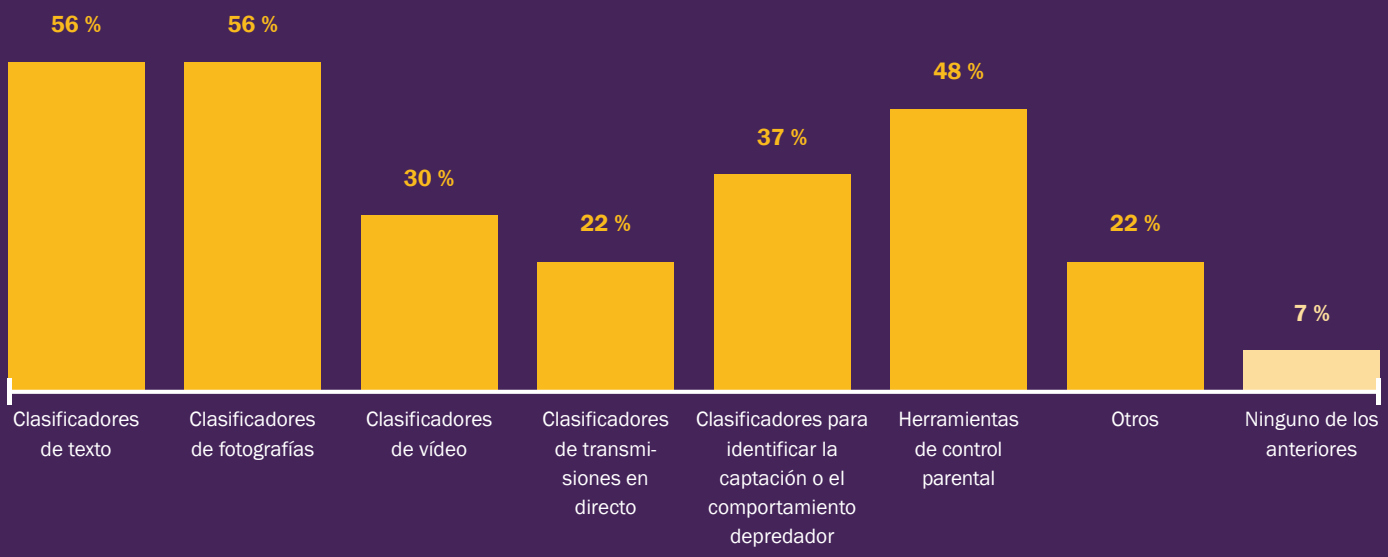


DETECCIÓN AVANZADA:

La detección avanzada se refiere a tecnologías como los clasificadores de inteligencia artificial. Estas medidas de detección avanzada se utilizan con menos frecuencia que las medidas de detección basadas en «hash». A pesar de los indicios de la creciente prevalencia del contenido en vídeo y la transmisión en directo, solo utilizan clasificadores para detectar dicho material el 30 % y el 22 % de los encuestados, respectivamente.

Figura 22: Medidas adicionales para combatir la explotación y el abuso sexual infantil en internet.

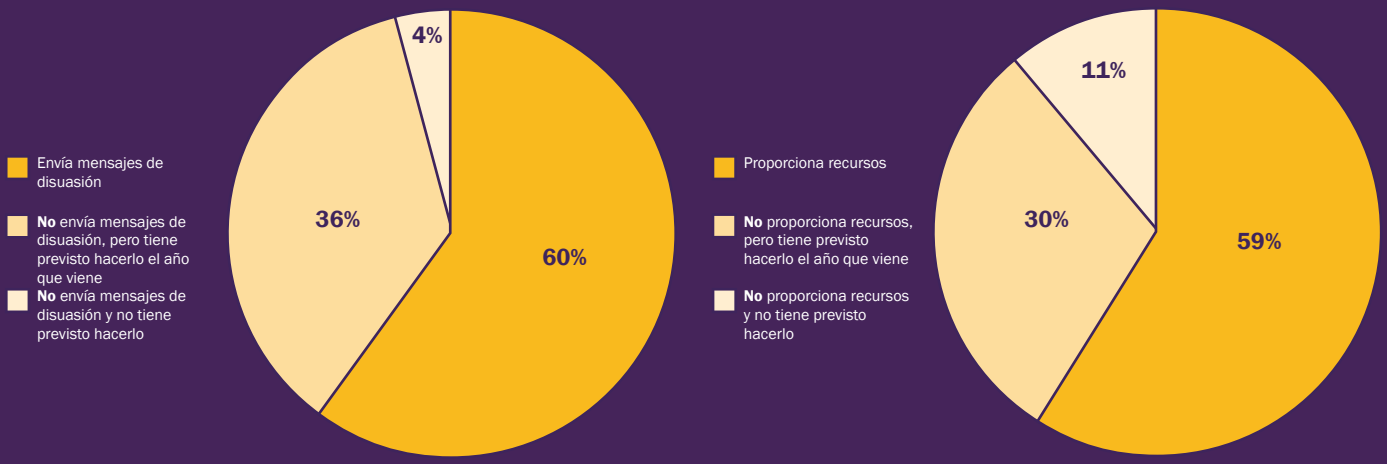
¿Qué medidas adicionales utilizan las empresas para combatir la explotación y el abuso sexual infantil en internet?



DISUASIÓN Y PREVENCIÓN:

La mayoría de los encuestados envían mensajes de disuasión a los posibles agresores y brindan recursos de ciberseguridad para menores para ayudar a prevenir el abuso antes de que ocurra, pero estas prácticas son menos comunes que los mecanismos para detectar material de abuso sexual infantil.

Figura 23: Uso por parte de la empresa de mensajes de disuasión y recursos de ciberseguridad para menores.



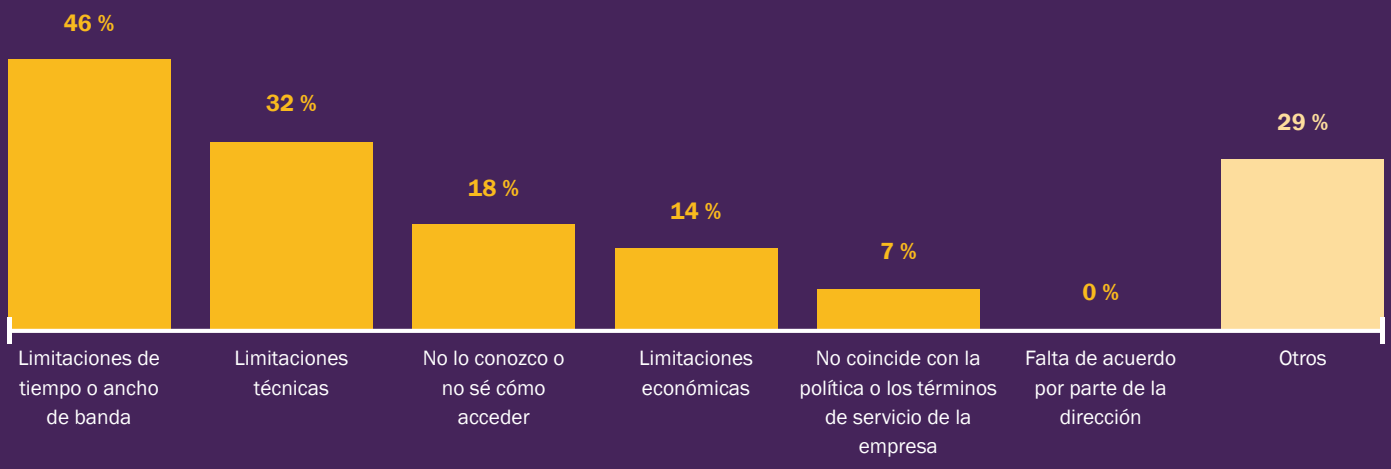
La encuesta reveló que la mayoría de los recursos de ciberseguridad para menores están dirigidos a los padres, lo cual es positivo dado que generalmente son el primer punto de contacto para un menor que corre un peligro en línea.[422] Sin embargo, también hay pruebas que sugieren que a menudo los perpetradores de la explotación y el abuso sexuales son miembros de la familia.[423] Para apoyar a estas víctimas y evitar la dependencia excesiva de un único grupo de protección, existe la posibilidad de proporcionar más recursos a los propios menores, a sus educadores y a la comunidad en general.

DESARROLLO DE HERRAMIENTAS:

Casi el 50 % de los encuestados utiliza clasificadores de contenido desarrollados por otras empresas, pero solo el 26 % hace accesibles a los demás las herramientas que ellos mismos desarrollan. Comprender el motivo requeriría más análisis, pero una mayor colaboración e intercambio de herramientas en la medida de lo posible podría ayudar a maximizar los beneficios de dichas herramientas.

Figura 24: Inconvenientes para el uso de herramientas contra el abuso sexual infantil en internet.

¿A qué obstáculos se enfrentan las empresas a la hora de utilizar recursos técnicos para luchar contra la explotación y el abuso sexual infantil en internet?



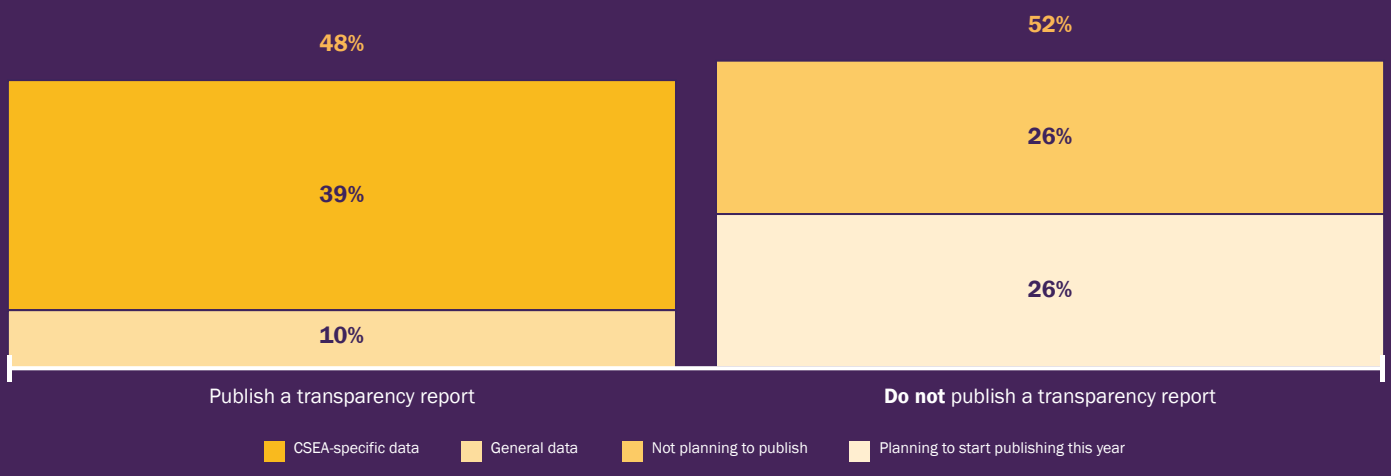
Las limitaciones de tiempo y el ancho de banda son los principales inconvenientes con que se encuentran las empresas que desarrollan e implementan herramientas para luchar contra el abuso sexual infantil en internet. Ninguno de los encuestados mencionó que faltara aceptación por parte de los directivos.

TRANSPARENCIA:

La transparencia es fundamental para afrontar de manera conjunta y bien fundamentada la explotación y el abuso sexual infantil en línea. Sin embargo, solo el 49 % de los encuestados publica regularmente un informe de transparencia. De estos, el 80 % publica datos específicos sobre la explotación y el abuso sexual infantil, lo cual es fundamental para comprender la dimensión y el alcance de esta amenaza.

Figura 25: Informes de transparencia de las empresas.

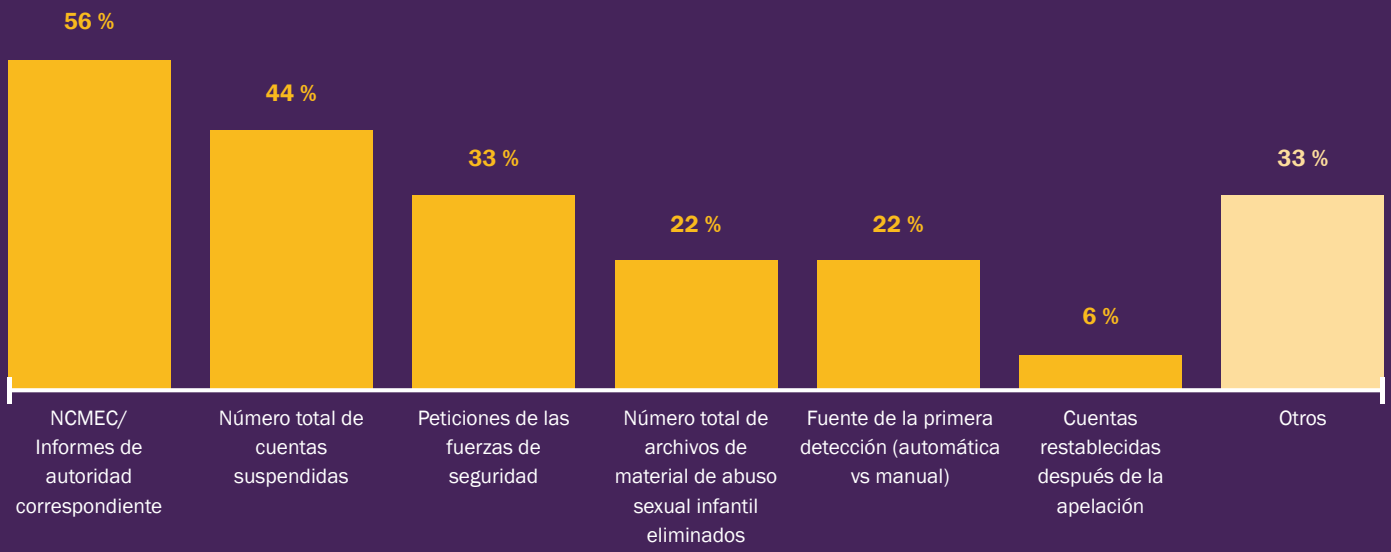
What proportion of companies publish regular transparency reports on child sexual exploitation and abuse on their platform?



Los datos presentados por las empresas pueden ser muy variados, tal y como se muestra en la Figura 26. Se necesita trabajar más para desarrollar modelos de informes universales. Esto garantizaría que los datos fueran consistentes y comparables y alentaría a las empresas que aún no publican sus datos a ponerlos a disposición del público.

Figura 26: Tipos de datos incluidos en los informes de transparencia.

Las empresas que publican un informe de transparencia, ¿qué tipo de datos relacionados con la explotación y el abuso sexual infantil en internet incluyen?



La Figura 26 muestra que es común que las empresas presenten sus datos en conjunto, como el total de archivos de material de abuso sexual infantil eliminados. Los datos de los informes de transparencia rara vez se desglosan para mostrar la prevalencia de diferentes tipos de abuso sexual infantil, como la captación o la transmisión en directo. Informar sobre estos datos arrojaría más luz sobre cuáles son los daños que más abundan, con miras a concentrar intervenciones específicas allí donde más se necesite.

La Alianza Global de WeProtect reúne a expertos del gobierno, el sector privado y la sociedad civil.

Analizamos problemas complejos y desarrollamos medidas y soluciones para proteger a los menores del abuso sexual en internet.

WeProtect
GLOBAL ALLIANCE

11

References

1 Annual Report 2020 (INHOPE, 2021) Accessed from: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf 06/05/2021

2 4 arrested in takedown of dark web child abuse platform with some half a million users (Europol, 2021) Accessed from: https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users 04/05/2021

3 NetClean Report COVID-19 Impact 2020 (NetClean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/# 04/05/2021

4 Fighting Child Exploitation with Big Data (Freethink, 2020) Accessed from: https://www.freethink.com/videos/child-exploitation 16/06/2021

5 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

6 Online child sexual abuse activity has increased (NetClean, 2021) Accessed from: https://www.netclean.com/netclean-report-2020/insight-2/ 26/01/2021

7 Online enticement reports skyrocket in 2020 (NCMEC, 2021) Accessed from: https://www.missingkids.org/blog/2021/online-enticement-reports-skyrocket-in-2020 24/02/2021

8 IWF Annual Report: 2020 Trends and Data (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends 22/04/2021

9 Research report: The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing (University of New South Wales, Sydney, 2021) Accessed from: https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and wong.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=New+briefings+and+reports+-from+the+Alliance+and+our+members&utm_campaign=-May+2021+newsletter 07/06/2021

10 COVID-19: Child sexual exploitation and abuse threats and trends (Interpol, 2020) Accessed from: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse 26/01/2021

11 By the Numbers (NCMEC, 2021) Accessed from: https://www.missingkids.org/gethelpnow/cybertipline 16/06/2021

12 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

13 Acion to end Child Sexual Abuse and Exploitation (UNICEF, 2020) Accessed from: https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 23/07/2021

14 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies

15 IWF Annual Report: Hidden Services (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/Trends/International/Other/Hidden 22/04

16 PA Consulting engagement with Australian Centre to Counter Child Exploitation, 01/03/2021

17 Violencia sexual a menores ya deja mas de mil victimas en lo corrido de 2021 (LAFM, 2021) Accessed from: https://www.lafm.com.co/colombia/violencia-sexual-menores-ya-deja-mas-de-mil-victimas-en-lo-corrido-de-2021 11/03/2021

18 Abuso sexual en internet y redes de trata (Infobae, 2020) Accessed from: https://www.infobae.com/america/mexico/2020/07/27/abuso-sexual-en-internet-y-redes-de-trata-los-crimenes-contra-la-ninez-que-aumentaron-durante-la-pandemia/ 25/02/2021

19 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021

20 Los casos de abuso sexual contra menores en espana se multiplican por 4 en la ultima decada (Levante, 2021) Accessed from: https://protect-eu.mimecast.com/s/WuEPCWnWgFxLBY3Hxchqm?domain=levante-emv.com 23/02/2021

21 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

22 A Global Strategic Response to Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/WeProtectGA-Global-Strategic-Response-EN.pdf 17/06/2021

23 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 13/05/2021

24 Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse (World Health Organisation, 2003) Accessed from: https://www.who.int/violence_injury_prevention/publications/violence/med_leg_guidelines/en/ 19/04/2021

25 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

26 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf (23/07/2021)

27 Global Threat Assessment 2019 (WeProtect Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 26/01/2021

28 Grooming (NSPCC) Accessed from: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/ 25/05/2021

29 Online Enticement (NCMEC) Accessed from: https://www.missingkids.org/netsmartz/topics/onlineenticement 25/05/2021

30 Netclean Annual Report; Comment to insight 4 – Simon Bailey (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-6/ 17/06/2021

31 Netclean Annual Report; Insight 2: Online Child Sexual Abuse Activity has increased (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-2/ 07/06/2021

32 Netclean Annual Report; Comment to insight 4 – Rob Jones (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-6/ 17/06/2021

33 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 07/06/2021

34 Protection of children should always trump protection of privacy (eSafety Commissioner, 2020) Accessed from: https://www.esafety.gov.au/about-us/blog/protecting-children-should-always-trump-protecting-privacy 07/06/2021

35 Abuso sexual infantil crece en un 50% durante la pandemia por coronavirus (El Imparcial, 2021) Accessed from: https://www.elimparcial.com/mundo/Abuso-sexual-infantil-crece-en-un-50-durante-la-pandemia-por-coronavirus-20210216-0011.html 07/06/2021

36 Online sexual abuse of children rising amid COVID 19 pandemic – Save the Children Philippines (Relief Web, 2021) Accessed from: https://reliefweb.int/report/philippines/online-sexual-abuse-children-rising-amid-covid-19-pandemic-save-children 22/04/2021

37 La pornografia infantile crecio 117% en Mexico (Jornada, 2020) Accessed from: https://www.jornada.com.mx/2020/08/10/politica/010n1pol 07/06/2021

38 Ending Violence Against Children and COVID-19 (Child Rights Now!, 2020) Accessed from: https://www.wvi.org/sites/default/files/2020-07/2020_06_JF_CRN_Ending%20Violence%20Against%20Children%20and%20COVID%2019%20ENG.pdf 07/06/2021

39 COVID-19 Conversations: The Crisis of Online Child Sexual Exploitation (Equality Now, 2020) Accessed from: https://www.equalitynow.org/covid_19_online_exploitation 07/06/2021

40 Keeping Children Safe in Uganda's COVID-19 Response (Save the Children, 2020) Accessed from: https://resourcecentre.savethechildren.net/node/17615/pdf/Joining%20Forces%20-%20Protecting%20children%20during%20Covid-19%20in%20Uganda.pdf 08/06/2021

41 La violencia contra los niños aumenta con la covid (Inter Press Service, 2021) Accessed from: https://ipsnoticias.net/2021/04/la-violencia-los-ninos-aumenta-la-covid/ 11/06/2021

42 Child Sexual Exploitation Materials Hotline Annual Report 2020 (EOKM, 2021) Accessed from: https://www.eokm.nl/wp-content/uploads/2021/04/EOKM-Jaarveslag-2020-DEF-ENG.pdf 17/06/2021

43 National Strategic Assessment of Serious and Organised Crime (National Crime Agency, 2021) Received by email from the NCA, 25/05/2021

44 Pedophilia and Sexual Offending Against Children: Theory, Assessment, and Intervention, Second Edition (Michael Seto, 2018)

45 Research report: The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing (University of New South Wales, Sydney, 2021) Accessed from: https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=New+briefings+and+reports+-from+the+Alliance+and+our+members&utm_campaign=-May+2021+newsletter 07/06/2021

46 IWF Annual Report 2020: Hidden Services (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other/hidden 07/06/2021

47 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment 20/04/2021

48 Why Children are at risk of sexual exploitation during COVID-19 (ECPAT International, 2020) Accessed from: https://ecpat.exposure.co/covid19?embed=true 07/06/2021

49 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment 20/04/2021

50 Netclean Annual Report 2020; Insight 4: Moderate increase in actual investigations and cases (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-4/ 06/05/2021

51 COVID-19 to add as many as 150 million extreme poor by 2021 (World Bank, 2020) Accessed from: https://www.worldbank.org/en/news/press-release/2020/10/07/covid-19-to-add-as-many-as-150-million-extreme-poor-by-2021 06/07/2021

52 Joint Leaders' statement – Violence against children: A hidden crisis of the COVID-19 pandemic (World Health Organisation, 2020) Accessed from: https://www.who.int/news/item/08-04-2020-joint-leader-s-statement---violence-against-children-a-hidden-crisis-of-the-covid-19-pandemic 07/06/2021

53 Children's screen time has soared in the pandemic, alarming parents and researchers (NY Times, 2021) Accessed from: https://www.nytimes.com/2021/01/16/health/covid-kids-tech-use.html 16/07/2021

54 Children at increased online risk during COVID-19 pandemic (UNICEF, 2020) Accessed from: https://www.unicef.org/bhutan/press-releases/children-increased-online-risk-during-covid-19-pandemic 16/07/2021

55 The impact of the coronavirus pandemic on child welfare: sexual abuse (NSPCC, 2020) Accessed from: https://learning.nspcc.org.uk/media/2280/impact-of-coronavirus-pandemic-on-child-welfare-sexual-abuse.pdf 16/07/2021

56 Aumentan casos de abuso infantil tras relajar medidas en Paraguay (Prensa Latina, 2021) Accessed from: https://www.prensa-latina.cu/index.php?o=rn&id=437283 07/06/2021

57 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 07/06/2021

58 Child protection in the time of COVID-19 (Australian Institute of Health and Welfare, 2021) Accessed from: https://www.aihw.gov.au/reports/child-protection/child-protection-in-the-time-of-covid-19/summary 16/06/2021

59 Protecting children from violence in the time of COVID-19: Disruptions in prevention and response services (Unicef, 2020) Accessed from: https://www.unicef.org/reports/protecting-children-from-violence-covid-19-disruptions-in-prevention-and-response-services-2020 07/06/2021

60 Netclean Annual Report; Insight 5: COVID-19 has affected the capacity to investigate child sexual abuse crimes (Netclean, 2021) Accessed from: https://www.netclean.com/netclean-report-2020/insight-5/ 07/06/2021

61 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf 22/04/2021

62 States divert funds, cut expenditure to foot COVID-19 bill (Economic Times, 2021) Accessed from: https://economictimes.indiatimes.com/news/india/states-divert-funds-cut-expenditure-to-foot-covid-19-bill/articleshow/82448577.cms?from=mdr 07/06/2021

63 Policy Responses to COVID-19: Iraq (International Monetary Fund, 2021) Accessed from: https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19#top 07/06/2021

64 UK's drastic cut to overseas aid risks future pandemics, say Sage experts (Guardian, 2021) Accessed from: https://www.theguardian.com/education/2021/mar/20/uks-drastic-cut-to-overseas-aid-risks-future-pandemics-say-sage-experts 16/07/2021

65 100+ Internet Statistics and Facts for 2021 (Website Hosting Rating, 2021) Accessed from: https://www.websitehostingrating.com/internet-statistics-facts/ 29/04/2021

66 Worldwide digital population as of January 2021 (Statista, 2021) Accessed from: https://www.statista.com/statistics/617136/digital-population-worldwide/ 29/04/2021

67 In-depth analysis of changes in world internet performance (GSMA, 2019) Accessed from: https://www.gsma.com/membership/resources/in-depth-analysis-of-changes-in-world-internet-performance-using-the-speedtest-global-index/ 29/04/2021

68 Number of mobile devices worldwide 2020-2024 (Statista, 2020) Accessed from: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/ 29/04/2021

69 Children in a digital world (Unicef, 2017) Accessed from: https://www.unicef.org/media/48601/file 29/04/2021

70 Africa Is the Next Frontier For The Internet (Forbes, 2020) accessed from: https://www.forbes.com/sites/miriamtuerk/2020/06/09/africa-is-the-next-frontier-for-the-internet/?sh=e8ecd3b49001 04/05/2021

71 Strong mobile growth predicted for sub-Saharan Africa (Connecting Africa, 2020) Accessed from: http://www.connectingafrica.com/author.asp?section_id=761&doc_id=764310 04/05/2021

72 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 02/04/2021

73 Mobile technology the key to bringing 'education to all', says UN Broadband Commission (Unesco, 2014) Accessed from: https://en.unesco.org/news/mobile-technology-key-bringing-education-all-says-broadband-commission 14/05/2021

74 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

75 The Internet of Toys: Implications of increased connectivity and convergence of physical and digital play in young children (LSE, 2017) Accessed from: https://blogs.lse.ac.uk/parenting4digitalfuture/2017/07/19/the-internet-of-toys-implications-of-increased-connectivity-and-convergence-of-physical-and-digital-play-in-young-children/ 20/07/2021

76 Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking (Thorn, 2021) Accessed from: https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/ 15/07/2021

77 Exposure to sexually explicit media in early adolescence (Lin et al., 2020) Accessed from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0230242 16/02/2021

78 Growing up in a connected world (UNICEF, 2019) Accessed from: https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf 30/04/2021

79 Child and adolescent pornography exposure (Hornor, 2020) Accessed from: https://www.jpedhc.org/article/S0891-5245(19)30384-0/fulltext 30/04/2021

80 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)

81 Action to End Child Sexual Abuse and Exploitation (UNICEF, 2020) p.50 Accessed from: https://www.unicef.org/media/89026/file/CSAE-Report.pdf 17/05/2021

82 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

83 Growing up in a connected world (UNICEF, 2019) Accessed from: https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf 30/04/2021

84 Impact of online and offline child sexual abuse: "Everyone deserves to be happy and safe" (NSPCC, 2017) Accessed from: https://learning.nspcc.org.uk/research-resources/2017/impact-online-offline-child-sexual-abuse 17/05/2021

85 Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking (Thorn, 2021) Accessed from: https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/ 15/07/2021

86 How Everyone's Invited's 'rape culture' claims sparked a #MeToo movement in UK schools (Evening Standard, 2021) Accessed from: https://www.standard.co.uk/insider/everyones-invited-rape-culture-metoo-movement-schools-b925924.html 18/05/2021

87 #MeToo in school: too many children are sexually harassed by classmates (The Guardian, 2018) Accessed from: https://www.theguardian.com/commentisfree/2018/feb/11/metoo-school-children-teens-sexual-harassment (18/05/2021)

88 Everyone's Invited (Everyone's Invited, 2020) Accessed from: https://www.everyonesinvited.uk/ 18/05/2021

89 Children and parents: Media use and attitudes report 2019 (Ofcom, 2019) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf 18/05/2021

90 PA Consulting Engagement with Edward Dixon (Rigr AI), 18/03/2021

91 'End Online Violence: Learnings from Sri Lanka' Conference (End Violence Against Children, 25/02/2021)

92 Darknet Cybercrime Threats to South East Asia (UNODC, 2021) Accessed from: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf 29/04/2021

93 PA Consulting engagement with Interpol, 25/03/2021

94 Interpol: International police coordination required to combat global cyberthreats (CSO, 2021) Accessed from: https://www.csoonline.com/article/3624992/interpol-international-police-coordination-required-to-combat-global-cyberthreats.html 20/07/2021

95 Child sexual abuse material: Model legislation and global review (ICMEC, 2021) Accessed from: https://www.icmec.org/csam-model-legislation/ 29/04/2021

96 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

97 PA Consulting engagement with Europol, 17/03/2021

98 'Legality of Child Pornography' (Wikipedia, 2021) Accessed from: https://en.wikipedia.org/wiki/Legality_of_child_pornography 17/05/2021

99 PA Consulting engagement with United States Department of Justice, 22/03/2021

100 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf 18/05/2021

101 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021

102 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021

103 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 2/4/2021

104 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 2/4/2021

105 Metadata-based detection of child sexual abuse material (Periera, Dodhia and Brown, 2020) Accessed from: https://arxiv.org/pdf/2010.02387.pdf 29/04/2021

106 PA Consulting engagement with Terre des Hommes, 25/02/2021

107 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf 18/05/2021

108 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021

109 Together to #ENDviolence: Global Policy Briefing; Key Messages (The End Violence Partnership, 2020) Received via email from the End Violence Partnership on 13/07/2021

110 Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf 02/06/2021

111 Handbook for policy makers on the rights of the child in the digital environment (Council of Europe, 2020) Accessed from: https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8 06/05/021

112 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

113 Germany's Network Enforcement Act and its impact on social networks (Taylor Wessing, 2018) Accessed from: https://www.taylorwessing.com/download/article-germany-nfa-impact-social.html 10/06/21

114 Email received from the Office of the e-Safety Commissioner, 13/07/2021

115 UK to introduce world first online safety laws (GOV.UK, 2019) Accessed from: https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws 10/06/2021

116 The EU unveils its plan to rein in big tech (Economist, 2020) Accessed from: https://www.economist.com/business/2020/12/15/the-eu-unveils-its-plan-to-rein-in-big-tech 10/06/2021

117 Online Safety and Media Regulation Bill (GOV.IE, 2020) Accessed from: https://www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/ 10/06/2021

118 Communication from the Commission to the European parliament, the council, the European economic and Social Committee and the Committee of the Regions: EU Strategy for a more effective fight against child sexual abuse (European Commission, 2020) Accessed from: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf 10/06/2021

119 End-to-End Encryption: Understanding the impacts for child safety online (NSPCC, 2021) Accessed from: https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf 10/06/2021

120 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021

121 Google is testing end-to-end encryption in android messages (Wired, 2020) Accessed from: https://www.wired.com/story/google-is-testing-end-to-end-encryption-in-android-messages/ 10/06/2021

122 NSPCC urges Facebook to stop encryption plans (BBC News, 2020) Accessed from: https://www.bbc.co.uk/news/technology-51391301 10/06/2021

123 End-to-End Encryption (NSPCC, 2021) Accessed from: https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf 25/05/2021

124 Briefing on the future of digital tools to detect child sexual exploitation and abuse online in Europe (WeProtect Global Alliance, 2021) Accessed from: https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/600086ba8f223010c1b4b756/1610647258029/WPGA+European+ePrivacy+briefing+Jan+21.pdf 10/06/2021

125 A battle won, but not the war in the global fight for child safety (NCMEC, 2021) Accessed from: https://www.missingkids.org/childsafetyfirst#:~:text=As%20NCMEC%20has%20recently%20reported%2C%20we%20have%20seen,to%20offer%20permanent%20solutions%20for%20child%20safety%20online. 10/06/2021

126 Provisional agreement on temporary rules to detect and remove online child abuse (News, European Parliament, 2021) Accessed from: https://www.europarl.europa.eu/news/en/press-room/20210430IPR03213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse 22/06/2021

127 Project Beacon: EU comes to political agreement to continue the use of online tools against CSAM (ECPAT, 2021) Accessed from: https://www.ecpat.org/news/tag/project-beacon/ 21/07/2021

128 The EU Strategy on the Rights of the Child and the European Child Guarantee (European Commission, 2021) Accessed from: The EU Strategy on the Rights of the Child and the European Child Guarantee | European Commission (europa.eu) 21/07/2021

129 Fighting against child sexual abuse: join the stakeholder consultation (European Commission, 2021) Accessed from: https://ec.europa.eu/home-affairs/news/fighting-against-child-sexual-abuse-join-stakeholder-consultation_en 21/07/2021

130 NCMEC's Statement Regarding End-to End Encryption (NCMEC, 2019) Accessed from: https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption 10/06/2021

131 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021

132 Statement on end-to-end encryption and public safety (Australian Government Department of Home Affairs, 2021) Shared by the Australian Department of Home Affairs by email, 19/05/2021

133 VGT position on End-to-End Encryption (Virtual Global Taskforce, 2021 Received via email from the NCA on 14/06/2021

134 NCA National Strategic Assessment of Serious and Organised Crime (National Crime Agency, 2021) Received via email from the NCA on 25/05/2021

135 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021

136 Opinion: Facebook's encryption makes it harder to detect child abuse (Berkeley, 2019) Accessed from: https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-encryption-makes-it-harder-detect-child-abuse 10/06/2021

137 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021

138 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021

139 Opinion: Facebook's encryption makes it harder to detect child abuse (Berkeley, 2019) Accessed from: https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-encryption-makes-it-harder-detect-child-abuse 10/06/2021

140 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021

141 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021

142 End-to-End Encryption (NSPCC, 2021) Accessed from: https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf 25/05/2021

143 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021

144 Project Arachnid: Online Availability of Child Sexual Abuse Material (Canadian Centre for Child Protection, 2021) Accessed from: https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/ 10/06/2021

145 Webinar: The Online Harms Bill – more harm than good? (11KBW, 20/05/2021)

146 Protection of children should always trump protection of privacy (Julie Inman Grant, eSafety Commissioner, 2020) Accessed from: https://www.esafety.gov.au/about-us/blog/protecting-children-should-always-trump-protecting-privacy 10/06/2021

147 The Decentralised Web of Hate: White Supremacists are starting to use peer-to-peer technology; are we prepared? (Rebellious Data LLC, 2020) Accessed from: https://rebellious-data.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf 10/06/2021

148 Messaging services are providing a more private internet (Economist, 2021) Accessed from: https://www.economist.com/international/2021/01/23/messaging-services-are-providing-a-more-private-internet 10/06/2021

149 Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf 02/06/2021

150 Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2020) Accessed from: https://www.weprotect.org/library/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/ 10/06/2021

151 Tech giants list principles for handling harmful content (Axios, 2021) Accessed from: https://www.axios.com/tech-giants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html 10/06/2021

152 The Technology Coalition Announces Project Protect (Technology Coalition, 2020) Accessed from: https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/ 24/06/2021

153 Online enticement reports skyrocket in 2020 (NCMEC, 2021) Accessed from: https://www.missingkids.org/blog/2021/online-enticement-reports-skyrocket-in-2020 24/02/2021

154 Online enticement (NCMEC) Accessed from: https://www.missingkids.org/netsmartz/topics/onlineenticement 19/04/2021

155 Online child sexual abuse activity has increased (NetClean, 2021) Accessed from: https://www.netclean.com/netclean-report-2020/insight-2/ 26/01/2021

156 Trends identified in CyberTipline sextortion reports (NetClean, 2016) Accessed from: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf 01/03/2021

157 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 02/04/2021

158 Out of the Shadows (Economist Impact, 2018) Accessed from: https://outoftheshadows.eiu.com/ 25/01/2021

159 Online grooming of children for sexual purposes (ICMEC, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf 04/02/2021

160 Kids & Tech: Evolution of Today's Digital Natives (Influence Central, 2017) Accessed from: https://influence-central.com/trendspotting/launching-the-new-influence-central-trend-report 12/04/2021

161 Technology working group report (Child Dignity Foundation, 2018) Accessed from: https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf 26/02/2021

162 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

163 Online grooming: What it is, how it happens, and how to defend children (Thorn, 2020) Accessed from: https://www.thorn.org/blog/online-grooming-what-it-is-how-it-happens-and-how-to-defend-children/ 07/04/2021

164 The impact of the Coronavirus pandemic on child welfare: Online abuse (NSPCC, 2020) Accessed from: https://learning.nspcc.org.uk/media/2390/impact-of-coronavirus-pandemic-on-child-welfare-online-abuse.pdf 10/03/2021

165 Trends identified in cybertipline sextortion reports (NetClean, 2016) Accessed from: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf 01/03/2021

166 The impact of the Coronavirus pandemic on child welfare: Online abuse (NSPCC, 2020) Accessed from: https://learning.nspcc.org.uk/media/2390/impact-of-coronavirus-pandemic-on-child-welfare-online-abuse.pdf 11/03/2021

167 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation 28/01/2021

168 COVID-19 accelerates global video gaming market to $170bn (Consultancy-me.com, 2020) Accessed from: https://www.consultancy-me.com/news/3041/covid-19-accelerates-global-gaming-market-to-170-billion 16/02/2021

169 The Marie Collins Foundation, Accessed from: https://www.mariecollinsfoundation.org.uk/ 29/04/2021

170 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies

171 Online grooming of children for sexual purposes (ICMEC, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf 04/02/2021

172 Safety-by-design overview (eSafety Commissioner, 2019) Accessed from: https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf 11/02/2021

173 Digital Age Assurance Tools and Children's Rights Online across the Globe (UNICEF, 2021) Accessed from: https://www.unicef.org/media/97461/file/Digital%20Age%20Assurance%20Tools%20and%20Children%E2%80%99s%20Rights%20Online%20across%20the%20Globe.pdf 07/05/2021

174 Video games and online chats are 'hunting grounds' for sexual predators (New York Times, 2019) Accessed from: https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html 21/04/2021

175 Case study submission from TikTok, received on 10/05/2021

176 Continuing to Make Instagram Safer for the Youngest Members of Our Community (Instagram, 2021) Accessed from: https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community 21/04/2021

177 What is a supervised experience on YouTube? (Google, 2021) Accessed from: https://support.google.com/youtube/answer/10314940?hl=en 20/07/2021

178 Perpetrators of sexual violence: statistics (RAINN) Accessed from: https://www.rainn.org/statistics/perpetrators-sexual-violence 16/04/2021

179 The sexual exploitation and abuse of deaf and disabled children online (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/Intelligence-briefing-2021-The-sexual-exploitation-and-abuse-of-disabled-children.pdf 23/02/2021

180 Ending violence against children: key messages and statistics (End Violence Against Children) https://www.end-violence.org/sites/default/files/paragraphs/download/Key Messages_Long_0.pdf 12/04/2021

181 CyberTipline: 2019 & 2020 Reports by country (NCMEC, 2020) accessed from: https://www.missingkids.org/gethelpnow/cybertipline 19/04/2021

182 Online sexual exploitation of children in the Philippines (International Justice Mission, 2020) Accessed from: https://www.ijm.org/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 17/02/2021

183 Annual Report 2020 (INHOPE, 2021) Accessed from: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf 06/05/2021

184 IWF Annual Report: International Overview (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/overview 21/04/2021

185 Self-generated child sexual abuse (IWF Annual Report, 2020) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 29/07/2021

186 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 04/03/2021

187 Violencia sexual a menores ya deja mas de mil victimas en lo corrido de 2021 (LAFM, 2021) Accessed from: https://www.lafm.com.co/colombia/violencia-sexual-menores-ya-deja-mas-de-mil-victimas-en-lo-corrido-de-2021 11/03/2021

188 Abuso sexual en internet y redes de trata (Infobae, 2020) Accessed from: https://www.infobae.com/america/mexico/2020/07/27/abuso-sexual-en-internet-y-redes-de-trata-los-crimenes-contra-la-ninez-que-aumentaron-durante-la-pandemia/ 25/02/2021

189 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021

190 Los casos de abuso sexual contra menores en espana se multiplican por 4 en la ultima decada (Levante, 2021) Accessed from: https://protect-eu.mimecast.com/s/WuEPCWnWgFxLBY3Hxchqm?domain=levante-emv.com 23/02/2021

191 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021

192 Online enticement of children: an in-depth analysis of CyberTipline reports (National Center for Missing and Exploited Children, 2017) Accessed from: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel1.pdf 11/02/2021

193 The cycle of child sexual abuse stops now (Project Arachnid) Accessed from: https://projectarachnid.ca/en/ 07/04/2021

194 PA Consulting engagement with United States Department of Justice, 22/03/2021

195 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021

196 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic 26/01/2021

197 Child abuse predator 'handbook' lists ways to target children during coronavirus lockdown (The Guardian, 2020) Accessed from: https://www.theguardian.com/society/2020/may/14/child-abuse-predator-handbook-lists-ways-to-target-children-during-coronavirus-lockdown 23/02/2021

198 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic 26/01/2021

199 PA Consulting engagement with Australian Centre to Counter Child Exploitation, 01/03/2021

200 South Korea confronts its voyeurism epidemic (The Guardian, 2018) Accessed from: https://www.theguardian.com/world/2018/jul/03/a-part-of-daily-life-south-korea-confronts-its-voyeurism-epidemic-sexual-harassment 08/03/2021

201 Netclean Report 2019: A report about child sexual abuse crime (Netclean, 2019) Accessed from: https://www.netclean.com/netclean-report-2019/ 28/01/2021

202 A deepfake porn bot is being used to abuse thousands of women (WIRED, 2020) Accessed from: https://www.wired.co.uk/article/telegram-deepfakes-deepnude-ai 19/03/2021

203 Cybersex, erotic tech and virtual intimacy are on the rise during COVID-19 (The Conversation, 2020) Accessed from: https://theconversation.com/cybersex-erotic-tech-and-virtual-intimacy-are-on-the-rise-during-covid-19-141769 19/03/2021

204 Immersive Technologies – Position Statement (e-Safety Commissioner, 2021) Accessed from: https://www.esafety.gov.au/about-us/tech-trends-and-challenges/immersive-tech 14/07/2021

205 CGI (Computer Generated Imagery) (TechTarget, 2016) Accessed from: https://whatis.techtarget.com/definition/CGI-computer-generated-imagery 08/04/2021

206 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 17/03/2021

207 What is deepfake? (Business Insider, 2021) Accessed from: https://www.businessinsider.com/what-is-deepfake?r=US&IR=T#:~:text=Recently%2C%20deepfake%20technology%20has%20been,with%20another%20in%20recorded%20video 08/04/2021

208 PA Consulting engagement with Terre des Hommes, 25/02/2021

209 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT France, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 09/08/2021

210 Non-photographic visual depictions (Internet Watch Foundation, 2007) Accessed from: https://www.iwf.org.uk/what-we-do/who-we-are/consultations/non-photographic-visual-depictions 17/03/2021

211 Child Sexual Abuse Material: Model Legislation and Global Review (International Center for Missing and Exploited Children, 2018) Accessed from: https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf 05/03/2021

212 Computer-generated 'Sweetie' catches online predators (BBC News, 2013) Accessed from: https://www.bbc.co.uk/news/uk-24818769 08/03/2021

213 Child sexual abuse in the digital era: Rethinking legal frameworks and transnational law enforcement collaboration (Universiteit Leiden, 2020) Accessed from: https://scholarlypublications.universiteitleiden.nl/access/item%3A2966712/view 07/05/2021

214 National Strategic Assessment of Serious and Organised Crime 2020 (National Crime Agency, 2020) Accessed from: https://www.nationalcrimeagency.gov.uk/news/nsa2020 24/03/2021

215 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic 26/01/2021

216 PA Consulting engagement with Interpol, 25/03/2021

217 PA Consulting engagement with Ethel Quayle, 04/03/2021

218 The Internet: Investigation Report (Independent Inquiry into Child Sexual Exploitation and Abuse, 2020) Accessed from: https://www.iicsa.org.uk/publications/investigation/internet 02/02/2021

219 Internet Organised Crime Threat Assessment (IOCTA) 2020 (Europol, 2020) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 30/03/2021

220 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment 20/04/2021

221 Child Rescue Coalition (CRC): Protecting Innocence Through Technology (CRC, 2021) Email received from CRC, 30/03/2021

222 Global Threat Assessment 2019 (WeProtect Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 26/01/2021

223 Hackers leaked 22 million records on the dark web in 2020 (ID Agent, 2020) Accessed from: https://www.idagent.com/hackers-leaked-22-million-records-on-the-dark-web-in-2020 29/04/2021

224 Trends in Online Child Sexual Abuse Material (ECPAT, 2017) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/05/Emerging-Issues-and-Global-Threats-Children-online-2017-1.pdf 25/03/2021

225 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation 20/04/2021

226 Brave.com now has its own Tor onion service, providing more users with secure access to Brave (Brave.com, 2020) Accessed from: https://brave.com/new-onion-service/ 20/04/20

227 Tor (Investopedia, 2019) Accessed from: https://www.investopedia.com/terms/t/tor.asp 07/05/2021

228 PA Consulting engagement with United States Department of Justice, 07/04/2021 NCMEC Engagement

229 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021

230 PA Consulting engagement with United States National Centre for Missing and Exploited Children, 16/03/2021

231 Millions of attempts to access child sexual abuse online during lockdown (Internet Watch Foundation, 2020) Accessed from: https://www.iwf.org.uk/news/millions-of-attempts-to-access-child-sexual-abuse-online-during-lockdown 08/02/2021

232 COVID-19 conversations: The Crisis of Online Child Exploitation (Equality Now, 2021) Accessed from: https://www.equalitynow.org/covid_19_online_exploitation 07/06/2021

233 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 04/03/2021

234 The Motivation-Facilitation Model of Sexual Offending (Michael C. Seto, 2017) Accessed from: https://journals.sagepub.com/doi/full/10.1177/1079063217720919 29/07/2021

235 Internet Sex Offenders (Seto, Michael C., 2013)

236 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

237 Sexual interests of child sexual exploitation material (CSEM) consumers (Fortin and Proulx, 2018) Accessed from: https://journals.sagepub.com/doi/10.1177/0306624X18794135 11/02/2021

238 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo 05/03/2021

239 How extreme porn has become a gateway drug into child abuse (The Guardian, 2020) Accessed from: https://www.theguardian.com/global-development/2020/dec/15/how-extreme-porn-has-become-a-gateway-drug-into-child-abuse 15/02/2021

240 Effects of automated messages on internet users attempting to access 'barely legal' pornography (Prichard, Wortley, Watters, Spiranovic, Hunn, Krone, 2020) Received from Donald Findlater (Lucy Faithfull Foundation), 16/02/2021

241 Exposure to sexually explicit media in early adolescence (Lin et al., 2020) Accessed from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0230242 16/02/2021

242 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)

243 On Youtube's Digital Playground, an Open Gate for Pedophiles (The New York Times, 2019) Accessed from: https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html?module=inline 04/03/2021

244 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo 05/03/2021

245 On Youtube, a network of paedophiles is hiding in plain sight (WIRED, 2019) Accessed from: https://www.wired.co.uk/article/youtube-pedophile-videos-advertising 31/03/2021

246 Barriers Abusers Overcome In Order To Abuse (Psychology Tools) Accessed from: https://www.psychologytools.com/resource/barriers-abusers-overcome-in-order-to-abuse/ 29/03/2021

247 Child Sexual Abuse (Finkelhor, 1984)

248 The Four Rs of Responsibility, Part 1: Removing Harmful Content (Youtube, 2019) Accessed from: https://blog.youtube/inside-youtube/the-four-rs-of-responsibility-remove/ 27/07/2021

249 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (NatCen Social Research, 2017) Accessed from: https://natcen.ac.uk/media/1535277/Behaviours-and-characteristics-of-perpetrators-of-online-facilitated-child-sexual-abuse-and-exploitation.pdf 09/02/2021

250 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies

251 Online sexual exploitation of children in the Philippines (International Justice Mission, 2020) Accessed from: https://www.ijm.org/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 23/02/2021

252 Effects of automated messages on internet users attempting to access 'barely legal' pornography (Pritchard et al., 2020)

253 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo 05/03/2021

254 Ground-breaking research on perpetrator prevention (Oak Foundation, 2021) Accessed from: https://oakfnd.org/groundbreaking-research-on-perpetration-prevention/ 13/07/2021

255 IWF Annual Report: About Our Year (IWF, 2020) Accessed from: https://annualreport2020.iwf.org.uk/about/year/ceo 21/04/2021

256 Game-changing chatbot to target people trying to access child sexual abuse online (IWF, 2020) Accessed from: https://www.iwf.org.uk/news/game-changing%E2%80%99-chatbot-to-target-people-trying-to-access-child-sexual-abuse-online 20/04/2021

257 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo 05/03/2021

258 Suojellaan Lapsia, Accessed from: https://suojellaanlapsia.fi/ 29/04/2021

259 COVID-19 and Missing and Exploited Children (NCMEC, 2021) Accessed from: https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children 22/04).

260 IWF Annual Report: 2020 Trends and Data (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends 22/04/2021

261 Annual Report 2020 (INHOPE, 2021) Accessed from: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf 06/05/2021

262 PA Consulting engagement with NCMEC, 16/03/2021

263 PA Consulting Engagement with NCMEC, 22/04/2021

264 IWF Annual Report: Site types analysis (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/sitetypes 22/04/2021

265 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation 28/01/2021

266 PA Consulting engagement with Interpol, 25/03/2021

267 IWF Annual Report: Hidden Services (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/Trends/International/Other/Hidden 22/04

268 IWF Annual Report: Glossary (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/glossary 10/05/2021

269 How child sexual abuse material is stored (Netclean, 2019) Accessed from: https://www.netclean.com/netclean-report-2019/insight-4/ 22/04/2021

270 Annual Report 2020 (INHOPE, 2021) Accessed from: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf 06/05/2021

271 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021

272 PA Consulting engagement with United States Department of Justice, 22/03/2021

273 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021

274 Preventing Child Exploitation on our Apps (Facebook, 2020) Accessed from: https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/#:~:text=Using%20our%20apps%20to%20harm,authorities%20to%20keep%20children%20safe. 22/04/2021

275 Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims (Thorn, 2018) Accessed from: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM_FullReport_FINAL.pdf 15/07/2021

276 Study on the effects of new information technologies on the abuse and exploitation of children (United Nations Office on Drugs and Crime, 2015) Accessed from: https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf 22/04/2021

277 Crime investigations of 'child abuse material' - Challenges and opportunities posed by digital technology (Marie Eneman, 2020) Accessed from: https://www.researchgate.net/publication/344072738_Crime_investigations_of_'child_abuse_material'_-_Challenges_and_opportunities_posed_by_digital_technology 10/05/2021

278 Production of child sexual abuse material by parental figures (Australian Government, Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 16/07/2021

279 Understanding the intentions of Child Sexual Abuse Material (CSAM) sharers (Facebook Research, 2021) Accessed from: https://research.fb.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/ 29/06/2021

280 IWF Annual Report: Commercial content (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/Trends/International/Commercial 22/04/2021

281 IWF Annual Report: Domain analysis (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/domain 22/04/2021

282 IWF Annual Report: Commercial content (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/Trends/International/Commercial 22/04/2021

283 Cryptocurrency and the trade of online child sexual abuse material (ICMEC, 2021) Accessed from: https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf 22/04/21

284 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other 22/04/2021

285 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other 22/04/2021

286 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other 22/04/2021

287 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: https://www.netclean.com/2018/10/30/hash-values/ 22/04/2021

288 International Child Sexual Exploitation Database (INTERPOL, 2018) Accessed from: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database 22/04/2021

289 IWF Annual Report: Hidden Services (IWF, 2020) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other/hidden 10/05/2021

290 IWF Annual Report: Geographical hosting (IWF, 2020) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/geographic 10/05/2021

291 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies

292 PA Consulting engagement with IWF, 01/03/2021

293 PA Consulting engagement with Interpol, 25/03/2021

294 PA Consulting engagement with IWF, 01/03/2021

295 Technology working group report (Child Dignity Foundation, 2018) Accessed from: https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf 26/02/2021

296 Child Dignity Alliance: Technical Working Group Report (Child Dignity Alliance, 2017) Accessed from: https://static1.squarespace.com/static/5a4d5d4e7131a5845cdd690c/t/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf 22/04/2021

297 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021

298 IWF Annual Report: Self-generated content study (IWF, 2012) Accessed from: https://www.iwf.org.uk/sites/default/files/reports/2016-02/IWF%202012%20Annual%20and%20Charity%20Report%20%28web%29.pdf 06/05/2021

299 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021

300 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

301 PA Consulting engagement with Internet Watch Foundation, 01/03/2021

302 Interim code of practice on online child sexual exploitation and abuse (accessible version)(GOV.UK, 2020) Accessed from: https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-online-child-sexual-exploitation-and-abuse-accessible-version 19/07/2021

303 Initial Situational Analysis on Online Child Sexual Exploitation in Cambodia (Royal Government of Cambodia, 2019) Accessed from: https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia_ENG.pdf 06/05/2021

304 Prevalence of Multiple Forms of Sexting Behaviour Among Youth (Madigan et al., 2018) Accessed from: https://jamanetwork.com/journals/jamapediatrics/fullarticle/2673719?resultClick=1 06/05/2021

305 'Staying Safe Online' survey: wat unwanted sexual images are being sent to teenagers on social media? (University College London, 2019) Accessed from: https://blogs.ucl.ac.uk/ioe/2020/06/19/staying-safe-online-survey-what-unwanted-sexual-images-are-being-sent-to-teenagers-on-social-media/ 20/07/2021

306 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021

307 IWF Annual Report: Who we are (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/about/us 11/05/2021

308 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

309 An Exploratory Study of Sexting Behaviours Among Heterosexual and Sexual Minority Early Adolescents (Van Ouytsel et al., 2019) Accessed from: https://pubmed.ncbi.nlm.nih.gov/31473082/ 14/05/2021

310 Look at me: Teens, Sexting, and Risks (Internet Matters, 2021) Accessed from https://www.internetmatters.org/wp-content/uploads/2020/06/Internet-Matters-Look-At-Me-Report-1.pdf 06/05/2021

311 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (National Centre for Social Research, 2018) Accessed from: https://www.iicsa.org.uk/key-documents/3720/download/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf 06/05/2021

312 Online harmful sexual behaviours in children and young people under 18 (eSafety Commissioner, 2020) Accessed from: https://www.esafety.gov.au/sites/default/files/2020-09/Online%20harmful%20sexual%20behaviours%20Position%20statement.pdf 13/07/2021

313 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

314 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://info.thorn.org/hubfs/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf 28/07/2021

315 A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people (NSPCC, Children's Commissioner, Middlesex University London, 2016) Accessed from: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/MDX-NSPCC-OCC-Online-Pornography-Report.pdf 28/07/2021

316 A Rapid Assessment of Live Streaming of Online Sexual Abuse and Exploitation of Children and Young People in Kathmandu (ECPAT Luxembourg, ChildSafeNet) Draft, due to be published in 2021. Received by email from ChildSafeNet Nepal, 04/03/2021

317 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

318 Online Nation: 2021 Report (Ofcom, 2021) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf 24/06/2021

319 Faster Takedown of Online Sexual Abuse Sought (Manila-Standard.Net, 2021) Accessed from: https://manilastandard.net/mobile/article/349129 06/05/2021

320 Initial Situational Analysis on Online Child Sexual Exploitation in Cambodia (Royal Government of Cambodia, 2019) Accessed from: https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia_ENG.pdf 06/05/2021

321 The children selling explicit videos on OnlyFans (BBC News, 2021) Accessed from: https://www.bbc.co.uk/news/uk-57255983 07/07/2021

322 Netclean Annual Report 2020; Insight 4: Moderate increase in actual investigations and cases (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-4/ 06/05/2021

323 'Grave threat' to children from predatory internet groomers as online child sexual abuse material soars to record levels (IWF, 2021) Accessed from: https://www.iwf.org.uk/news/%E2%80%98grave-threat%E2%80%99-children-predatory-internet-groomers-online-child-sexual-abuse-material-soars 07/05/2021

324 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (National Centre for Social Research, 2018) Accessed from: https://www.iicsa.org.uk/key-documents/3720/download/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf 06/05/2021

325 Emerging Patterns and Trends Report: Online-Produced Sexual Content (IWF, 2015) p.3 Accessed from: https://www.iwf.org.uk/sites/default/files/inline-files/Online-produced_sexual_content_report_100315.pdf 19/05/2021

326 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf?__hstc=208625165.851aa734d938b21fee07aa6d05-bc-9e7.1604505256798.1614622415296.1614700924025.7&__hssc=208625165.2.1614700924025&__hsfp=723267087 06/05/2021

327 The Internet: Investigation Report (Independent Inquiry into Child Sexual Exploitation and Abuse, 2020) Accessed from: https://www.iicsa.org.uk/publications/investigation/internet 02/02/2021

328 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

329 PA Consulting Engagement with SafeBAE, 02/03

330 SafeToNet acquires German mobile phone stores to safeguard children online (PR Newswire, 2021) Accessed from: https://www.prnewswire.com/news-releases/safetonet-acquires-german-mobile-phone-stores-to-safeguard-children-online-301247334.html 14/05/2021

331 Handbook for policy makers on the rights of the child in the digital environment (Council of Europe, 2020) Accessed from: 1680a069f8 (coe.int) 06/05/021

332 Teen sexting is decriminalised between partners of similar age (news.com.au, 2018) Accessed from: https://www.news.com.au/national/nsw-act/courts-law/teen-sexting-is-decriminalised-between-partners-of-similar-age/news-story/3fdceb4adbd2c6028eab1f76a86ba5ab 06/05/2021

333 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Council of Europe, 2007) Accessed from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/699615/MS4.2018_Lanzarote_CM9602_WEB.pdf 22/06/2021

334 Police Response to Youth Offending Around the Generation and Distribution of Indecent Images of Children and its Implications (University of Suffolk/ Marie Collins Foundation, 2019) Accessed from: https://www.uos.ac.uk/sites/www.uos.ac.uk/files/FOI-Report-Final-Outcome-21_2.pdf 13/05/2021

335 Sharing nudes and semi-nudes: advice for education settings working with children and young people (GOV.UK, 2020) Accessed from: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people 01/06/2021

336 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 13/05/2021

337 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 13/05/2021

338 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 13/05/2021

339 Sexting among high school students in a metropolis in Ghana: an exploratory study (Baiden et al., 2019) Accessed from: https://www.tandfonline.com/doi/abs/10.1080/17482798.2020.1719854 07/05/2021

340 Sexting: Prevalence, Predictors, and Associated Sexual Risk Behaviors among Postsecondary School Young People in Ibadan, Nigeria (Olatunde and Balogun, 2017) Accessed from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5420550/ 07/05/2021

341 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf?__hstc=208625165.851aa734d938b21fee07aa6d05bc9e7.1604505256798.1614622415296.1614700924025.7&__hssc=208625165.2.1614700924025&__hsfp=723267087 06/05/2021

342 A Rapid Assessment of Live Streaming of Online Sexual Abuse and Exploitation of Children and Young People in Kathmandu (ECPAT Luxembourg, ChildSafeNet) Draft, due to be published in 2021. Received by email from ChildSafeNet Nepal, 04/03/2021

343 The reception of sexual messages among young Chileans and Uruguayans (Alfaro et al., 2020) Accessed from: https://www.researchgate.net/publication/347336149_The_reception_of_sexual_messages_among_young_Chileans_and_Uruguayans 28/05/2021

344 Online Harms White Paper (UK Government, 2019) Accessed from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf 07/05/2021

345 Teenage Sexting and Sexual Behaviours in an Iranian Setting (Ghorashi, 2019) Accessed from: https://www.researchgate.net/publication/333826458_Teenage_Sexting_and_Sexual_Behaviors_in_an_Iranian_Setting 19/05/2021

346 Demystifying Sexting: Adolescent Sexting and its Associations With Parenting Styles and Sense of Parental Social Control in Israel (Dolev-Cohen and Ricon, 2020) Accessed from: https://cyberpsychology.eu/article/view/11878/11340 19/05/2021

347 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf 22/04/2021

348 COVID-19: Child sexual exploitation and abuse threats and trends (Interpol, 2020) Accessed from: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse 26/01/2021

349 Safe from harm: Tackling webcam child sexual abuse in the Philippines (UNICEF, 2016) Accessed from: https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines 09/08/21

350 Online sexual abuse of children rising amid COVID 19 pandemic – Save the Children Philippines (Relief Web, 2021) Accessed from: https://reliefweb.int/report/philippines/online-sexual-abuse-children-rising-amid-covid-19-pandemic-save-children 22/04/2021

351 Technical and Financial Sector Indicators of Livestreaming (IJM, 2020) Shared by IJM, 11/03/2021

352 Technical and Financial Sector Indicators of Livestreaming (IJM, 2020) Shared by IJM, 11/03/2021

353 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021

354 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

355 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021

356 Victims of livestreamed child sexual abuse (Netclean, 2019) Accessed from https://www.netclean.com/netclean-report-2019/insight-2/ 22/04/2021

357 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf 22/04/2021

358 UNICEF: What works to prevent online and offline child sexual exploitation and abuse: Review of national education strategies in East Asia and the Pacific (UNICEF, 2020) Accessed from https://www.sddirect.org.uk/media/1874/what-works-to-prevent-online-and-offline-csae-in-east-asia-and-the-pacific.pdf 22/04/2021

359 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021

360 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021

361 Impact of the COVID 19 pandemic on trafficking in persons (UNODC, 2021) Accessed from: https://www.unodc.org/documents/Advocacy-Section/HTMSS_Thematic_Brief_on_COVID-19.pdf 22/04/2021

362 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021

363 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment 20/04/2021

364 National Study of Online Sexual Abuse and Exploitation of Children in the Philippines (UNICEF, 2020) Accessed from: UNICEF Philippines study 22/04/2021

365 Why are human trafficking cases difficult to identify and prosecute (John Vanek, 2018) Accessed from: https://johnvanek.com/2018/01/25/why-are-human-trafficking-cases-difficult-to-identify-and-prosecute/ 11/05/2021

366 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf 22/04/2021

367 Online sexual exploitation of children in the Philippines (IJM, 2020) Accessed from: https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 22/04/2021

368 Cryptocurrency and the Blockchain (International Centre for Missing and Exploited Children, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/05/ICMEC-FCACPCryptocurrencyPaperFINAL5-17.pdf 22/04/2021

369 Case Study: The Fintel Alliance – a public private partnership (AUSTRAC, 2021) Shared by the Australian Department of Home Affairs, 19/05/2021

370 IJM Composite Case Study - 'Follow the Money' – Trafficking for livestreamed Online Child Sexual Exploitation. Received by email 31/03

371 Cryptocurrency and the Blockchain (International Centre for Missing and Exploited Children, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/05/ICMEC-FCACPCryptocurrencyPaperFINAL5-17.pdf 22/04/2021

372 Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence: Public Bulletin (Egmont Group, 2020) Accessed from: https://egmontgroup.org/sites/default/files/filedepot/20200901_CSAE%20Public%20Bulletin.pdf 16/07/2021

373 National Study of Online Sexual Abuse and Exploitation of Children in the Philippines (UNICEF, 2020) Accessed from: UNICEF Philippines study 22/04/2021

374 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021

375 Child Dignity Alliance: Technical Working Group Report (Child Dignity Alliance, 2017) Accessed from: https://static1.squarespace.com/static/5a4d5d4e7131a5845cdd690c/t/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf 22/04/2021

376 Cambodia feared lagging behind predators in cybersex trafficking crackdown (Reuters, 2019) Accessed from: https://www.reuters.com/article/us-cambodia-sexcrimes-children/cambodia-feared-lagging-behind-predators-in-cybersex-trafficking-crackdown-idUSKCN1VW00B 22/04/2021

377 Informe de monitoreo de país sobre la explotación sexual comercial de niños, niñas y adolescentes (ECPAT, 2014) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/04/IMP%20MEXICO.pdf 22/04/2021

378 A Global Strategic Response to Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/WeProtectGA-Global-Strategic-Response-EN.pdf 17/06/2021

379 Together to #ENDviolence: Global Policy Briefing; Key Messages (The End Violence Partnership, 2020) Received via email from the End Violence Partnership on 13/07/2021

380 Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse (World Health Organisation, 2003) Accessed from: https://www.who.int/violence_injury_prevention/resources/publications/en/guidelines_chap7.pdf 25/05/2021

381 Glossary on Sexual Exploitation and Abuse (United Nations, 2017) Accessed from: https://hr.un.org/sites/hr.un.org/files/SEA%20Glossary%20%20%5BSecond%20Edition%20-%202017%5D%20-%20English_0.pdf 25/05/2021

382 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

383 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf (23/07/2021)

384 Child Sexual Abuse Material (NCMEC) Accessed from: https://www.missingkids.org/theissues/csam 25/05/2021

385 IWF Annual Report: Glossary (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

386 Non-Photographic Visual Depictions (IWF, 2007) Accessed from: https://www.iwf.org.uk/what-we-do/who-we-are/consultations/non-photographic-visual-depictions 25/05/2021

387 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

388 Grooming (NSPCC) Accessed from: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/ 25/05/2021

389 Online Enticement (NCMEC) Accessed from: https://www.missingkids.org/netsmartz/topics/onlineenticement 25/05/2021

390 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

391 What is a deepfake? Everything you need to know about the AI-powered fake media (Business Insider, 2021) Accessed from: https://www.businessinsider.com/what-is-deepfake?r=US&IR=T#:~:text=Recently%2C%20deepfake%20technology%20has%20been,with%20another%20in%20recorded%20video. 25/05/2021

392 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic 26/01/2021

393 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)

394 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

395 IWF Annual Report: Glossary (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

396 Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children (United Nations, 2000) Accessed from: https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx

397 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

398 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

399 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

400 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

401 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

402 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf 25/05/2021

403 Safety by Design (Australian eSafety Commissioner, 2019) Accessed from: https://www.esafety.gov.au/sites/default/files/2019-10/LOG%207%20-Document8b.pdf 25/05/2021

404 The Decentralised Web of Hate (Bevensee & Rebellious Data LLC, 2020) Accessed from: https://rebelliousdata.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf 25/05/2021

405 What is a VPN? – Virtual Private Network (Cisco) Accessed from: https://www.cisco.com/c/en_uk/products/security/vpn-endpoint-security-clients/what-is-vpn.html 25/05/2021

406 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: https://www.netclean.com/2018/10/30/hash-values/ 25/05/2021

407 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: https://www.netclean.com/2018/10/30/hash-values/ 25/05/2021

408 Use of AI in Online Content Moderation (Cambridge Consultants, 2019) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf 25/05/2021

409 Darknet Cybercrime Threats to Southeast Asia (UNODC, 2020) Accessed from: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf 25/05/2021

410 End-to-End Encryption (NSPCC, 2021) Accessed from: https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf 25/05/2021

411 IWF Annual Report: Glossary (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

412 Metadata (WhatIs.com, 2021) Accessed from: https://whatis.techtarget.com/definition/metadata 24/06/2021

413 Tor (Investopedia, 2019) Accessed from: https://www.investopedia.com/terms/t/tor.asp 07/05/2021

414 Convention on the Rights of the Child (United Nations, 1989) Accessed from: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx 25/05/2021

415 How we protect children's rights with the UN Convention on the Rights of the Child (UNICEF) Accessed from: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx 25/05/2021

416 Explanatory Notes: General Comment no.25 on children's rights (5Rights Foundation, 2021) Accessed from: https://5rightsfoundation.com/uploads/ExplanatoryNotes_UNCRCGC25.pdf 25/05/2021

417 Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (WePROTECT Global Alliance, 2020) Accessed from: https://www.weprotect.org/response/technology/ 25/05/2021

418 Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response (WePROTECT Global Alliance, 2016) Accessed from: https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf 25/05/2021

419 Lanzarote Convention (Council of Europe) Accessed from: https://www.coe.int/en/web/children/lanzarote-convention 25/05/2021

420 Glossary: E-privacy Directive 2009/136/EC (European Data Protetion Supervisor) Accessed from: https://edps.europa.eu/data-protection/data-protection/glossary/e_en#e-privacy_directive2009-136-ec 25/05/2021

421 The EU will continue to protect children from child sexual abuse online (European Commission, 2020) Accessed from: https://ec.europa.eu/home-affairs/news/20200910_eu-continue-protect-children-from-child-sexual-abuse-_en 25/05/2021

422 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf

423 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 28/05/2021